الحماية القانونية لأساليب الدفع الإلكتروني

إعداد الطالبة
سارة جمال زين العابدين*

إشراف الدكتور
جميل صابوني**

ملخص

تسبر هذه المقالة أغوار الآفاق القانونية المتصلة بحماية أساليب الدفع الإلكتروني قانونياً، آخذةً بالحسبان أنَّ نجاح أساليب الدفع الإلكتروني في تحقيق الأغراض المنشودة من وراء استحداثها، إنما يتوقف أساساً على مدى الحماية القانونية لها.

وهذا مرده اتصال فعالية عمل أساليب الدفع الإلكتروني بأسلوب الحماية المقرر لها من الناحيتين الفنية والتشريعية.

وموضوع هذه المقالة، هو تحليل الحماية الفنية لأنظمة الدفع الإلكتروني، ودراسة الجوانب المختلفة للحماية التشريعية لأنظمة الدفع الإلكتروني من منظور مقارن، وقد تم التوصل إلى مجموعة من المقترحات، بما يسهم في تأمين حماية قانونية لأساليب الدفع الإلكتروني انسجاماً مع طبيعتها غير التقليدية.

الكلمات المفتاحية: دفع إلكتروني، حماية فنية، مخاطر إلكترونية، حماية تشريعية.

* طالبة دكتوراه، جامعة دمشق، كلية الحقوق، قسم القانون العام.

** أستاذ، جامعة دمشق، كلية الحقوق، قسم القانون العام.

Legal protection of electronic payment methods

Submitted By
Sarah Jamal Zain AlAbdeen [*]

Supervised By
Prof. Jamil Sabouni [**]

Abstract

]This article explores the legal perspectives relating to the legal regime for the protection of electronic payment methods, bearing in mind that the success of electronic payment methods in achieving the desired latitude as a result of their development depends mainly on their legal protection.

This is due to the relevance of the effectiveness of the electronic payment methods' work to their planned technical and legislative protection.

The subject of this article is the analysis of the technical protection of electronic payment systems, the examination of the various aspects of legislative protection of electronic payment systems from a comparative perspective, and a series of proposals have been reached, contributing to the legal protection of electronic payment methods in line with their non-traditional nature.

Keywords: electronic payment, technical protection, electronic risk, legislative protection.

[*] PhD Student, Damascus University, Faculty of Law, Department of Public Law.

[**] Professor, Damascus University, Faculty of Law, Department of Public Law.

المقدمة

تُقبِل المجتمعات المعاصرة كل يوم، نحو مراحل جديدة من مراحل نموها الاجتماعي والاقتصادي، وقد رافق ذلك سلوكيات مستحدثة تعتمد على البيانات والمعلومات المتداولة عبر شبكة الإنترنت، وبفضل تطور البيئة العالمية لتقنية المعلومات لم يكن من المفاجئ ظهور آثار على سلوكيات بعض الأفراد، والتي أفرزت أنماطاً جديدةً من الجرائم ذات العلاقة بتكنولوجيا المعلومات؛ يرتكبها مجرمون محترفون متخصصون لديهم قدرة فائقة من المهارات التقنية، يستغلونها في اختراق الشبكات وكسر كلمات السر وفك الشيفرات.

إنَّ تنوع وتطور أساليب الدفع الإلكتروني والتوسع المستمر في استخدامها ساعد على تزايد فرص واحتمالات ارتكاب الجرائم الإلكترونية (السايبرانية) عليها، وذلك جعلنا نذهب إلى ضرورة الاهتمام بإنشاء نظم خاصة تحمي أنظمة الدفع الإلكتروني من أخطار الاعتداءات عليها، بتقنيات وآليات خاصة؛ بل وجعل ذلك الدول تنبّه إلى ضرورة تبني نصوص تشريعية متلائمة مع تحديات العصر الرقمي بما فيه أساليب الدفع الإلكتروني من أجل تعزيز الثقة في مصداقيتها والتعامل بها.

إشكالية البحث:

تتمثل إشكالية البحث من خلال أن تنوع وتطور أساليب الدفع الإلكتروني والتوسع في استخدامها أدى إلى احتمالية أن تكون تلك الأساليب محلاً لأعمال إجرامية ذات طابع غير تقليدي، وهذا ما يؤدي بالضرورة إلى وضع نظام قانوني يؤمن الحماية الكافية لأساليب الدفع الإلكتروني، وفي هذا الصدد تبرز تساؤلات عدة، وهي:

– هل تعد الحماية الفنية لأساليب الدفع الإلكتروني مفهوماً تقليدياً أم غير تقليدي إزاء خصوصية أساليب الدفع الإلكتروني؟

– ما هي المخاطر التي تحيط بأنظمة الدفع الإلكتروني؟

– كيف تتمثل الحماية الفنية لأساليب الدفع الإلكتروني؟

– هل عمل المشرع على تأمين حماية كافية لأساليب الدفع الإلكتروني؟

– إزاء الطابع العابر للحدود الوطنية للاعتداء على أساليب الدفع الإلكتروني، هل ثمة جهوداً دولية لحماية أساليب الدفع الإلكتروني؟

أهداف البحث:

تكمن أهداف البحث من خلال الآتي:

– دراسة مفهوم الحماية الفنية لأنظمة الدفع الإلكتروني أو بيان خصوصيتها.

– دراسة المخاطر التي تهدد أنظمة الدفع الإلكتروني.

– بيان الآليات الفنية المستحدثة لحماية أنظمة الدفع الإلكتروني.

– دراسة جوانب الحماية التشريعية لأنظمة الدفع الإلكتروني وصولاً إلى معرفة مدى فاعلية الحماية التشريعية.

أهمية البحث:

تبرز أهمية البحث من خلال الانتشار غير المسبوق لأساليب الدفع الإلكتروني، واستحواذ الأخيرة على غالبية معاملاتنا اليومية، والتوسع الكبير في نوعية الخدمات التي تعتمد على أنظمة الدفع الإلكتروني، وقد بات ضرورياً وضع نظام قانوني يؤمن حماية كافية لأنظة الدفع الإلكتروني، ويراعي خصوصيتها.

فرضية البحث:

تتمثل فرضية البحث من خلال أنَّ وجود آليات فنية معززة بحماية تشريعية لأساليب الدفع الإلكتروني، سيؤدي إلى تعزيز دورها كأداة وفاء في المعاملات الخدماتية والاقتصادية.

منهج البحث:

بغية الإجابة العلمية عن التساؤلات الواردة في إشكالية البحث، وتأمين تغطية شاملة لجوانب البحث، فإننا سنتبع المنهج التحليلي من خلال دراسة تحليل الإجراءات الوقائية المتمثلة بالحماية التقنية لأنظمة الدفع الإلكتروني، وسنتبع أيضاً المنهج المقارن بغية معرفة الاتجاهات التشريعية حول حماية أنظمة الدفع الإلكتروني.

خطة البحث:

يقتضي الطرح التحليلي لفكرة النظام القانوني لحماية أساليب الدفع الإلكتروني إلى تقسيمه إلى مطلبين اثنين وذلك على النحو الآتي:

المطلب الأول: الحماية الفنية لأنظمة الدفع الإلكتروني.

المطلب الثاني: الحماية التشريعية لأنظمة الدفع الإلكتروني.

المطلب الأول

الحماية الفنية لأنظمة الدفع الإلكتروني

أدّى استعمال أساليب الدفع الإلكتروني، إلى ظهور نمط جديد من الجرائم، يطلق عليه مسمى جرائم المعلومات[1].

وقد تصدّى المختصون والمشرعون لهذا النمط الإجرامي الحديث، وتجلى ذلك من خلال العمل على سد ثغرات الأنظمة الأمنية، وتطوير أساليب الحماية الفنية للنظم والبرامج المعلوماتية.

باعتبار أنَّ عدم التصدي لتلك الثغرات من الناحية الفنية سيشكل تهديداً خطيراً لبيئة العمل في عالمنا المعاصر التي تقوم على وسائل وأساليب دفع إلكتروني حديثة.

والبحث في الحماية الفنية لأنظمة الدفع الإلكتروني، يقتضي منا الوقوف عند مفهوم الحماية الفنية أو التقنية لأنظمة الدفع الإلكتروني في فرع أول، والوقوف عند أهم الآليات التقنية المستخدمة في حماية أساليب أنظمة الدفع الإلكتروني في فرع ثانٍ.

الفرع الأول – مفهوم الحماية الفنية (التقنية) لأنظمة الدفع الإلكتروني:

تقتضي اعتبارات أمن المعلومات وحماية الخصوصية عبر شبكة الإنترنت، لا سيما أنظمة الدفع الإلكتروني، توفير حماية تقنية كافية للدفع الإلكتروني وأساليبه.

---

[1] د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي (دراسة متخصصة في القانون المعلوماتي)، دار الكتب القانونية، 2007، ص14.

أولاً – تعريف الحماية الفنية لأنظمة الدفع الإلكتروني:

ترافق الإنتاج في مجال التقنيات الحديثة، مع زيادة إنتاج سبل الحماية التقنية أكثر من إنتاج التقنية نفسها[2]، فالمجرمون الذين يرتكبون الاعتداءات على أنظمة الحماية ذاتها، يطلق البعض عليهم اسم مجرمون أذكياء[3]، بسبب ارتكاب جرائمهم في الخفاء وفي بيئة إلكترونية فضائية مكونة من إشارات مغناطيسية تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصالات، دون أن تخلف جرائمهم آثار محسوسة، وخصوصاً أن أنظمة الحماية ذاتها قد صُمِّمت لمنع الاعتداء على أنظمة التقنية العالية بما تشتمل عليه هذه الأنظمة من حواسيب وبرامج وشبكات ربط واتصال.

وفي هذا الصدد، أشار مجلس الشيوخ الفرنسي إلى ضرورة الحماية التقنية عندما عرَّف مفهوم نظم المعالجة الآلية للمعطيات بأن هذا النظام هو: كل مركب يتكون من وحدة أو مجموعة أو وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج، والمعطيات، وأجهزة الربط، والتي تربط بينها مجموعة من العلاقات والتي عن طريقها تتحقق نتيجة معينة وهي حماية معالجة المعطيات، على أن يكون هذا المركب خاضعاً لنظام الحماية الفنية[4].

وقد أولت العديد من المبادرات المحلية والعالمية اهتماماً بالغاً بضرورة حماية أمن المعلومات تقنياً وتشريعياً، ويُعرَّف أمن المعلومات بأنه: حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها، ووسائط المعلومات التي تحتوي على بيانات المنشأة، ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات، وهي الكنز الثمين الذي يجب على المنشأة المحافظة عليه[5].

---

[2] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، ص133.

[3] أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، 2011، ص121.

[4] علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1996، ص120.

[5] حسن طاهر داوود، الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض، ص23.

وقد عَرَّف جانب من المختصين أمن المعلومات بأنه: الجهود الرامية إلى حماية موارد معلومات المنظمة من سوء الاستخدام من قبل الأطراف غير المصرح لهم من خلال تحديد التهديدات التي قد تواجه أمن المعلومات وتشخيص نقاط الضعف التي يعاني منها برنامج أمن المعلومات ومن ثم تحديد المخاطر المترتبة على تلك التهديدات واستغلال نقاط الضعف، ووضع سياسة أمن المعلومات وتنفيذ الضوابط والمعايير التي تسهم في تعزيز أمن المعلومات[6].

ويُقصد بالحماية التقنية للدفع الإلكتروني جميع الإجراءات الوقائية التي يتخذها مصدر وسيلة الدفع الإلكتروني أو صانعها، أثناء وضعه لها، وذلك لرد أي اعتداء خارجي قد يقع عليها[7].

كما يقصد بها، الحماية التي تعمل على إيجاد أنظمة أمان لحماية نظم المعلوماتية وتقنية المعلومات المتداولة عن طريق الشركات المنتجة للبرامج[8].

وتعرف الحماية التقنية للدفع الإلكتروني أيضاً بأنها: حماية أنواع المعلومات ومصادر الأدوات التي يتعامل معها، وتعالجها من منظمة، وغرفة تشغيل أجهزة، والأجهزة ووسائط التخزين والأفراد من السرقة والتزوير والتلف والضياع والاختراق[9].

وبناءً على جميع التعاريف السابقة يتضح لنا أن الحماية الفنية لأنظمة الدفع الإلكتروني تُعنى بجميع الوسائل والتدابير الوقائية التقنية التي تحمي نظم الدفع الإلكترونية من وقوع أي اعتداء على نظم المعلومات الخاصة بها من خلال متخصصين وذوو كفاءات عالية ومن خلال مراكز تنظيمية مسؤولة عن هذه الحماية.

---

[6] أ.د. محمد عبد حسين الطائي، د. ينال محمود الكيلاني، إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015، ص37.

[7] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر – أساليب وثغرات–، دار الهدى، الجزائر، 2010، ص111.

[8] طارق إبراهيم الدسوقي عطية، الموسوعة الأمنية – الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، 2015، ص549.

[9] محمد دباس الحميد، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007، ص34.

أما من الناحية التشريعية فقد عرف المشرع السوري أمن المعلومات بأنه: الوسائل والتدابير الخاصة بالحفاظ على سرية وتوافرية وسلامة المعلومات وحمايتها من الأنشطة غير المشروعة التي تستهدفها[10].

وقد سلطت الباحثة الضوء على حماية أساليب أنظمة الدفع الإلكتروني لأن هذه الأنظمة تعتبر المصدر الأكثر تهديداً للخصوصية، فكما تقدم تقنية الدفع الإلكتروني تسهيلات في كافة مجالات الحياة، لها أيضاً مخاطر تترتب عليها، كأن يتم إساءة استعمال بطاقة الدفع الإلكتروني من الغير كسرقة البطاقة واستعمالها أو سرقة الرقم السري واستخدامه أو تزويرها، كما يمكن التلاعب في بطاقات الائتمان عن طريق الأرقام السرية والمعلومات من المواقع، وإنشاء مواقع وهمية على أنها مواقع أصلية، وبتلقي طلبات المعاملات الخاصة بالتجارة الإلكترونية، يتم الحصول على المعلومات الموجودة فيها والاستيلاء عليها واستعمالها بشكل غير مشروع[11].

ثانياً – المخاطر المهددة لأنظمة الدفع الإلكتروني وأمن المعلومات:

ما يزيد الاهتمام بأمن المعلومات هو أنها تُستخدم من قبل الجميع بلا استثناء، الدول، الشركات والأفراد، كما أنها أصبحت هدفاً للاختراق من جانب الكثيرين، وكذلك أيضاً بلا استثناء، حيث تكون المعلومات في بعض الحالات فاصلاً بين مكسب وخسارة لشركة ما، وعلينا حماية هذه المعلومات من الأخطار التي تهددها[12]، وتتنوع الأخطار والطرق المستخدمة لإتلاف البيانات والمعلومات والبرامج، ويسمى البعض الجرائم المرتكبة بواسطة هذه المخاطر، جرائم باستخدام الكمبيوتر Computer– related

---

[10] القانون رقم /7/ لعام 2023، الذي أقره مجلس الشعب السوري في جلسته المنعقدة بتاريخ 2023/3/27.

[11] شيماء جودي، تمثلات الأستاذ الجامعي للخصوصية الرقمية، مذكرة مقدمة لنيل شهادة الماستر، جامعة العربي التبسي، تبسة، قسم علوم الإعلام والاتصال، الجزائر، 2021، ص16.

وانظر أيضاً: د. عبود السراج، شرح قانون العقوبات الاقتصادي في التشريع السوري والمقارن، الطبعة الأولى، منشورات جامعة دمشق، 2010م، ص294.

[12] وافد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة لنيل درجة الماجستير في القانون، جامعة مولود معمري، وزر، كلية الحقوق، 2011، ص147.

Crimes[13]، لأن الكمبيوتر أو الإنترنت أو الشبكة هي وسيلة ارتكاب الجاني للجريمة والتي من الممكن ارتكابها بأي وسيلة أخرى.

وفيما يلي نستعرض الأدوات التي تهدد أنظمة الدفع الإلكتروني على النحو الآتي:

1. فيروسات الحاسب الآلي:

وهي عبارة عن برامج خبيثة تتسلل إلى البرمجيات بحيث تدخل إليها وتنسخ نفسها على برامج أخرى في الحاسب الآلي.

وتعرّف البرامج الخبيثة بأنها: برمجيات حاسوبية مصممة لإلحاق الضرر بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو المواقع الإلكترونية، أو الشبكة، أو تعطيل عملها أو تبطئته، أو تخريب محتوياتها أو مواردها، أو جمع معلومات عنها، أو عن مالكيها، أو مستخدميها، أو عن بياناتها دون إذنهم، أو إتاحة الدخول إليها أو استخدام مواردها بصورة غير مشروعة[14].

وتتعدد أوجه استخدام البرامج الخبيثة أو الفيروسات، فهي إما أن تكون بغرض حماية أو بغرض تخريب[15]، حيث يكون غرضها الحمائي هو حماية البرامج والبيانات من النسخ غير المرخص أو غير المشروع، حيث يقوم الفيروس بتنشيط نفسه بمجرد الضغط على زر النسخ ويدمر نظام الحاسب الآلي أو البرنامج الذي يعمل عليه.

أما غرضها التخريبي، فهو واضح من اسمها، ويكون غرض واضعها التخريب من أجل الابتزاز أو الدعاية أو الحصول على منفعة شخصية.

---

[13] Brian Carrier. Defining Digital Forensics Examination and analysis Tools. In Digital Research workshop II, 2002, available at: http://www.dfrws.org/dfws2002/papers/papers/Briancarrier.pdf.

[14] القانون السوري رقم /20/ لعام 2022 الخاص بالجريمة الإلكترونية ومكافحة اللجريمة المعلوماتية، المواد /1-16/ والتعليمات التنفيذية الخاصة به.

[15] د. محمد حسام محمود لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان "الجرائم الواقعة في مجال تكنولوجيا المعلومات"، القاهرة، 1993، منشورات النهضة العربية، ص496.

وهذه الفيروسات تنتقل في حال تم نسخ البرامج التي تحملها أو عن طريق تحميل البيانات والمعلومات بحيث تنسخ نفسها داخل وحدة التخزين الرئيسية الصلبة داخل الجهاز (HD)، وتسيطر على نظام التشغيل حتى تُعَطِّل الجهاز كلياً، وقد تنسخ نفسها بشكل متكرر، بحيث يتعذر تنزيلها على الذاكرة العشوائية (RAM) مما يؤدي إلى عدم إمكانية تشغيل البرامج[16].

وتقسم أنواع البرمجيات الخبيثة (فيروسات الحاسب الآلي) إلى أربعة أنواع[17]:

أ. فيروس عام العدوى: وهو فيروس ينتقل إلى أي برنامج أو ملف وهدفه تعطيل نظام التشغيل بأكمله.

ب. فيروس محدد العدوى: وهو فيروس يستهدف نوعاً معيناً من النظم ليهاجمه، ويتميز في صعوبة اكتشافه وبطء انتشاره.

ج. فيروس عام الهدف: وهو فيروس سهل الإعداد، ويتسع مدى تدميره، وتتدرج تحته غالبية الفيروسات.

د. فيروس محدد الهدف: وهو فيروس سيقوم بتغيير الهدف من عمل البرامج دون أن يقوم بتعطيلها، وهو يحتاج مهارة عالية وذكاء بالتطبيق أو البرنامج المستهدف، كأن يحدث تلاعباً مالياً أو تعديل معين في تطبيق عسكري كفيروس طروادة، والتي سهلت مواقع الانترنت انتشاره، حيث يعتبر فيروس طروادة أو ما يعرف بحصان طرواده برنامجاً يضعه المخرب داخل برامج عادية، وهو يختفي ويتكرر حتى يبدو غير مؤذٍ، ويواصل الحاسب الآلي عمله بصورة طبيعية ويتم إجراء تعديلات سرية في البرامج

---

[16] علي محمد الشوابكة، جرائم الشبكة الدولية للإنترنت ووسائل مكافحتها، مؤتمر التطور التقني وفاعلية العملية التدريبية، الإمارات العربية المتحدة، بحث رقم /10/، 1998، ص30.

[17] محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، بعنوان "جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات"، القاهرة، 1993، ص191.

والملفات ويمحو أو يدمر البيانات أو حتى يسبب إغلاقاً كاملاً، كما يمكن أن تبرمج أحصنة الطروادة لتدمير كل آثار وجودها بعد التنفيذ[18].

كما أنه لا توجد نوعية واحدة لحصان طروادة، حيث تندرج تحت هذه التسمية عدة أنواع من الفيروسات[19].

2. برامج تقنيات السلامي:

ويقصد بها أن يقوم المخرب بإعداد مجموعة من الرموز السرية لبرامج الكمبيوتر، بحيث يؤدي إلى تغييرات صغيرة جداً لا يمكن توقعها أو اكتشافها، ولكنها تؤثر تراكمياً في البرامج، وهذا التأثير التراكمي يسبب ضرراً كبيراً[20].

3. برامج الدودة:

وهي عبارة عن برامج تستغل أي فجوة في نظام التشغيل كي ينتقل حاسب إلى آخر، أو من شبكة إلى أخرى، وتتكاثر أثناء عملية الانتقال بإنتاج نسخ منها، وتهدف هذه البرامج إلى العمل على تخفيض كفاءة الشبكة، أو تخريب الملفات والبرامج ونظم التشغيل، وذلك بإشغال حيز من سعة الشبكة[21].

ولقد ظهرت برامج الدودة لأول مرة في عام 1988 في الولايات المتحدة الأمريكية على يد طالب في جامعة كورنل ويسمى موريس، حتى سميت باسمه، وقد تسببت آنذاك في تدمير الآلاف من الحواسيب، وتتسبب حركة برامج الدودة في تجميد لوحة المفاتيح والشاشة والذاكرة وغيرها من عمليات التخريب، وهناك عدة أشكال من برامج الدودة، أشهرها دودة الحب وAnna Virus[22].

---

[18] طارق عبد العال حماد، التجارة الإلكترونية، الأبعاد التكنولوجية والمالية والتسويقية القانونية، الدار الجامعية، ط2، الإسكندرية، 2007، ص160.

[19] د. طارق الخن، جرائم المعلوماتية، الجامعة الافتراضية السورية، 2018، ص45.

[20] طارق عبد العال حماد، نفس المرجع، ص101.

[21] د. محمد سامي الشوا، مرجع سابق، ص193.

[22] د. طارق الخن، نفس المرجع، ص45.

4. القنبلة الزمنية والقنبلة المنطقية:

والقنبلة المنطقية هي عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى، وتهدف إلى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة بحيث تعمل على مبدأ التوقيت، فتحدث تدميراً أو تغييراً في المعلومات والبرامج عند إنجاز أمر معين في الحاسب الآلي، أو برنامج معين، ومثالها زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف بحيث تنفجر لتنمحي سجلات الموظفين الموجودة في الأصل داخل المنشأة، ففي أمريكا ولاية لوس أنجلوس تمكن أحد العاملين بإدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها، مما أدى لتخريب هذا النظام على عدة مرات[23].

أما القنبلة الزمنية، فسميت بذلك لقيامها بالتخريب في وقت محدد سلفاً، والقنبلة الزمنية على عكس المنطقية فهي تثير حدثاً في لحظة زمنية محددة بالتاريخ واليوم والساعة اللازمة، ومن أمثلتها، قيام محاسب خبير في نظم المعلومات، بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة، وذلك انتقاماً من المنشأة التي يعمل بها لفصله منها، حيث انفجرت بعد مضي 6 أشهر من رحيله، وترتب عليه إتلاف كل البيانات المتصلة بها[24].

5. الحفلة التنكرية:

حيث تتم كتابة برامج حاسب آلي تنشط أو تحفز البرنامج الحقيقي، كأن تتم كتابة برنامج لتنشيط شاشة (Log in)، وعندما يحاول المستخدم الدخول (Log in) يلتقط الحاسب رقم هوية المستخدم وكلمة السر الخاصة به، ويعرض رسالة خاطئة،

---

[23] محمد الشوا، مرجع سابق، ص196.

[24] د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان الجرائم الواقعة في مجال تكنولوجيا المعلومات، القاهرة، 1993، منشورات دار النهضة العربية، ص427.

فيحاول المستخدم الدخول من جديد، وينجح فعلاً في المرة الثانية، بعد أن كانت المرة الأولى للحصول على ID التعريف الخاص به[25].

6. فيروسات التصيد الاحتيالي:

تعتبر الملفات الحاملة للفيروس فهي وسائل التصيّد الجذابة، حيث تسمح للمهاجمين بالتفاعل مع المستخدمين بشكل فعال، مما يجعل مخططاتهم الاحترافية قابلة للتصديق بشكل أكبر على عكس عمليات التصيّد المعتمدة على البريد الإلكتروني، وأبرز توجهات وأساليب اعتمدها المهاجمون في عام 2020 لشن هجمات التصيد الاحتيالي بالاعتماد على ملفات من نوع PDF، وملفات التحقق المزيفة، قائم الكوبون الوهمية، صورة ثابتة مع زر التشغيل، تبادل الملفات[26].

وفي النهاية تجدر الإشارة إلى ضرورة حماية قواعد البيانات أو البرامج أو نظم المعلوماتية من خطر هجمات الهاكرز، لا سيما إذا تعلقت بأنظمة الدفع الإلكتروني، لأن إساءة استعمال أنظمة الدفع الإلكتروني عن طريق إساءة استخدام شبكة الإنترنت يتداخل مع سير الحياة الاجتماعية، ولا بدّ من ضمان ممارسة الأفراد لحقوقهم وحرياتهم بصورة آمنة.

فضلاً عن حماية المصلحة العامة وإحداث التوازن بين حقوق الفرد وحرياته وبين الواجبات العامة، وذلك يتعلق بدستورية القوانين التي تضع الضمانات الأساسية لحماية تلك الحقوق والحريات وتكفل استعمالها وعدم التعدي عليها[27].

وعليه تستعرض الباحثة في الفرع الثاني أهم آليات الحماية التقنية المعدة لذلك.

---

[25] طارق عبد العال حماد، مرجع سابق، ص101.

[26] صحيفة الخليج، 2023، توجهات لهجمات التصيد الاحتيالي عبر ملفات بي دي إف 5، 19، أبريل، ص1و2.

[27] د. حسن مصطفى البحري، القانون الدستوري (النظرية العامة)، كلية الحقوق، الجامعة الافتراضية السورية، دمشق، 2009، ص7.

الفرع الثاني – الآليات الفنية المستخدمة في حماية أساليب أنظمة الدفع الإلكتروني:

دفع التطور الحاصل في أنظمة الدفع الإلكتروني إلى ضرورة إيجاد وسائل وتقنيات وضعت تحت تصرف المتعاملين بها، كي يضمن ذلك أكبر قدر ممكن من الثقة والطمأنينة ذلك لأن المساس في هذه الأنظمة من شأنه أن يؤثر على الذمة المالية لعملاء البنوك، وعلى سمعة البنوك أيضاً، ومن الممكن أن تنتج خسائر مادية للبنوك نتيجة الإضرار بسمعتها[28].

لذلك ستتناول الباحثة أهم الآليات التقنية المستخدمة في مجال تأمين المعلومات المتداولة، وتأمين حماية الحاسبات الشخصية والحاسبات الخادمة، تأمين وحماية شبكة الربط بالإنترنت والتأمين من التهديدات والاختراقات[29]، على النحو الآتي:

أولاً – تقنية الكلمات السرية أو الأرقام السرية كوسيلة لحماية الدفع الإلكتروني:

تعتبر كلمة السر وسيلة من وسائل حماية الحاسب الآلي الشخصي، إذ لا يمكن الدخول إلى الحاسب واستعماله دون معرفة كلمة العبور، وكذلك بالنسبة للملفات المخزنة على الحاسب، فلا يمكن الدخول إليها إلا بمعرفة كلمة السر التي تعد مانعاً من الوصول إلى هذه الملفات[30].

---

[28] محمود محمد أبو فروة، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة، عمان، الأردن، 2009، ص76.

[29] د. أحمد الشربيي، د. وفائي بغدادي، حماية وتأمين الإنترنت، التحدي القادم وأساليب المواجهة، سلسلة العلوم والتكنولوجيا، الهيئة المصرية العامة للكتاب، القاهرة، 2010، ص156.

[30] د. عبد الفتاح بيومي حجازي، الحماية التقنية والجنائية لنظام الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2004، ص103.

وتعد كلمة السر أحد أبرز الوسائل التأمينية (الحمائية) لأنظمة الدفع الإلكتروني[31]، التي تمكن المصارف والمؤسسات المصدرة لوسائل الدفع الإلكتروني من الكشف عن هوية المخترقين وأماكن دخولهم إلى الشبكة، بحيث تمنع هذه البرامج اقتحام الشبكات أو نظم المعلومات[32].

وهناك نظام أمني يتشابه مع –كلمات العبور– في منع الدخول إلى ملفات ومعلومات الشبكة ونظم تشغيلها، وإن كان يختلف عنها، وهو نظام البروكسي (Proxy)، حيث أن مزودات البروكسي تقوم بدور الوسيط بين المشتركين في خدمة الإنترنت لدى الجهة التي تقوم بذلك، مثل مؤسسة اتصالات في دولة الإمارات وما بين المواقع الموجودة على الشبكة العالمية، حيث أن مزود البروكسي يستخدم كذلك كحائط منع أو جدار ناري (Fire Wall) حيث يفلتر رزم المعلومات الصادرة من وإلى الشبكات من شبكة إنترنت[33].

وعليه، فإن إجراء الحماية بواسطة كلمة السر يعتبر الإجراء الأكثر أماناً واستعمالاً في الفضاء الرقمي في هذا العصر، وإن استعمال كلمة السر يخول صاحبها تأمين معاملاته لما يريده من البيانات السرية والشخصية وكذلك تأمين كافة معطياته[34].

وفي نطاق بحثنا، لا بد من التنويه، إلى أن بعض البنوك بدأت تصدر بطاقات تجيز السحب والوفاء في آنٍ واحد، تحمل هذه البطاقات رمزاً سرياً لا تتم عملية السحب والوفاء إلا به، وقد ساهم استخدام كلمة السر في التقليل من الاستخدام غير المشروع لبطاقات الاعتماد، بحيث يمنع سارق البطاقة أو مزورها من استخدامها[35].

---

[31] يقصد بالوسائل التأمينية لأنظمة الدفع الإلكتروني إلزام الشركات المنتجة للبرامج بوضع عراقيل فنية للحيلولة دون دخول المتلصصين أو القراصنة إلى تلك البرامج، وما تحويه بنوك المعلومات وقواعد البيانات والبريد الإلكتروني من أسماء تجارية وصناعية أو مراسلات خاصة، طارق إبراهيم الدسوقي، المرجع السابق، ص549.

[32] طارق إبراهيم الدسوقي، المرجع نفسه، ص549.

[33] د. ممدوح عبد الحميد عبد المطلب، الجريمة عبر الإنترنت، منظور أمني، بحث مقدم إلى مؤتمر القانون والكمبيوتر (99)، والإنترت، ص108.

[34] Jeffry F. Rayport, Bernard J. Jauroski, Commerce électrenique, Editiion chenelierem MC Gram– Hill, Montréal– toronto, 2003, p. 56.

[35] نضال سليم برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة، عمان، الأردن، ط1، 2009، ص161.

كما أنه ومن أجل الحد من الاستخدام غير المشروع للبطاقات، استحدثت بطاقات وفاء ذكية تحمل رقم سري خاص، وتشكل بطاقة دفع آمنة، حيث يتولد الرقم السري عن طريق خوارزميات، بحيث يدخل العمل البطاقة في آلة قراءة مع إدخال الرقم السري الموجود في البطاقة، فإذا كانا متطابقين تتم العملية، أما إذا كانا غير متطابقين، فإنه يعطي حامل البطاقة محاولتين ثانيتين، فإذا أخطأ رغم ذلك في إدخال الرقم السري الصحيح، يعطي أمراً تلقائياً لتعطيل نفسه، فتصبح البطاقة غير صالحة للاستخدام[36].

وعلى الرغم من هذا الإجراء الحمائي الذي يستخدمه العميل، فإن الابتكارات الخاصة التي يحترفها مجرمو الانترنت، تمكنهم من الوصول لمعرفتها.

ثانياً – تشفير البيانات كوسيلة لحماية الدفع الإلكتروني:

يقصد بالتشفير فن حماية المعلومات عن طريق تحويلها إلى رموز غير مقروءة، ولا يمكن حلها إلا من خلال مفتاح سري يحوّل تلك الرموز إلى نصوص عادية مقروءة[37]، وهو تغيير لمظهر المعلومات بحيث يختفي معناها الحقيقي، من خلال إخفائها عن كل من ليس له صفة الاطلاع عليها، أو العبث بمحتوياتها بتغيير شكلها إلى صورة لا يمكن فهمها، إلا بعد إعادتها إلى صورتها الأصلية، وهذا لا يمكن أن يتم إلا باستخدام مفتاح معين، لا يملكه سوى صاحب الحق في الاطلاع على المعلومات[38].

كما يقصد بالتشفير، التغيير في شكل البيانات، عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها[39].

---

[36] نضال اسماعيل برهم، المرجع نفسه، ص160-161.

[37] عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، 2009، ص62.

[38] عادل محمود شرف، عبد الله إسماعيل عبد الله، ضمانات الأمن والتأمين في شبكة الإنترنت، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة في الفترة ما بين 1-3 ماي 2003، الطبعة الثالثة، المجلد الثاني، 2004، ص398.

[39] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، ص311.

والهدف من إجراء التشفير هو ضمان الخصوصيات، وعدم السماح لأحد العبث بها، أو الاطلاع عليها كونها سرية جداً[40].

إذ يقوم التشفير كإجراء بتوفير الثقة والأمان في المعاملات الإلكترونية، حيث يسمح من خلال أدوات ووسائل وأساليب تحويل الملفات، بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها غير المشروع، بحيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي ذات البيانات التي قام المرسل بالتوقيع عليها[41].

وتفادياً لأي اختراق أو عبث في الثغرات الموجودة في برامج التشفير فإن هذه البرامج تتم بعدة أساليب أهمها:

1. التشفير باستخدام المفتاح المتماثل:

ويعد أهم أنواع التشفير المستخدمة، والذي يستخدم فيه مفتاح سري لتشفير رسالة ما، من مرسلها وفك تشفيرها من المستقبل، وسبب تسميته بالتشفير المتماثل، كون المفتاح المستخدم في عملية التشفير هو ذاته المستخدم في عملية فك تشفيرها[42].

2. التشفير باستخدام المفتاح غير المتماثل:

ويتم فيه تشفير البيانات وفكها باستخدام مفتاحين أحدهما عام والآخر خاص، ويكون المفتاح الخاص معروفاً لدى جهة واحدة فقط (المرسل)، ويستخدم لتشفير البيانات وفك شيفرتها، أما المفتاح العام فيكون معروفاً لدى أكثر من شخص أو جهة، ويستطيع المفتاح العام فك شيفرة الرسالة التي تم تشفيرها بالمفتاح الخاص بذلك، وليس لأحد أن

---

[40] عصام عبد الفتاح مطر، نفس المرجع، ص62.

[41] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001، ص31.

[42] عصام عبد الفتاح مطر، مرجع سابق، ص56.

يستخدم المفتاح العام لفك الشيفرة، سوى مالك المفتاح الخاص هو الوحيد القادر على فك شيفرة البيانات المشفرة بالمفتاح العام[43].

3. المزج بين نظامي المفتاح المتماثل والمفتاح العام (اللامتماثل):

ويعتبر هذا النظام مختلطاً، حيث يقوم المنشئ بعد كتابة الرسالة بتشفيرها بالمفتاح المتماثل وتشفير المفتاح المتماثل بالمفتاح العام، ويرسلها بعد ذلك للمستقبل الذي سيقوم بحل شيفرة المفتاح العام عن طريق مفتاحه الخاص، ليحصل بعد ذلك على المفتاح المتماثل المستخدم في تشفير الرسالة المستلمة، وبعدها يقوم بحل شيفرة الرسالة باستخدام المفتاح المتماثل[44].

وتخضع تقنية التشفير لعدة ضوابط وقواعد أهمها[45]:

أ. استخدام التشفير كوسيلة مقبولة قانوناً في شأن تحرير البيانات والمعلومات بواسطة الجهات المختصة.

ب. احترام سرية البيانات المشفرة والاعتراف بحق الخصوصية مع تجريم اختراقها والعبث فيها.

ج. إباحة تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل فيها من خلال الوسائط الإلكترونية.

ثالثاً – تقنية جدران الحماية النارية كوسيلة لحماية الدفع الإلكتروني:

ويقصد بجدار الحماية، الأنظمة التي توفر وسيلة أمنية بين شبكة الإنترنت وشبكة المؤسسة الداخلية والخروج منها للمرور عبر هذا الجدار، الذي يتصدّى لكل

---

[43] محمد فواز محمد المطالقة، الوجيز في عقود التجارة الإلكترونية، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006، ص165.

[44] مليكاوي مولود، التجارة الإلكترونية، دار هومة للطباعة والنشر والتوزيع، بوزريعة، الجزائر، 2019، ص143.

[45] هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، المنعقد في الفترة من 10 إلى 12 مايو، 2003، المجلد الثاني، ص590.

محاولات الدخول إلى الشبكة بدون صفة، حيث تمنع جدران الحماية من دخول الأخطار القادمة من شبكة الإنترنت، إلى الشبكة الداخلية الخاصة بالبنك[46].

وتستخدم جدران الحماية في تركيز الإجراءات الأمنية عند نقطة واحدة، لأن ذلك أفضل من توزيعها، فرض السياسة الأمنية التي يريدها البنك على عملائه، تسجيل وقائع استخدام الموقع بدقة عند مرورها بجدار الحماية، والحد من درجة تعرض الشبكة الداخلية للأخطار القادمة من الإنترنت[47].

ويمكن القول بأنّ وظيفة الجدار الناري هي عملية مسح المعلومات التي تصل من شبكة الإنترنت ويقوم بتحليلها، وعندما يجد أي شك في المعلومات التي تصل إليه لمحاولة الدخول أو الاختراق إلى المناطق المؤمنة، فإنه يقوم بمنع هذه المحاولة وطردها خارج الشبكة، أما إذا كانت المعلومات عادية وآمنة فإن الجهاز يسمح لها بالمرور والدخول على أجهزة الحاسبات الآلية[48]، كما أنه يقوم بأكبر قدر ممكن من التغلب على الثغرات الأمنية وفق أسس وقواعد يتم تحديدها وبناءها في الجدار الناري المنفذ في شبكة البنك[49].

وعادةً ما تلجأ المصارف إلى تقنية الجدار الناري، ومن أجل تسهيل تبادل المعلومات بين فروع المصرف، إذ يقوم المصرف بربط فروعه بشبكة واحدة تدعى بالشبكة الداخلية الخاصة؛ كما يمكن للمصرف أن ينشئ شبكة خاصة افتراضية وهي عبارة عن قناة اتصال مشفرة تقام من خلال شبكة الإنترنت مثلاً، وتكون هذه الشبكة

---

[46] إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون، الكمبيوتر والإنترنت، المنظم من قبل جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة، 2004، ص976.

[47] محمود محمد أبو فردة، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة، عمان، الأردن، 2009، ص94.

[48] أيمن عبد الحفيظ، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دار انهضة العربية، القاهرة، 2003، ص158.

[49] محمد الصيرفي، الإدارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص330.

الافتراضية عادةً رابطة بين شركتين أو موقعين لتشفير جميع المعلومات المتبادلة بينهما[50].

ومن خلال دراسة الطرق الفنية المختلفة في حماية أنظمة الدفع الإلكتروني يمكن القول بأن تقنية الحوائط النارية Fire wall من أهم الأدوات الأمنية المستخدمة في تأمين الشبكات ومنع الاتصالات الخارجية المترتبة في الانترنت دون الوصول إلى داخل الشبكة، فضلاً عن قيامها ببعض الخدمات المتوفرة على الشبكة الدولية[51]، وسننتقل إلى دراسة كيفية تصدي المشرع لحماية أنظمة الدفع الإلكتروني من الناحية التشريعية.

---

[50] حسن طاهر داوود، أمن شبكات المعلومات، معهد الإدارة العامة، السعودية، 2004، ص385.

[51] أمير حيدر، حماية الدفع الإلكتروني، مقال منشور على الموقع الإلكتروني:
www.islamonline.com..2004/11/12 تاريخ النشر

المطلب الثاني

الحماية التشريعية لأنظمة الدفع الإلكتروني

تصدى المشرع في دول عالمنا المعاصر إلى التحديات القانونية التي تواجه أنظمة الدفع الإلكتروني، وذلك من خلال استحداث نصوص قانونية إجرائية تحمل في طياتها طرقاً إجرائية، تمكن القائمين في الحكومات من توفير حماية تشريعية لوسائل أنظمة الدفع الإلكتروني.

وعليه سنتعرض، في هذا المطلب إلى الحماية القانونية في ظل التشريعات العربية في فرع أول، ثم التعرض إلى التعاون الدولي لحمايةأنظمة الدفع الإلكتروني في فرع ثانٍ.

الفرع الأول: حماية أنظمة الدفع الإلكتروني وفق التشريعات العربية.

الفرع الثاني: حماية أنظمة الدفع الإلكتروني وفق الجهود الدولية.

الفرع الأول – حماية أنظمة الدفع الإلكتروني وفق التشريعات العربية:

تبنت معظم دول العالم تشريعات خاصة لحماية أنظمة الدفع الإلكتروني ضمن تشريعاتها الداخلية، وذلك بسن قوانين تعاقب على الجرائم الواقعة عليها عبر شبكة الإنترنت، وذلك لحماية المتعاملين عبر هذه الشبكة.

أولاً – في التشريعات العربية المقارنة:

1. الحماية التشريعية لأنظمة الدفع الإلكتروني في دولة الإمارت العربية المتحدة:

تصدى المشرع الإماراتي لجرائم تقنية المعلومات بسن التشريعات ووضع العديد من الضوابط لمواجهتها، وفي هذا الصدد انصب اهتمام دولة الإمارات العربية بمكافحة جرائم المعلومات والتصدي لأخطارها اهتماماً واضحاً، حيث عقدت عدة مؤتمرات أهمها مؤتمر مؤسسة الاتصالات في الإمارات العربية المتحدة عن نظم الأمن وإثبات الجرائم عبر الكمبيوتر، وهو المؤتمر الذي عقد في دبي، أكتوبر، 2003[52]، وأصدرت العديد من التشريعات المتعلقة بهذه النوعية من الجرائم عالية التقنية وهي:

[52] وثائق مؤتمر الأمن والإثبات في الكمبيوتر، دبي، الإمارات، أكتوبر،2004.

القانون العربي الاسترشادي الصادر عام 2003 بشأن مكافحة جرائم تقنية المعلومات وما في حكمها، المعتمد بموجب قرار مجلس وزراء العدل العرب المنعقد في دورته التاسعة عشر رقم (495 – د 19– 2003/10/8م) ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (417– 215 – 2004م).

وفي عام 2006 أصدرت القانون رقم /2/ لسنة 2006 الخاص بمكافحة جرائم تقنية المعلومات، ثم تلاه إصدار القانون رقم /3/ لسنة 2012م، الخاص بإنشاء الهيئة الوطنية للأمن الإلكتروني، وفي عام 2012م أصدرت المرسوم الاتحادي رقم /5/ لسنة 2012م، المتعلق بمكافحة جرائم تقنية المعلومات، وفي عام 2018 قامت بإصدار المرسوم الاتحادي رقم /2/ لسنة 2018م، الخاص بتعديل المرسوم الاتحادي رقم /5/ لسنة 2012م.

ومؤخراً صدر المرسوم بقانون اتحادي رقم /46/ لسنة 2012 بشأن المعاملات الإلكترونية وخدمات الثقة.

وأحد أهم الجرائم التي تهمنا في نطاق بحثنا، جريمة الدخول بصورة مقترنة باعتداء، فقد تضمن المرسوم بقانون اتحادي رقم /5/ جرائم الدخول في صورته المصحوبة باعتداء، أي دخول موقع إلكتروني أو نظام معلوماتي إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح أو بتجاوز حدود التصريح أو بالبقاء فيه بصورة غير مشروعة والتي يترتب عليها إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو فسخ أو نشر أو إعادة نشر أي بيانات أو معلومات، وكذلك عندما تكون البيانات أو المعلومات محل الاعتداء شخصية، وأيضاً عندما يرتكب الجاني الاعتداء بمناسبة أو بسبب تأدية عمله[53].

وتتخذ هذه الجريمة عدة صور أهمها:

- جريمة الإضرار بالبيانات أو المعلومات بصفة عامة.
- جريمة الإضرار ببيانات أو معلومات شخصية.

[53] المادة /2/ من المرسوم بقانون اتحادي رقم /5/ لسنة 2012م.

– ارتكاب الجاني جرائم الاعتداء بمناسبة أو بسبب تأدية عمله.
– الدخول بدون تصريح بقصد الحصول على بيانات حكومية.
– الدخول بدون تصريح بقصد الحصول على معلومات غير حكومية سرية.
– الإضرار بالبيانات أو المعلومات الحكومية أو غير الحكومية السرية.
– جريمة دخول موقع إلكتروني بغير تصريح لتغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه.

ونجد في المرسوم بقانون اتحادي رقم /5/ لعام 2012 الحماية من المشرع الإماراتي أو نظام المعلومات الإلكتروني أو شبكة المعلومات أو وسيلة تقنية المعلومات بصورة غير مشروعة وفق الآتي:

1. يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة المعلومات أو وسيلة تقنية معلومات بدون تصريح أو يتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة.

2. تكون العقوبة بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تتجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذ ترتب على فعل من الأفعال المنصوص عليها بالفقرة /1/ من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات.

وفي ضوء دراستنا لحماية الدفع الإلكتروني وعلاقتها بالمستندات المقدمة إلكترونياً، فقد جاء المرسوم بقانون اتحادي رقم /46/ لعام 2021 ليخدم المتعاملين بالوثائق الإلكترونية وليجدد الأمان والثقة في نفوس هؤلاء المتعاملين عندما أفرد في عدد من مواده عقوبات مشددة لكل من قام بتزوير أي مستند أو اشترك في تزويره وفق ما يلي:

المادة /39/:

يعاقب بالحبس والغرامة التي لا تقل عن (100.000) مائة ألف درهم ولا تزيد على (300.000) ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من زور أو اشترك

في تزوير المستند الإلكتروني أو التوقيع الإلكتروني أو الختم الإلكتروني، أو شهادة المصادقة أو خدمات الثقة وخدمات الثقة المعتمدة الأخرى.

ويعاقب بالحبس المؤقت والغرامة التي لا تقل عن (150.000) مائة وخمسون ألف درهم ولا تتجاوز (750.000) سبعمائة وخمسين ألف درهم كل من زور أو اشترك في تزوير المستند الإلكتروني أو التوقيع الإلكتروني أو الختم الإلكتروني أو شهادة المصادقة أو خدمات الثقة وخدمات الثقة المعتمدة الأخرى الخاصة بالحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية أو المحلية، ويعاقب بذات العقوبة المقررة لجريمة التزوير، بحسب الأحوال، من استعمل المستند الإلكتروني المزور مع علمه بتزويره.

المادة /40/:

يعاقب بالحبس مدة لا تزيد على سنة والغرامة التي لا تقل عن (100.000) مائة ألف درهم ولا تزيد على (1.000.000) مليون درهم أو بإحدى هاتين العقوبتين كل من:

1. استعمل بغير وجه حق أي خدمة من خدمات الثقة أو خدمات الثقة المعتمدة.

2. استعان بطريقة احتيالية أو اتخذ اسماً كاذباً أو صفة غير صحيحة للحصول على خدمة من خدمات الثقة المعتمدة ويعتبر ظرفاً مشدداً القيام بأي من الأفعال السابقة بهدف ارتكاب جريمة.

2. الحماية التشريعية لأنظمة الدفع الإلكتروني في سلطة عمان:

صدر في سلطنة عمان المرسوم السلطاني رقم /72/ لعام 2001 الذي نص على جرائم الحاسب الآلي في المادة /276/، حيث اشتمل المرسوم على معاقبة كل من

يعتمد استخدام الحاسب الآلي استخداماً غير مشروعاً للمعلومات أو البيانات، كما اشتمل على معاقب كافة صور التعامل غير المشروع بالبطاقات[54].

كما نص القانون نفسه على تجريم الأفعال غير المشروعة في مجال استخدامات الحاسب الآلي وبطاقات الإلكتروني، حيث نصت المادة /276/ بأنه: يعاقب بالسجن لمدة لا تقل عن ثلاثة أشهر ولا تزيد على السنتين وبغرامة تتراوح بين مائة ريال عماني إلى خمسمائة ريال أو بإحدى هاتين العقوبتين، كل من تعمد استخدام الحاسب الآلي في ارتكاب الأفعال الآتية:

1. الالتقاط غير المشروع للبيانات أو المعلومات.
2. الدخول غير المشروع على أنظمة الحاسب الآلي.
3. التجسس والتنصت على البيانات والمعلومات.
4. انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات أو الوثائق المبرمجة.
5. اتلاف وتغيير ومحو البيانات والمعلومات.
6. حمع البيانات والمعلومات وإعادة استخدامها.
7. التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع.
8. نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية.

كما نصت المادة /276/ من القانون نفسه، أن يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تتجاوز ألف ريال عماني، على كل من:

1. قام بتقليد أو تزوير بطاقة من بطاقات الائتمان أو السحب.
2. استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك.
3. قبل الدفع ببطاقة الائتمان المزورة أو المقلدة مع العلم بذلك.

---

[54] موقع وزارة العدل العمانية:

http://www.moj.gov.

ونصت أيضاً المادة /276/ من القانون ذاته: أن يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تتجاوز خمسمائة ريال عماني كل من:

1. استخدم البطاقة كوسيلة للسحب مع علمه بعدم وجود رصيد لها.
2. استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائه وهو على علم بذلك.
3. استعمل بطاقة الغير بدون علمه.

3. الحماية التشريعية لأنظمة الدفع الإلكتروني في مصر:

صدر في مصر القانون رقم /15/ لسنة 2004[55]، ونصت المادة /23/ من القانون على أنه: مع عدم الإخلال بأي عقوبة أشد في قانون العقوبات أو في أي قانون آخر يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من:

1. أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط.
2. أتلف أو عيب توقيعاً أو وسيطاً أو محرراً إلكترونياً، وزور شيئاً من ذلك بالاصطناع أو التعديل أو التحوير أو بأي طريق آخر.
3. استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً معيباً أو مزوراً مع علمه بذلك.
4. خالف أي من أحكام المادتين /19- 21/ من هذا القانون.
5. توصل بأي وسيلة بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو اعترضه أو عطّله عن أداء وظيفته.

وإدراكاً من المشرع المصري، بمدى أهمية حماية الفضاء المعلوماتي، فقد أصدر قانون مكافحة جرائم تقنية المعلومات رقم /175/ لسنة 2018[56]، وقد نص القانون على الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات، ونصت المادة /23/ على ما يلي: ((يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تتجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين كل من استخدم الشبكة

---

[55] قانون رقم /15/ لسنة 2004 بشأن التوقيع الإلكتروني.

[56] القانون المصري رقم /175/ لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

المعلوماتية أو بإحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية)).

ثانياً – في التشريع الوطني:

الحماية التشريعية لأنظمة الدفع الإلكتروني في ظل التشريع الوطني (الجمهورية العربية السورية):

سعياً منه، المشرع السوري، لمواكبة التطورات والتقدم الهائل والمتسارع، ضمن سلسلة الإصلاحات التشريعية التي تنهض بها الجمهورية العربية السورية مؤخراً فقد صدر في عام 2022 قانون مكافحة الجريمة المعلوماتية[57]؛ وفي عام 2023 صدر قانون التوقيع الرقمي وخدمات تقانة المعلومات[58].

وذلك بهدف صبط العمل والتوعية لمدى خطورة وقوع الاعتداء على سلامة وأمن المعلومات وخصوصية وسرية الأفراد، وبهدف ضمان حسن الالتزام بالضوابط الموضوعة فقد شدد القانون رقم /6/ على العقوبات لمرتكبي جرائم الأمن السيبراني، وفيما يلي أهم ما جاءت به نصوص القوانين في نطاق بحثنا.

– نصت المادة /24/ من قانون مكافحة الجريمة المعاقبة لعام 2022 على ما يلي:

أ. تحدث في الوزارة الداخلية ضابطة عدلية مختصة تكلف باستقصاء الجرائم المعلوماتية وجمع أدلتها الرقمية، والقبض على فاعليها، وإحالتها على المحاكم الموكول إليها الأمر لمعاقبتهم.

ب. تستعين الضابطة العدلية المشار إليها في الفقرة /أ/ من هذه المادة بخبراء دائمين أو مؤقتين من وزارة الدفاع ووزارة العدل، ووزارة الاتصالات والتقانة، لتنفيذ المهام الموكولة إليها، ويقسم هؤلاء الخبراء اليمين القانونية.

---

[57] القانون رقم /20/ لعام 2022 الخاص بالجريمة الإلكترونية.

[58] القانون رقم /7/ لعام 2023، الخاص بالتوقيع الرقمي وخدمات تقانة المعلومات.

وتنفيذاً لهذا النص فقد أصدر السيد وزير الداخلية القرار 564/ ق تاريخ 2012/3/22 المتضمن إحداث فرع خاص في إدارة الأمن الجنائي يسمى (فرع مكافحة جرائم المعلوماتية) لمكافحة هذه الجرائم والتحقيق فيها.

وحسناً فعل المشرع السوري بإصداره قانون الجريمة الإلكترونية لعام 2022، والذي اعتُبِر خطوة مهمة لحماية التعاملات الإلكترونية بكافة أشكالها.

وقد حدد القانون ذاته عدداً من الالتزامات التي من الواجب على مقدمي الخدمات على الشبكة التقيد بها، كما حدد عدداً من الجرائم التي يُعاقب مقترفها بعقوبات تتواءم مفعل الجاني، وأهم هذه الجرائم في حدود بحثنا لا بد من ذكر الآتي:

الامتناع عن حفظ نسخة من المحتوى الرقمي أو المعلومات:

حيث يُعاقب بالحبس من شهر إلى ستة أشهر وغرامة مليوني ليرة سورية إلى أربعة ملايين ليرة سورية، مقدم الخدمات على الشبكة الذي يمتنع عن تنفيذ إلتزامه بحفظ نسخة من المحتوى الرقمي أو المعلومات المخزنة لديه أو بيانات الحركة التي تسمح بالتحقق من هوية الأشخاص الذين يسهمون في وضع هذا المحتوى على الشبكة، أو يهمل تنفيذ هذا الالتزام.

وفي المادة التاسعة منه عاقب المشرع السوري بالحبس من ستة أشهر إلى السنة والغرامة من خمسة ملايين ليرة سورية إلى سبعة ملايين ليرة سورية، مقدم الخدمات على الشبكة الذي يقوم بصورة غير مشروعة بتغيير أو حذف المحتوى الرقمي أو المعلومات أو بيانات الحركة المخزنة لديه.

وتشدد العقوبة لتصبح السجن المؤقت من ثلاث سنوات وغرامة عشرة ملايين ليرة سورية إلى اثني عشر مليون ليرة سورية إذا كان التغير أو التعديل أو الحذف متعلقاً بمعلومات جهة عامة.

ولا بد من الوقوف على ما أفرد له المشرع السوري من عقوبات بشأن من يحاول أن يصمم أي برمجيات خبيثة أو يروّج لها لغايات إجرامية، فقد عاقب المشرع السوري

في المادة /16/ من قانون مكافحة الجريمة المعلوماتية[59] بالسجن المؤقت من خمس سنوات إلى سبع سنوات وغرامة ستة ملايين ليرة سورية إلى عشرة ملايين ليرة سورية كل من استخدام البرمجيات الخبيثة بقصد الإضرار بوسائل تقانة المعلومات أو نظم المعلومات أو الشبكة أو الحساب الشخصي.

وشدّد العقوبة لتصبح السجن المؤقت من سبع سنوات إلى عشر سنوات وبغرامة من عشرين مليون ليرة سورية إلى خمسة وعشرين مليون ليرة سورية إذا كان استخدام البرمجيات الحديثة ضد جهة عامة أو مصرف أو مؤسسة مالية مشتركة أو خاصة.

وتستند جريمة تصميم وترويج البرمجيات الخبيثة إلى ركنين، الركن المادي يتمثل بفعل التصميم والترويج للبرمجيات الخبيثة، ويقصد بالتصميم القدرة على تخليق البرامج الخبيثة باستخدام إحدى لغات الحاسوب، أما الترويج فهو الإعلان عن هذه البرامج وإبراز مميزاتها وقدراتها التقنية، أما الركن المعنوي فيجب أن يعلم الجاني بأنه يقوم بتصميم برمجيات خبيثة وأن تتجه إرادته إلى خلق هذه البرمجيات أو ترويجها وأن يكون ذلك لأغراض إجرامية[60].

والركن المادي في جرم استخدام البرمجيات الخبيثة يتمثل في فعل الاستخدام أي استعمال البرمجيات أو تحميلها أو نشرها عبر الشبكة، وركنها المعنوي يتطلب القصد الجرمي العام بعنصريه العلم والإرادة، وتوفر القصد الجرمي المتثمل بقصد الإضرار بالأجهزة الحاسوبية أو الشبكية[61].

أما أهم ما جاء به القانون رقم /7/ لعام 2023 في نطاق بحثنا فقد حدد القانون السياسات والمعايير والشروط والإجراءات الواجب التقيد بها، ويُعاقب كل كمن يخالف هذه الشروط والمعايير بعقوبات شديدة تتناسب والفعل الجرمي المرتكب نتيجة لاختراقها، ومع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر فقد نصت المادة /31/ من القانون على أنه:

---

[59] القانون رقم /20/ لعام 2022.

[60] د. طارق الخن، جرائم المعلومات، مرجع سابق، ص46.

[61] د. طارق الخن، جرائم المعلومات، نفس المرجع السابق، ص47.

أ. يعاقب بغرامة من مليون ليرة سورية إلى ثلاثة ملايين ليرة سورية كل من قام بتقديم خدمات للعموم عبر التطبيقات الإلكترونية على الشبكة قبل الحصول على الاعتمادية من الهيئة.

ب. يُعاقب بالحبس من سنة إلى ثلاثة سنوات وبغرامة من مليوني ليرة سورية إلى خمسة ملايين ليرة سورية كل من قام بارتكاب أحد الأفعال الآتية:

1. تقديم خدمات تتعلق بأمن المعلومات دون الحصول على الاعتمادية من الهيئة.

2. تقديم خدمات الاستضافة والحوسبة السحابية دون الحصول على الاعتمادية من الهيئة.

3. بيع شهادات الاتصال الآمن للعموم دون الحصول على تصريح أو اعتمادية من الهيئة.

ج. يُعاقب بالحبس من سنتين إلى ثلاث سنوات وبغرامة من ثلاثة ملايين ليرة سورية إلى خمسة ملايين ليرة سورية كل من قام بارتكاب أحد الأفعال الآتية:

1. إصدار شهادات توقيع رقمي أو تقديم أو خدمات تتعلق بالتوقيع الرقمي للعموم دون الحصول على تراخيص من الهيئة.

2. الحصول بأي وسيلة كانت بغير حق على بيانات إنشاء توقيع رقمي أو منظومة إنشاء توقيع رقمي أو وثيقة إلكترونية، أو اختراق أي منها أو اعتراضها أو تعطيلها عن أداء وظيفتها.

3. تقديم أوراق أو معلومات مزورة أو غير صحيحة بقصد الحصول على شهادة تصديق رقمي أو تعليق العمل فيها أو إلغائها.

4. إفشاء أي بيانات تتعلق باستخدام التوقيع الرقمي أو التحقق من عائديته، أو استخدامها في غير الغرض الذي قُدمت لأجله من قبل أحد العاملين لدى مزود خدمات التصديق الرقمي.

د. يعاقب بالحبس من ثلاث سنوات إلى خمس سنوات وبغرامة من خمسة ملايين ليرة سورية إلى سبعة ملايين ليرة سورية كل من قام بارتكاب أحد الأفعال الآتية:

1. تزوير أو تحريف توقيع رقمي أو بيانات أو منظومة إنشاء توقيع رقمي.

2. استعمال توقيع رقمي مزور أو منظومة إنشاء توقيع رقمي محرّفة أو شهادة توقيع رقمي مزورة مع علمه بذلك.

هـ. تشدد العقوبة إلى السجن من خمس سنوات إلى سبع سنوات وغرامة سبعة ملايين ليرة سورية إلى عشرة ملايين ليرة سورية إذا ارتُكب تزوير التوقيع الرقمي أو استُعمل التوقيع المزور على وثيقة رسمية صادرة عن إحدى جهات القطاع العام أو المشترك أو المصارف العامة أو الخاصة أو المشتركة.

و. يعاقب بغرامة من خمسة ملايين ليرة سورية إلى سبعة ملايين ليرة سورية، مزود خدمات التصديق الرقمي، إذا أثبت أن إخلال المسؤول عن الإدارة الفعلية للمزود بواجباته قد أسهم في وقوع الجرم المنصوص عليه بالبند رقم /4/ من الفقرة /ج/ من هذه المادة.

ومن المهم الإشارة بأن القانون الجديد وفيما يتعلق بتقانة المعلومات تحديداً قد ألغى الهيئة الوطنية لخدمات الشبكة المحدثة بموجب القانون رقم /4/ لعام 2009 لتحل محلها (الهيئة الوطنية لخدمات تقانة المعلومات) وذلك تلبيةً للخدمات الجديدة ولأنظمة الدفع الإلكتروني وأساليبها وبدقة (أسلوب التوقيع الإلكتروني)، وذلك دعماً للاستراتيجية الحديثة للخدمات الحكومية ضمن رؤية سورية الجديدة للتحول الرقمي.

الفرع الثاني – حماية أنظمة الدفع الإلكتروني وفق الجهود الدولي:

لم تقف ضرورة حماية أنظمة الدفع الإلكتروني الحدود المحلية والتشريعات الداخلية للدول، وإنما امتدت لتشمل ضرورة تظافر جهود دولية على نطاق ضيق بقصد وضع أطر قانونية تكفل الحماية المطلوبة لأساليب أنظمة الدفع الإلكتروني.

وكان أحدث هذه الجهود المرشد العام الذي أصدرته الأمم المتحدة حول مكافحة والحد من جرائم الكمبيوتر في يناير 2000[62].

---

[62] International Review of Criminal Policy – United nations "Manual on the Prevention and Control of Computer Related Crime, 2000:
[http://www.ifs.unvivie.ac.at/przg91/ser4334.html].

أولاً – في ظل الاتحاد الأوروبي:

يعود الاهتمام الأوروبي بالحماية التشريعية للمعاملات الإلكترونية إلى المجموعة الاقتصادية الأوروبية (CEE) التي سعت وراء ضرورة حماية الدفع الإلكتروني، ويظهر ذلك جلياً من خلال التوصية 598/87 التي وضعتها اللجنة الأوروبية في 8 ديسمبر 1987 حول القانون الأوروبي للسيرة الحسنة الخاصة بالدفع الإلكتروني، هذه التوصية تدعو كافة المتعاملين للمثول إلى هذا القانون من أجل ترقية الحماية والضمان للمستهلكين[63]، الحماية المتواصلة بين مقدمي الخدمات ومصدري هذا النوع من وسائل الدفع فيما بينها قبل تاريخ 31 ديسمبر، وكذلك تدعو هذه التوصية إلى إلزام المستهلك أو حامل البطاقة على ضرورة الأخذ بالعناية اللازمة لطريقة استعمل بطاقة الدفع الإلكتروني.

كما حرصت التوصية على ضرورة إضفاء الطابع الشخصي والسري للمعطيات أو البيانات المقدمة من طرف المستهلك، وحق الدخول المتساوي إلى كافة خدمات مقدمي الدفع الإلكتروني.

وصدرت كذلك، عن الاتحاد الأوروبي، التوصية رقم 489/97 في عام 1997 والمتعلقة بالمعاملات التي تتم بواسطة وسائل الدفع الإلكتروني، وخاصة تنظيم العلاقة بين مصدر البطاقات والحامل، فتطبق هذه التوصية في مجملها على المعاملات التي تتم بوسائل الدفع الإلكتروني عن بُعد، ومنها:

– انتقال الأموال المتعلقة باستخدام وسائل الدفع الإلكتروني.

---

(63) Recommandation N° 87 / 598/ CEE de la commission européenne du 8 décembre 1987 portant sur un code européen de bonne conduit en matiére de paiement électronique, jol 365, 24 décembre 1987.

– سحب الأموال السائلة بواسطة وسيلة دفع إلكترونية، وسيلة النقود الرقمية، والتي تتم في آلات السحب الآلي للأوراق أو غيرها[64].

كما حرصت هذه التوصية على ضرورة استعمال وسائل الدفع الإلكتروني بالطريقة الصحيحة وفقاً للشروط والمعايير المتفق عليها باستعمال أو إصدار هذه الوسائل، وأخذ كافة الاحتياطات اللازمة لحماية هذه الوسائل.

ثانياً – اتفاقية المجلس الأوروبي الخاصة بالجريمة المعلوماتية[65]:

صدر أول مشروع لهذه الاتفاقية في عام 2000 بعنوان "اتفاقية الجريمة عبر العالم الافتراضي"، ووافقت عليها (43) دولة أوروبية من الأعضاء في المجلس الأوروبي، وقد تم تعميمه للتعرض لموضوع الاتفاقية وطرح الاعتراضات عليها إلى أن تصبح صالحة للإصدار.

وتهدف هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وانسجام التشريعات الوطنية بعضها ببعض والتعزيز من قدرات القضاء، والتشدد في تطبيق القانون، وتقوية وتحسين التعاون الدولي في هذا الإطار، وإرساء المبادئ العامة ذات الصلة بالتعاون الدولي والمساعدة المتبادلة كما نوّهت الاتفاقية إلى الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق.

وقد تضمنت الاتفاقية في موضوعها أقسام مهمة ومفيدة للمجتمع الدولي بموضوع الجريمة عبر الإنترنت، أهم هذه الأقسام[66]:

---

[64] Recommandation 97/489/ CE du 30 juillet 1997, concernatles operations effectuées au moyens d'instruments de paiement électronique, relation entre émetteur et titulaire J.O. 208 du 2 Aout 1997.

[65] Council of Europe convention on Cybercrime, Budapest, 2001.

اتفاقية المجلس الأوروبي الخاصة بالإجرام السيبري، بودابست، 2001/11/23، حررت في بودابست باللغتين الإنجليزية والفرنسية متساويين في الحجية، وذلك في نسخة واحدة تودع في محفوظات مجلس أوروبا.

[66] عمر محمد بن يونس، ترجمة دراسة وتحقيق للاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، بلا دار نشر، 2005، ص410.

بالإضافة إلى المواد /2– 4– 7/ من اتفاقية المجلس الأوروبي الخاصة بالإجرام السيبري، بودابست، 2001.

1. مجموعة الجرائم التي يتعرض لها الإنترنت والحاسوب، ويشار هنا إلى أن مجموعة الجرائم هي نقل موسع عن الجرائم المتحررة في التشريع الأمريكي.

2. مجموعة الإجراءات الجنائية التي يمكن أن تتخذ في مواجهة هذه النوعية من الجرائم.

3. موضوع التعاون الدولي بين الدول الأعضاء الموقعين على الاتفاقية.

ثالثاً – الحماية في ظل منظمة التجارة العالمية (WTO):

أشارت المنظمة العالمية للتجارة في الإعلان الوزاري في الندوة الوزارية للمنظمة في دورة الدوحة عام 2001، أنها أخذت بعين الاعتبار كافة الأعمال التي قام بها المجلس العام والتي يدعمها الكثير من الهياكل والتي تعتبر دعامة للإعلان الوزاري الصادر في عام 1998[67].

حيث توجه اهتمام المنظمة العالمية للتجارة بموضوع التجارة الإلكترونية، حيث أصدرت المنظمة دراسة خاصة حول التجارة الإلكترونية، وتناولت الدراسة مفهوم المعلومات المعالجة بلغة الحاسب، والتنظيم القانوني للعقد الإلكتروني، ومواجهة المشاكل القانونية المرتبطة بالطبيعة الفنية لوسيلة التعاقد كالتوقيع الإلكتروني، وكيفية الاحتفاظ بالرسائل المتبادلة لاستخدامها في عملية الإثبات، وتكوين العقد وزمانه ومكانه، والالتزامات التي تقع على عاتق الأطراف لتحقيق الأمان التقني والقانوني لعملية التبادل[68].

كما تعترف منظمة التجارة العالمية بأهمية توفير والحفاظ على المحيط اللائق للتطوير المستقبلي للتجارة الإلكترونية، وقد تم الإعلان على أنه على الدول الأعضاء الحفاظ على الممارسات الحالية، والتي تترجم بعض فرض التعريفات الجمركية على

---

[67] وافد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة مقدمة لنيل درجة الماجستير في القانون، جامعة مولود معمري، وزر، كلية الحقوق، 2011، ص190.

[68] يونس عرب، التجارة الإلكترونية، مجلة البنوك، الجمعية المهنية للبنوك الأردنية، العدد (8)، المجد (18)، تشرين الأول، 1999، ص21.

التحويلات الإلكترونية إلى الدورة الخامسة[69]، وقد أكدت هذه التوصيات في الإعلان الوزاري الذي تم الاتفاق عليه في 18 ديسمبر عام 2005.

وتعتبر الأعمال المشار إليها بمثابة نتائج لمؤتمر جنيف الذي عقدته المنظمة العالمية للتجارة في عام 1998، حيث تمت مناقشة موضوع التجارة الإلكترونية، وتم الاتفاق على وضع برنامج عمل يراعي الاحتياجات الاقتصادية والفنية للدول النامية، إضافة إلى عدم فرض رسوم جمركية على الرسائل الإلكترونية، وتلخص موقف الدول المتقدمة وخاصة الولايات المتحدة الأمريكية في ضرورة خضوع السلع والخدمات الإلكترونية لمبادئ المنظمة، وتقنين عدم فرض الرسوم الجمركية على الرسائ الإلكترونية ريثما يتم الاتفاق على هذا الإعفاء، أما بالنسبة للدول النامية فقد تمثل في ضرررورة استمرار التفاوض في المووضعات المتعلقة بالتجارة الإلكترونية، وأهمية توفير الدعم المالي والفني لتتمكن هذه الدول من إنشاء بنى تحتية أساسية تؤهلها للمشاركة في التجارة الإلكترونية، وأخيراً العمل على تنفيذ الإعلان الوزاري الخاص بالتجارة الإلكترونية، خاصة فيما يتعلق بعدم فرض رسوم جمركية على الرسائل الإلكترونية إلى حين انعقاد المؤتمر الوزاري الرابع[70].

---

[69] "Nous déclarons que les membres maintiendront leur patrique qui na pas imposer de droit de douane sur les transnissions technologiques…" voir conférence ministérielle de 1'OMC, Doha 2001, déclaration ministérielle, WT/MIN/DEC1,20 novembre 2001, adopté le 14 novembre 2001.

[70] وثيقة المؤتمر الوزاري الثاني للمنظمة العالمية للتجارة، جنيف، 1998:
http://www.moqatel1.com/penshare.behoth/ektesad8/wto/sec.10.doccvt.htm.

الخاتمة:

تناولنا في هذه الدراسة مفهوم الحماية الفنية لأنظمة الدفع الإلكتروني، من حيث دراسة المخاطر التي تهددها، ومن ثمَّ المواجهة الفنية للمخاطر كأسلوب لحماية أنظمة الدفع الإلكتروني، ثم انتقلنا لدراسة الحماية التشريعية من خلال القوانين المقارنة، والجهود الدولية في حماية أنظمة الدفع الإلكتروني، وفيما يأتي النتائج والمقترحات التي توصلنا إليها:

أولاً – النتائج:

1. نجم عن شيوع استخدام أساليب الدفع الإلكتروني في سائر القطاعات الخدمية والاقتصادية ظهور نمط جديد من الجرائم ذو طبيعة بعيدة عن الجرائم التقليدية.

2. تعد المخاطر التي تهدد أنظمة الدفع الإلكتروني مخاطر من طبيعة خاصة، وغير مرئية مصممة خصيصاً لأغراض إجرامية تستهدف أنظمة الدفع الإلكتروني.

3. تتخذ الحماية الفنية لأساليب الدفع الإلكتروني آليات عدة بدءاً بالكلمات والأرقام السرية، وانتهاءً بجدران الحماية النارية.

4. تضمنت الحماية التشريعية لأساليب الدفع الإلكتروني تجريم سائر الممارسات التي تستهدف أنظمة الدفع الإلكتروني.

5. تتمتع النصوص التشريعية في إطار حماية أساليب الدفع الإلكتروني بطبيعة مرنة، قياساً بالنصوص الجزائية التي تواجه الجرائم التقليدية.

6. ثمة العديد من الجهود ذات الطابع الدولي بغية تكريس حماية فعالة وعابرة للحدود لأنظمة الدفع الإلكتروني.

ثانياً – التوصيات:

1. ضرورة وضع برامج توعوية للوقاية من جرائم الإنترنت والمعلوماتية، والعمل على نشر الوعي الأمني المعلوماتي، بين الأفراد والبنوك والمؤسسات، وأجهزة الدولة، لناحية أهمية مكافحة الجرائم المعلوماتية.

2. تحسين تدابير الأمن والوقاية المتعلقة بالحماية، مع مراعاة احترام خصوصية الأفراد، واحترام حقوق الإنسان وحرياته الأساسية.

3. ضرورة تدريب وتأهيل الجهات المعنية بالأمن المعلوماتي، واستقطاب أصحاب الخبرة في المجال المعلوماتي، وعقد دورات تدريبية دورية دائمة للاستفادة من خبراتهم وإرشاداتهم.

4. الحاجة الملحة إلى تعزيز التعاون الإقليمي والدولي، تكاثف الجهود الدولية وتوافق السياسات الجنائية في مواجهة ظاهرة الإجرام المعلوماتي.

5. يتوجب التوسع الطردي في حماية أنظمة الدفع الإلكتروني من الناحيتين الفنية والتشريعية، والحرص على مواكبة التشرعيات للتطورات الفنية المستجدة، لضرورة حمايتها.

6. يتوجب تحقيق التشريعية بين التشريعات الوطنية والجهود الدولية في حماية أنظمة الدفع الإلكتروني.

المراجع:

أولاً – الكتب:

- د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي (دراسة متخصصة في القانون المعلوماتي)، دار الكتب القانونية، 2007.
- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول.
- أمير فرح يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، 2011.
- علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1996.
- حسن طاهر داوود، الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض.
- أ.د. محمد عبد حسين الطائي، د. ينال محمود الكيلاني، إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015.
- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر– أساليب وثغرات–، دار الهدى، الجزائر، 2010.
- طارق إبراهيم الدسوقي عطية، الموسوعة الأمنية – الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، 2015.
- محمد دباس الحميد، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007.

- د. عبود السراج، شرح قانون العقوبات الاقتصادي في التشريع السوري والمقارن، الطبعة الأولى، منشورات جامعة دمشق، 2010م.
- وافد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة لنيل درجة الماجستير في القانون، جامعة مولود معمري، وزر، كلية الحقوق، 2011.
- طارق عبد العال حماد، التجارة الإلكترونية، الأبعاد التكنولوجية والمالية والتسويقية القانونية، الدار الجامعية، ط2، الإسكندرية، 2007.
- د. حسن مصطفى البحري، القانون الدستوري (النظرية العامة)، كلية الحقوق، الجامعة الافتراضية السورية، دمشق، 2009.
- محمود محمد أبو فروة، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة، عمان، الأردن، 2009.
- د. أحمد الشربيي، د. وفائي بغدادي، حماية وتأمين الإنترنت، التحدي القادم وأساليب المواجهة، سلسلة العلوم والتكنولوجيا، الهيئة المصرية العامة للكتاب، القاهرة، 2010.
- د. عبد الفتاح بيومي حجازي، الحماية التقنية والجنائية لنظام الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2004.
- د. ممدوح عبد الحميد عبد المطلب، الجريمة عبر الإنترنت، منظور أمني، بحث مقدم إلى مؤتمر القانون والكمبيوتر (99)، والإنترت.
- نضال سليم برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة، عمان، الأردن، ط1، 2009.
- عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، 2009.

- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني.
- مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001.
- محمد فواز محمد المطالقة، الوجيز في عقود التجارة الإلكترونية، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006.
- مليكاوي مولود، التجارة الإلكترونية، دار هومة للطباعة والنشر والتوزيع، بوزريعة، الجزائر، 2019.
- هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، المنعقد في الفترة من 10 إلى 12 مايو، 2003، المجلد الثاني.
- محمود محمد أبو فردة، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة، عمان، الأردن، 2009.
- أيمن عبد الحفيظ، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دار انهضة العربية، القاهرة، 2003.
- محمد الصيرفي، الإدارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
- حسن طاهر داوود، أمن شبكات المعلومات، معهد الإدارة العامة، السعودية، 2004.

رسائل الماجستير:

- شيماء جودي، تمثلات الأستاذ الجامعي للخصوصية الرقمية، مذكرة مقدمة لنيل شهادة الماستر، جامعة العربي التبسي، تبسة، قسم علوم الإعلام والاتصال، الجزائر، 2021.
- وافد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة مقدمة لنيل درجة الماجستير في القانون، جامعة مولود معمري، وزر، كلية الحقوق، 2011.

الأبحاث والمؤتمرات:

- د. محمد حسام محمود لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان "الجرائم الواقعة في مجال تكنولوجيا المعلومات"، منشورات النهضة العربية، القاهرة، 1993.
- علي محمد الشوابكة، جرائم الشبكة الدولية للإنترنت ووسائل مكافحتها، مؤتمر التطور التقني وفاعلية العملية التدريبية، الإمارات العربية المتحدة، بحث رقم /10/، 1998.
- محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، بعنوان "جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات"، القاهرة، 1993.
- د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان الجرائم الواقعة في مجال تكنولوجيا المعلومات، منشورات دار النهضة العربية، القاهرة، 1993.

- عادل محمود شرف، عبد الله إسماعيل عبد الله، ضمانات الأمن والتأمين في شبكة الإنترنت، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة في الفترة ما بين 1-3 ماي 2003، الطبعة الثالثة، المجلد الثاني، 2004.
- إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون، الكمبيوتر والإنترنت، المنظم من قبل جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة، 2004.

الصحف والمجلات:

- صحيفة الخليج، 2023، توجهات لهجمات التصيد الاحتيالي عبر ملفات بي دي إف 5، 19، أبريل2.
- يونس عرب، التجارة الإلكترونية، مجلة البنوك، الجمعية المهنية للبنوك الأردنية، العدد (8)، المجد (18)، تشرين الأول، 1999.

باللغة الأجنبية:

- Recommandation No 87 / 598/ CEE de la commission européenne du 8 décembre 1987 portant sur un code européen de bonne conduit en matiére de paiement électronique, jol 365, 24 décembre 1987.
- Recommandation 97/489/ CE du 30 juillet 1997, concernatles operations effectuées au moyens d'instruments de paiement électronique, relation entre émetteur et titulaire J.O. 208 du 2 Aout 1997.
- Council of Europe convention on Cybercrime, Budapest, 2001.
- Jeffry F. Rayport, Bernard J. Jauroski, Commerce électrenique, Editiion chenelierem MC Gram- Hill, Montréal- toronto, 2003,.
- Nous déclarons que les membres maintiendront leur patrique qui na pas imposer de droit de douane sur les transnissions technologiques…" voir conférence ministérielle de 1'OMC, Doha 2001, déclaration ministérielle, WT/MIN/DEC1,20 novembre 2001, adopté le 14 novembre 2001.

المواقع الالكترونية:

- أمير حيدر، حماية الدفع الإلكتروني، مقال منشور على الموقع الإلكتروني: www.islamonline.com..2004/11/12 تاريخ النشر
- وثائق مؤتمر الأمن والإثبات في الكمبيوتر، دبي، الإمارات، أكتوبر،2004.
- موقع وزارة العدل العمانية:

http://www.moj.gov.

- وثيقة المؤتمر الوزاري الثاني للمنظمة العالمية للتجارة، جنيف، 1998: http://www.moqatel1.com/penshare.behoth/ektesad8/wto/sec.10.doccvt.htm.

- Brian Carrier. Defining Digital Forensics Examination and analysis Tools. In Digital Research workshop II, 2002, available at: http://www.dfrws.org/dfws2002/papers/papers/Briancarrier.pdf.
- International Review of Criminal Policy – United nations "Manual on the Prevention and Control of Computer Related Crime, 2000: [http://www.ifs.unvivie.ac.at/przg91/ser4334.html].

القوانين:

- قانون رقم /15/ لسنة 2004 بشأن التوقيع الإلكتروني.
- القانون المصري رقم /175/ لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.
- القانون رقم /20/ لعام 2022 الخاص بالجريمة الإلكترونية.
- القانون رقم /7/ لعام 2023، الخاص بالتوقيع الرقمي وخدمات تقانة المعلومات.

الاتفاقيات:

- اتفاقية المجلس الأوروبي الخاصة بالإجرام السيبري، بودابست، 2001/11/23، حررت في بودابست باللغتين الإنجليزية والفرنسية متساويين في الحجية، وذلك في نسخة واحدة تودع في محفوظات مجلس أوروبا.
- عمر محمد بن يونس، ترجمة دراسة وتحقيق للاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، بلا دار نشر، 2005.