الجريمة الإلكترونية في المعاملات المالية من منظور الشريعة الإسلامية [دراسة فقهية قانونية]

خالد حسن سالم جار الله العجمي.

باحث دراسات إسلامية، وزارة الأوقاف والشؤون الاسلامية، الكويت.

البريد الالكتروني: ElJarallh@gmail.com

ملخص البحث

الشريعة الإسلامية قامت على جلب المنافع ودرء المضار والمفاسد، فلذا جاءت أحكما الشرع متوافقة مع هذا الغرض، ومن أهم الأمور التي يقع فيه الضرر المعاملات المالية، خاصة إذا كانت تتم عن طريق الإنترنت والتطبيقات التكنولوجية المعاصرة، ووقوع الجريمة في الفضاء الإلكتروني أمر مشاهد ويحدث بكثرة لعدة أسباب، ويتخذ صورًا عديدة.

ومع التطور التكنولوجي الذي يشهده العالم المعاصر، وفي ظل اعتماد قطاع كبير من الناس على التطبيقات الإلكترونية والمواقع الشبكية في معظم أمور الحياة من معاملات وتعليم واتصالات وقضاء الأمور الحياتية، فقد أصبحت هذه المواقع والشبكات مليئة بمسببات الجريمة الإلكترونية من احتيال ونصب وتزوير واختراقات، فكان لا بد من إفراد هذه الظاهرة بالبحث والدراسة.

وجاء في البحث لبيان معنى الجريمة الإلكترونية وصورها وأحكامها في الفقه الإسلامي، وكذلك بعض صور الجريمة الإلكترونية كالغش – الاحتيال – التزوير – النصب – سرقة الحسابات المالية – اختراق الحسابات والمعلومات واختراق الأسرار وسرقتها والمتاجرة بها.

وكذلك عالج البحث كل هذه المسائل وأحكامها في الفقه الإسلامي، وسبل الحماية الشرعية والقانونية والفنية من هذه الجرائم. وكذلك بيان موقف الفقه من أحكام السرقة الإلكترونية وهل ينطبق عليها ما ينطبق على السرقة الفعلية، ومدى انطباق شروط السرقة التقليدية على سرقة الأموال الإلكترونية، ومدى انطباق شروط

السرقة الحدية على سرقة البيانات الإلكترونية، وانتهى إلى أن السرقة الإلكترونية للأموال تطابق السرقة الموجبة لإقامة الحد على السارق.

وبين البحث القوانين التي تسنها معظم الدول الجهود الكافية للحماية من الجريمة الإلكترونية عبر سن القوانين.

وذكر البحث ضرورة أخذ الحيطة والحذر والحماية من الاختراقات، سواء حماية تقنية أو حماية قانونية أو حماية تثقيفية، مع إيضاح حكم الفقه الإسلامي في تحريم وتجريم كل أنواع الغش والسرقة والجريمة الإلكترونية.

وفي النهاية مجموعة من النتائج والتوصيات.

الكلمات الدلالية: الجريمة ، الإلكترونية ، الفقه ، المعاملات المالية ، القانون.

Cybercrime in Financial Transactions From the Perspective of Islamic Sharia [Legal Jurisprudential Study]

==========

Khaled Hassan Salem Jarallah Al-Ajmi.

Researcher of Islamic Studies, Ministry of Endowments and Islamic Affairs,

Email: ElJarallh@gmail.com

Abstract:

Islamic law is based on bringing benefits and warding off harms and corruptions, so the provisions of Sharia are compatible with this purpose. Among the most important matters in which harm occurs are: financial transactions, especially if they are carried out via the Internet and contemporary technological applications. The occurrence of crime in cyberspace is a visible matter and occurs frequently for several reasons, and takes many forms. With the technological development witnessed by the contemporary world, and in light of the reliance of a large segment of people on electronic applications and websites in most aspects of life from transactions, education, communications and spending life matters, these sites and networks have become full of causes of electronic crime from fraud, swindling, forgery and hacking, so it was necessary to single out this phenomenon for research and study .

The research came to clarify the meaning of electronic crime, its forms, and its provisions in Islamic jurisprudence, as well as some forms of electronic crime, such as: fraud, deception, forgery, fraud, theft of financial accounts, hacking accounts and information, hacking secrets, stealing them and trading in them .

The research also addressed all these issues and their provisions in Islamic jurisprudence. And the legitimate, legal and technical means of protection from these crimes. It also clarified the position of jurisprudence on the provisions of electronic theft and whether what applies to actual theft applies to it, and the

extent to which the conditions of traditional theft apply to the theft of electronic money, and the extent to which the conditions of theft of the limit apply to the theft of electronic data, and concluded that the electronic theft of money is identical to theft that requires the imposition of the limit on the thief.

The research clarified the laws enacted by most countries, and the sufficient efforts to protect against electronic crime through the enactment of laws.

The research mentioned the necessity of taking precautions and protection from breaches, whether technical protection, legal protection or educational protection, while clarifying the ruling of Islamic jurisprudence in prohibiting and criminalizing all types of fraud, theft and electronic crime

Finally, a set of results and recommendations.

Keywords: Crime , Electronic , Jurisprudence , Financial transactions , Law. Financial transactions – Law.

بسم الله الرحمن الرحيم

المقدمة

الحمد لله رب العالمين والصلاة والسلام على الرحمة المهداة والنعمة المسداة محمد بن عبد الله، وعلى آله وصحبه ومن والاه، أما بعد:

فبالرغم من التطور الهائل الذي شهده قطاع التكنولوجيا المالية، وما نتج عنه من آثار إيجابية، من خلال تطبيق أحدث وسائل التكنولوجيا الحديثة، سواء أكان في وسائل المعاملات والتطبيق، أم في استحداث العديد من المعاملات الحديثة، إلا أنه بالرغم من ذلك كله نتج عن تطبيق تقنية التكنولوجيا المالية بعض المشكلات، والتي تمثلت في ظهور الجريمة الإلكترونية.

وتُعرَّف الجريمة الإلكترونية بأنها: نشاط غير مشروع موجه لنسخ، أو تغيير، أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تُحوَّل عن طريقه(١).

والتي تُعرَّف -أيضًا- بأنها: المخالفات التي تُرتكَب ضد الأفراد أو المجموعات من الأفراد بدافع: الجريمة، وبقصد إيذاء سمعة الضحية، أو أذى ماديٍّ أو عقلي للضحية، مباشر أو غير مباشر باستخدام الاتصال مثل الإنترنت(٢).

وقد عَرَّفت منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة - الجريمة الإلكترونية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال

---

(١) ينظر: جرائم الحاسوب وأبعادها الدولية، محمود أحمد، دار الثقافة، عمان ٢٠٠٥م، (ص: ١٦).

(٢) ينظر: الجرائم الإلكترونية المفهوم والأسباب، ذياب موسى، مؤتمر الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، بكلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية، ٢٠١٤م، (ص: ٣).

المادية أو المعنوية، يكون ناتجًا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية(١).

سنتعرف من خلال البحث على صور الجريمة الإلكترونية وسبل الحماية منها في الفقه والقانون.

(١) ينظر: جرائم الحاسوب وأبعادها الدولية، د. محمد أحمد عبابنة، دار الثقافة، عمان، ط١، ٢٠٠٥م، (ص: ١٧)..

أهمية الموضوع وأسباب اختياره

تظهر أهمية الموضوع وأسباب اختياره من عدّة وجوه، يمكن إجمالها في النقاط الآتية:

(١)- أهمية التعرف على صور الجريمة الإلكترونية وبيان صورها.

(٢)- حاجة الناس الملحة للتعامل اليومي على شبكة الإنترنت يجعل الجريمة تجد لها مكانا في هذا العالم فكان لا بد من بيان صورة واشكاله.

(٣)- بيان مرونة الفقه الإسلامي وصلاحيته لكل زمان ومكان.

(٤)- رفع الضرر عن الناس ببيان تحريم وتجريم الفقه الإسلامي لكل صور الجرائم الإلكترونية، وبيان أن حفظ وصيانة المال والعرض مقصد عظيم من المقاصد الخمس في الشريعة الإسلامية.

أهداف البحث

يحقق هذا الموضوع -بإذن الله- عددًا من الأهداف، وهي:

(١)- بيان مخاطر الجريمة الإلكترونية.

(٢)- بيان صور الجريمة الإلكترونية.

(٣)- التوصل إلى حكم الفقه الإسلامي في كافة صور الجرائم الإلكترونية.

إشكالية البحث

• ضرورة التعامل عبر الإنترنت كثرت في الآونة الأخيرة، وأصبحت الحاجة إليه ضرورية لا تحسينية، ووجود بعض الناس ممن لا يحسنون التعامل عبر الإنترنت في المعاملات والأمور الخاصة بهم شجع صحاب النفوس المريضة لاستغلالهم عبر سرقة بياناتهم ومعلوماتهم وحساباتهم وأموالهم، فكان لا بد من بيان معنى الجريمة الإلكترونية وصورها وأشكالها وحكمها في الفقه الإسلامي وتحذير الناس منها، بما ينفي الضرر ويرفع الحرج.

حدود البحث

تتمثل حدود البحث في المحاور التالية:

الحد الأول: الجريمة الإلكترونية: فالبحث لا يتعرض لغير الجريمة الإلكترونية، وليس غيرها من الأمور التي تتم عبر الإنترنت.

الحد الثاني: المعاملات المالية: فالبحث يتعرض لأحكام الجريمة الخاصة بالمعاملات المالية فقط.

الحد الثاني: الفقه الإسلامي: فالبحث يتعرض للجريمة الإلكترونية من ناحية بيان حكمها وصورها في الفقه الإسلامي وتجريمها قانونا وبيان طرق الحماية.

الدراسات السابقة

وجدت أبحاث ومقالات ورسائل تعرضت لأحكام الجريمة الإلكترونية في الفقه الإسلامي، ومن أهمها:

(١)- الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: دراسة مقارنة - إبراهيم محمد الزنداني - رسالة ماجستير – جامعة فطاني بتايلاند – ٢٠١٨م.

(٢)- الجريمة الإلكترونية وسبل المواجهة في الشريعة الإسلامية – د. إبراهيم عطايا - مجلة كلية الشريعة والقانون بطنطا – ٢٠١٥ م. عدد ٣٠ – جزء ٢.

والملاحظ أن البحوث والدراسات السابقة تدرجت إلى أحكام متعلقة بالجريمة الإلكترونية من ناحية القانون الوضعي ودراسات مقارنة، أو من ناحية سبل المواجهة الشرعية فقط، أو من ناحية أحكام الجريمة بصفة عامة في كل المجالات الإلكترونية.

ولكن دراستنا هذه انصبت على إفراد البحث وقصره على الجريمة

الإلكترونية في المعاملات المالية من منظور الفقه الإسلامي، وإيراد بعض قوانين المكافحة لهذه الجريمة في القانون الحديث، كما في الدراسات السابقة.

خطة البحث

اقتضت طبيعة البحث أن يكون تقسيمه إجمالًا: مقدمة، ومبحثين، وخاتمة، وفهارس.

المقدمة.

- أهمية الموضوع.
- أهداف البحث.
- إشكالية البحث
- حدود البحث.
- الدراسات السابقة.
- خطة البحث.

❖ المبحث الأول: مخاطر الغش والاحتيال.

❖ المطلب الأول: مفهوم الغش والاحتيال، وحكمه في الشريعة الإسلامية.

❖ المطلب الثاني: صور الغش والاحتيال الإلكتروني في المعاملات المالية.

❖ المطلب الثالث: المسائل الشرعية في الغش الإلكتروني.

❖ المبحث الثاني: خطر الاختراقات الإلكترونية.

❖ المطلب الأول: مفهوم الاختراقات الإلكترونية.

❖ المطلب الثاني: وسائل، ونماذج الاختراقات الإلكترونية.

❖ المطلب الثالث: تجريم الاختراقات الإلكترونية.

❖ الخاتمة.

❖ وفيها:

❖ النتائج.

❖ التوصيات.

❖ فهرس الموضوعات.

□

المبحث الأول

مخاطر الغش والاحتيال

المطلب الأول

مفهوم الغش والاحتيال، وحكمه في الشريعة الإسلامية

الغش هو إظهار الشيء على غير ما هو عليه في الواقع؛ وذلك بكتمان العيب وإخفائه، فالغش خيانة وخداع[(١)]. والغش حرام بإجماع المسلمين، وفاعله مذموم عقلًا وشرعًا، وقد ثبت تحريم الغش بالكتاب، والسنة والإجماع:

أما الكتاب فبعموم الآيات التي تنهى عن أكل أموال الناس بالباطل ومنه قوله تعالى: ﴿وَلا تَأْكُلوا أَموالَكُم بَينَكُم بِالباطِلِ﴾ [سورة البقرة: ١٨٨].

أما السنة فقد جاءت أحاديث كثيرة تدل على تحريم الغش، ومنها قوله ﷺ: "من غشّ فليس مني"[(٢)]. وأما الإجماع فقد أجمعت الأمة على تحريم الغش[(٣)].

والغش الإلكتروني في المعاملات المالية لا يخرج عن التصور العام للغش، وجريمة الغش التجاري تكاد تكون السمة الغالبة على معاملات التجارة الإلكترونية، ويقع في وسيلة الربط بين المستهلك وبين السلعة أو الخدمة، وهذه الوسيلة هي الدعاية، فالمنتج عادة ما يعتمد على الدعاية التسويقية، وهذه الدعاية تكون غير مطابقة لمواصفات السلعة أو الخدمة الحقيقية، وعادة ما تحتوي على مغالطات تضلل المستهلك مما يجعله عرضة للتلاعب.

---

(١) ينظر: مواهب الجليل للحطاب، شمس الدين أبو عبد الله محمد بن محمد بن عبد الرحمن الطرابلسي المغربي، المعروف بالحطاب الرُّعيني المالكي، (٤٣٧/٤)، ونهاية المحتاج، للرملي (٢/٣)، والمغني لابن قدامة، (١٠٨/٤).

(٢) تقدَّمَ تخريجه.

(٣) ينظر: المنهاج شرح صحيح مسلم بن الحجاج للنووي، (٤٦٧/٢)، مرجع سابق.

والغش التجاري في التجارة الإلكترونية متعددة، لدرجة أنه لا يمكن عدها أو الإلمام بها على وجه التحديد؛ لكونها تتسم بذات الصفات التي تتسم بها التجارة الإلكترونية.

ويعرف الغش التجاري الإلكتروني بأنه: "كل فعل أو ممارسة غير أخلاقية تستخدم فيها التقنيات الإلكترونية، وتهدف إلى تحقيق كسب مادي غير مشروع"(١).

كما عُرِّف -أيضًا-، بأنه: "الجرم الذي يقع من خلال استخدام أجهزة الحاسب الآلي، حيث إن العملية الإلكترونية التي يتم من خلالها عملية البيع والشراء يعتريها في كثير من الأحيان الغش، من خلال المعلومات المقدمة من الإعلانات، خصوصًا مع ظهور الشركات وهمية تعمل على عرض السلع بقصد الغش والاحتيال، فما أن تقبض الثمن حتى لا تكاد تجدها في صفحات الانترنت، أو استغلال عدم قدرة المتعاقد على التمييز كأن يكون الشخص له ميل لسلعة معينة كسيارة من نوع معين، فيتم تزويده بمواصفات أخرى لا يكون المشتري مدركا لها"(٢).

وتُعرِّف منظمة التعاون الاقتصادي والتنمية(٣) الغش الالكتروني بأنه: "كل

---

(١) الغش التجاري الإلكتروني، عبد الإله بن أحمد عبد المالك بن علي، أطروحة دكتوراه د. ط. كلية العدالة الجنائية المملكة العربية السعودية جامعة نايف العربية للعلوم الأمنية، ٢٠١٤، (ص: ٢٧).

(٢) عقوبات الغش التجاري في بيئة التعاملات الإلكترونية ودورها في حماية حقوق المستهلك، مسفر بن حسن مسفر القحطاني، المجلة العربية للدراسات الأمنية، العدد ٧٠، المجلد ٣٣، ٢٠١٧م، (ص: ١٣٣-١٦٤).

(٣) ينظر: منظمة التعاون الاقتصادي والتنمية منظمة التعاون الاقتصادي والتنمية هي منظمة اقتصادية حكومية دولية تضم ٣٨ دولة عضو، تأسست في عام ١٩٦١م؛ لتحفيز التقدم

=

سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها"[١].

والغش التجاري في التعاملات الإلكترونية لا يمكن أن يتحقق إلا في حالة خداع أحد طرفي التعامل الإلكتروني للآخر؛ وعليه يمكن تعريف الغش التجاري في التعاملات الإلكترونية بأنه: "وصف أو عرض أو تسويق منتج أو خدمة بما يخالف الحقيقة؛ بمعلومات كاذبة أو خادعة أو مضللة من أجل تبادل أو تعاقد، أو أي إجراء آخر يبرم أو ينفذ -بشكل كلي أو جزئي- بأي وسيلة إلكترونية"[٢].

حيث يقوم مرتكب الغش التجاري في البيئة الإلكترونية بعرض منتجات تم تقليدها بصورة تشبه إلى حد كبير المنتجات الأصلية، مع استخدام مجموعة من الوسائل التي توقع المستهلك الإلكتروني في الوهم بأنها أصلية، كما يمكن أن يقوم مرتكب الغش التجاري الإلكتروني بإعلان كاذب عن سلع معينة أو إعلان مضلل يخدع المستهلك، وهناك العديد من الأساليب والصور للغش التجاري الإلكترونية.

إن الغش التجاري الإلكتروني يشكل نوعًا خاصًا من الغش التجاري، الذي يرتبط بالمجتمع الإلكتروني، إلا إنه يتميز عن الغش التجاري التقليدي في أنه قد يرتكب باستخدام وسائل التقنية الحديثة.

ويمكن القول بأن تحديد أشكال الغش التجاري المحتملة في التقنيات

الاقتصادي والتجارة العالمية، ومقرها في باريس بفرنسا.

(١) الآليات الجنائية لمكافحة الغش التجاري الإلكتروني في التشريع الجزائري، فاطمة ضيف الله، مجلة آفاق للعلوم، المجلد٦، العدد٤، ٢٠٢١م، (ص: ٤٤٠).

(٢) عقوبات الغش التجاري في بيئة التعاملات الإلكترونية ودورها في حماية حقوق المستهلك، مسفر بن حسن بن مسفر القحطاني، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد٣٣، العدد ٧٠، ٢٠١٧م، (ص: ١٤٠).

الإلكترونية يعد مهمة في غاية الصعوبة، ويمكن تحديد الأسباب الرئيسية وراء صعوبة إثبات الغش التجاري الإلكتروني أنه لا يترك أثرًا بعد ارتكابه، وصعوبة الاحتفاظ الفني بآثاره إن وجدت، وأنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها، وأنه يعتمد على قمة الذكاء في ارتكابه[١].

(١) ينظر: فكرة الحماية الجنائية لبرامج الحاسب الآلي، د. محمد محمد شتاء، دار الجامعة الجديدة للنشر، الإسكندرية ٢٠٠١م، (ص: ٤٢).

المطلب الثاني

صور الغش والاحتيال الإلكتروني في المعاملات المالية

أولًا: الغش في المعاملات تتعدد صوره بتعدد المعاملات وتطورها، فقد عرف الغش أولًا في البيع، ومن أكثرها شيوعًا الكذب، وهو ضد الصدق، وقد حذر الإسلام من الكذب في البيع، وأمر بالصدق فيهما، فيقول: {يَا أَيُّهَا الَّذِينَ آمَنُوا اتَّقُوا اللَّهَ وَكونوا مَعَ الصّادِقِينَ} [سورة التوبة: ١١٩].

ويقول ﷺ: «البَيِّعانِ بِالخِيارِ ما لَمْ يَتَفَرَّقا، فَإِنْ صَدَقا وَبَينا بُورِكَ لَهُما فِي بَيْعِهِما، وَإِنْ كَذَبا وَكَتَما مُحِقَتْ بَرَكَةُ بَيْعِهِما»(١).

وقال ﷺ: «التَّاجِرُ الصَّدُوقُ الْأَمِينُ مَعَ النَّبِيِّينَ وَالصِّدِّيقِينَ وَالشُّهَدَاءِ»(٢).

ومن صور الغش في البيع: كتمان العيب، وعدم إظهاره، فلا يحل لمن يبيع سلعة أن يكتم ما بها من عيوب للنهي عن ذلك، فقد جاء عن النبي ﷺ أنه قال: «المُسلِمُ أخو المسلِمِ، لا يحلُّ لِمُسلِمٍ باعَ مِن أخيهِ بيعًا وفيهِ عيبٌ؛ إلَّا بيَّنَهُ»(٣).

---

(١) متفق عليه: رواه البخاري في صحيحه، (٥٨/٣)، كتاب: البيوع، باب: إذا بيَّن البيعان ولم يكتما ونصحا، رقم الحديث: (٢٠٧٩)، وفي صحيح مسلم، (١١٦٤/٣)، كتاب: البيوع، باب: الصدق في البيع والبيان، رقم الحديث: (١٥٣٢).

(٢) رواه الترمذي في سننه، (٣/ ٥١٥)، كتاب: البيوع عن رسول الله -صلى الله عليه وسلم-، باب: ما جاء في التجار، وتسمية النبي -صلى الله عليه وسلم- إياهم، حديث رقم: (١٢٠٩)، وقال: "حديث حسن"، وفي الزوائد: "إسناده صحيح، ورجاله ثقات"، وقال المنذري في الترغيب والترهيب: "إسناده صحيح" (٣٨/٣).

(٣) رواه ابن ماجه في سننه، (٧٥٥/٢)، كتاب: التجارات، باب: من باع عيبًا فليبينه، رقم الحديث: (٢٢٤٦)، والحاكم في المستدرك، (١٠/٢)، كتاب: البيوع، وأما حيث: بن أبي ثابت، رقم الحديث: (٢١٥٢)، من حديث عقبة بن عامر الجهني I، وقال: "هذا حديث صحيح على شرط الشيخين ولم يخرجاه"، ورواه البيهقي في الكبرى، (١٨٧/١١)،

=

وفي هذا الجانب لا يقتصر إظهار ما بالبيع من عيوب عن صاحبه فقط، بل يجب على كل مَن يعلم ذلك أن يبينه، وقد رُوِيَ في ذلك عن النبي ﷺ أنه قال: "لا يحل لأحد أن يبيع شيئًا إلا بين ما فيه، ولا يحل لأحد يعلم ذلك إلا بينه"(١).

ومن صور الغش في البيع ما يكون من: خداع المتعاملين، والتدليس عليهم، فهو مِن أكل أموال الناس بالباطل، ويدخل في الغش نقصان الكيل، والميزان، وعدم بخسهما؛ لما يترتب عليه من ظلم وأضرار للمتعاملين، وقد حذر الإسلام من ذلك، وأمر بالوفاء بالكيل والميزان بالعدل، فقال: ﴿وَأَوفُوا الكَيلَ وَالميزانَ بِالقِسطِ﴾ [سورة الأنعام: ١٥٢].

ثانيًا: الغش في المعاملات الإلكترونية فله -أيضًا- صور متعددة، وهذه الصور تتكرر وتختلف من بيئة لأخرى، ومن وقت لآخر، ونشير فقط إلى أهم هذه الصور، ومنها:

أ.الغش في منتج أصلي بمنتج مقلد:

حيث يتم عرض منتجات مقلدة وتشبه الأصلية إلى حد كبير مع إيهام المستهلك بأنها ذات السلعة بثمن أقل كعرض خاص من الموقع، وتحمل هذه الجريمة بعدا آخر، وهي جريمة التعدي على حقوق الملكية الفكرية لهذا المنتج، كما تستخدم المرأة في الترويج لهذه السلع؛ مما يغري الزبون بالشراء، ثم يتبين بعد استعمالها عيوبها، وفي الغالب لا يستطيع إرجاعها؛ لبعده عن مكان الشركة، حيث قد يكون في دولة أخرى، أو لاختفاء مندوبها ومسح أرقام هواتفها أو

كتاب: البيوع، باب: ما جاء في التدليس وكتمان العيب في المبيع، حديث رقم: (١٠٨٣٦)، وصححه الألباني في صحيح الترغيب والترهيب، (٣٣٨/٢)، وقال: " وهو عند البخاري موقوف على عقبة لم يرفعه"، كتاب: البيوع وغيرها، برقم: (١٧٧٥).

(١) تقدّم تخريجه، (الصفحة السابقة)، وينظر: نيل الأوطار، للشوكاني، (٣٦٩/٦).

تعطيلها[١].

ب. الترويج لسلع غير موجودة أصلًا:

وفي هذه الحالة يقوم المنتج للسلعة غير المشهورة بالإعلان لها بإعلان كاذب، والكذب هو: "الإخبار عن شيء بخلاف ما هو عليه في الواقع"[٢]، وهو يقوم على عنصرين:

الأول: مضمون زائف.

الثاني: قصد تزييف الحقيقة.

أما الإعلان المضلل فهو الذي يكون من شأنه خداع المستهلك، فهو لا يذكر بيانات كاذبة، بل يصاغ في عبارات تؤدي إلى خداع المستهلك المتلقي[٣].

وهذا الأسلوب يعرف -أيضًا- بالغش في المزادات الإلكترونية، حيث يرتكز سوق المزاد عبر الإنترنت على الصورة، وتوصيف البضاعة من خلال نص مقتضب في الغالب؛ ونظرًا لصعوبة تفحصها عن قرب لا يبق أمام المشتري سوى الثقة بعارضها، وحسب تقرير الاتحاد الفيدرالي للتجارة والمراقبة، فإن جرائم الاحتيال التي تحدث في المزادات على الإنترنت تعتبر من أكثر جرائم الإنترنت شيوعًا وانتشارًا [٤].

---

(١) ينظر: الحماية الجنائية للمستهلك، حسني أحمد الجندي، الكتاب الأول – قانون منع التدليس والغش-، دار النهضة العربية، القاهرة، ١٩٨٦م، (ص: ٥١-٥٣).

(٢) ينظر: فتح الباري لابن حجر، (٢٠١/١)، مرجع سابق.

(٣) ينظر: التجارة الإلكترونية هبه مصطفى كافي، تقديم ومراجعة مصطفى يوسف كافي، ألفا للوثائق، الجزائر، الطبعة الأولى، ٢٠١٧م، (ص: ٢٥٢-٢٥٣).

(٤) ينظر: الغش التجاري في المجتمع الإلكتروني مركز البحوث والدراسات، ورقة عمل مقدمة للندوة الرابعة لمكافحة الغش التجاري في دول مجلس التعاون الخليجي، خلال

=

ت. الغش والخداع عن طريق الموقع الوهمي:

ما يقوم به بعض اللصوص من وضع موقع وهمي قريب من الموقع الأصلي؛ لاستغلال السقطات الكتابية التي قد يخطئ بها من يريد الدخول على الموقع الحقيقي؛ فيضعون أرقامهم السرية وهم يظنون أنهم يتعاملون مع الموقع الرسمي فعلى سبيل المثال:

بدلا من كتابة **www. Siab. com. sa**. فإن هؤلاء المتربصين يقومون بتهيئة موقع مشابه تمامًا بموقع البنك عندما يقوم العميل بكتابة **www. Saib. com. sa** ويعتمدون على هؤلاء العملاء الذين يخطئون أثناء كتابة (**Siab**) بدلًا من (**Saib**)، وذلك كما في المثال المذكور بتقديم حرف على آخر بمنتصف الكلمة؛ فقدّموا حرف الـ(**a**) على الـ(**i**) إيهامًا للعميل، ليُصبح بعدها من عميل للبنك إلى مجني عليه من المحتالين الإلكترونيين؛ لذا فأكثر البنوك والشركات المالية توقفت عن إرسال روابط للعملاء لتجديد بيانتهم، وينصح بعدم اتباع الروابط، وإنما كتابة الموقع من جديد، أو استخدام المفضلة الشخصية(١).

ث. الاحتيال في التحصيل:

قد تتجه مؤسسات الأعمال إلى تنفيذ أنشطة المشتريات والتحصيل إلكترونيًا، فقد انتشرت خلال الفترة الأخيرة توجهات الشركات لإتمام عملية التحصيل وتوثيقها إلكترونيا؛ الأمر الذي يؤدي إلى مستويات أعلى من المرونة والثقة والتعاون الذي ينشأ بين أطراف عملية التحصيل وتنتاب عملية التحصيل الإلكتروني بعض مخاطر الاحتيال نتيجة عدم وجود الرقابة الداخلية عندما يتم

الفترة ٢١-٢٠ سبتمبر عام ٢٠٠٥م، ١٤٢٦ه، (ص: ١٨).

(١) ينظر: التعدي في المعاملات المالية الإلكترونية بين الفقه الإسلامي والقانون الأردني، سامي نجيب رشيد كلية الدراسات العليا، الجامعة الأردنية عمان، ٢٠١٠م، (ص: ٥٧).

تنفيذ أنظمة التحصيل الإلكتروني الجديدة[١].

ج. الغش في بطاقات الائتمان:

إن بطاقات الائتمان هي البطاقات التي ينحصر دورها في كونها أداة للوفاء بثمن السلع والخدمات التي يحصل عليها حاملها من بعض التجار المقبولين من الجهة التي أصدرت هذه البطاقة، و-أيضًا- هي عقد يتعهد بموجبه مصدر البطاقة بفتح اعتماد بمبلغ معين لمصلحة شخص معين، وهو حامل البطاقة؛ لكي يستطيع شراء ما يريد والوفاء بذلك.

فمثلًا سرقة المال عبر الإنترنت باستخدام أرقام لبطاقات مصرفية تعود للغير، أو الحض على الفجور وممارسة الفاحشة مع قاصر عبر الإنترنت، أو الإرشادات التي تحمل في طياتها تعليمات إرهابية كلها موجهة ضد أشخاص أو جهات بعينها[٢].

ومنها -أيضًا-: الطلبات الاحتيالية. أي: تقديم طلبات وهمية للحصول على بطاقة باستخدام معلومات شخصية زائفة، أو بطاقات هوية مسروقة أو مزورة. هذا النوع من أسلوب التجسس **Spying** حيث يقوم قراصنة الكمبيوتر باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالشركات والمؤسسات التجارية العاملة على شبكة الإنترنت؛ وبالتالي يتمكنون من الحصول على ما يريدون من المعلومات، ومنها المتعلقة ببطاقات الوفاء التي استخدمت في التجارة الإلكترونية عبر الشبكة.

---

(١) ينظر: جرائم الحاسوب وأبعادها الدولية، محمد أحمد عبابنة، ومحمد معمر الرازقي، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٥م، (ص: ١٣٢).

(٢) ينظر: بروتوكولات وقوانين الإنترنت، منير محمد الجنيهي، وممدوح محمد الجنيهي، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٥م، (ص: ٧٦-٧٧).

وقد انتشرت مؤخرًا استقبال الأجهزة الخلوية الخاصة بالعديد من العملاء الرسائل قصيرة، sms محتواها أن صاحب الرقم قد فاز بمبلغ خيالي من خلال عبارات مختلفة للإيقاع بالضحايا، وحيث إن الشركات الخلوية المختلفة لم تقم بإجراء مثل هذه المسابقات، وتعتبر أسلوبًا احتياليًا جديدًا من خلال سرقة معلومات الأشخاص الذين يقومون بالاتصال بالأرقام والعناوين المبينة في الرسائل القصيرة لغايات استخدامها في عمليات احتيالية إلكترونية.

وعلى الرغم من اتخاذ العديد من الاحتياطات لحماية المستهلك من التصرفات الاحتيالية على شبكة الإنترنت، فإنه لا يزال هناك تزايد مستمر في أعداد الشكاوى التي تصدر من المستهلكين الذين يتعرضون لأفعال احتيالية على الإنترنت، وتزداد خطورة هذا الأمر بمعرفة مدى التنوع الكبير في أشكال وصور هذا الاحتيال، حيث ظهرت أشكال جديدة للاحتيال لم تكن موجودة، مثل: احتيال الشيكات، واحتيال الاستثمار، والزيادة في نسب الشكاوى المرتبطة باحتيال بطاقات الائتمان [١].

□

(١) ينظر: عالمية التجارة الإلكترونية وعقودها وأساليب مكافحة الغش التجاري الإلكتروني، أمير فرج يوسف، المكتب الجامعي الحديث، ٢٠٠٩م، (ص: ٣٤٣).

المطلب الثالث

المسائل الشرعية في الغش الإلكتروني

الغش حرام بإجماع المسلمين -كما بينا في الحكم الشرعي-، وفاعله مذموم عقلًا وشرعًا، وقد ثبت تحريم الغش بالكتاب، والسنة والإجماع، وتواترت الأدلة على ذلك، ومنها: ما روي عن أبي هريرة -رضي الله عنه- أن رسول الله ﷺ: "مر على صبرة طعام، فأدخل يده فيها، فأصابت أصابعه بللًا، فقال: "ما هذا يا صاحب الطعام؟" قال: أصابته السماء يا رسول الله، قال: "أفلا جعلته فوق الطعام كي يراه الناس؟ من غش فليس مني"[(١)].

ولأجل منع الغش، وقطع أسبابه حرم الإسلام على المسلمين، النجش وتلقي الركبان، وتصرية بهيمة الأنعام، وثبت النهي عنه في أحاديث في الصحيحين[(٢)] وفي غيرهما، وأجمع العلماء[(٣)] على تحريم النجش، وإنما حرم لما فيه من الغش والخداع.

قال ابن الجلاب: "ولا يجوز النجش في البيوع، ولا ينبغي أن يقر الغش في

---

(١) تقدّم تخريجه صفحة: (٢٤٦).

(٢) عن أبي هريرة -رضي الله عنه- قال: «نَهَى رَسُولُ اللهِ ﷺ عَنِ التَّلَقِّي، وَأَنْ يَبْتَاعَ الْمُهَاجِرُ لِلْأَعْرَابِيِّ، وَأَنْ تَشْتَرِطَ الْمَرْأَةُ طَلَاقَ أُخْتِهَا، وَأَنْ يَسْتَامَ الرَّجُلُ عَلَى سَوْمِ أَخِيهِ، وَنَهَى عَنِ النَّجْشِ، وَعَنِ التَّصْرِيَةِ»، رواه البخاري، (١٩٢/٣)، كتاب: الشروط، باب: الشروط في الطلاق، حديث رقم: (٢٧٢٧)، ومسلم، (٤/٥)، كتاب: البيوع، باب: تحريم بيع الرجل على بيع أخيه، وسومه على سومه، حديث رقم: (١٢)، مراجع سابقة.

(٣) نقل الإجماع ابن بطّال في شرح للبخاري، قال: "وأجمع العلماء أن الناجش عاصٍ بفعله"، ينظر: شرح صحيح البخاري، (٢٧٠/٦)، كتاب: البيوع، باب: النجش ومَن يقول لا يجوز ذلك البيع، تأليف: علي بن خلف بن عبد الملك بن بطال، تحقيق: أبو تميم ياسر بن إبراهيم، مكتبة الرشد، الرياض – السعودية، الطبعة: الثانية، ١٤٢٣ه – ٢٠٠٣م.

شيء من أسواق المسلمين بوجه من الوجوه، ولا يسمح فيه لأحد"[١].

وقال ابن عبد البر: النجش: "مكر وخداع، لا يجوز عند أحد من أهل العلم؛ لنهي الرسول ﷺ عن النجش، وقوله ﷺ: «لَا تَنَاجَشُوا» وأجمعوا أن فاعله عاصٍ لله إذا كان بالنهي عالمًا"[٢].

فالغش والاحتيال منهي عنه بجميع صوره وأشكاله: الواقعي منه، والإلكتروني؛ إذ هو من قبيل الضرر التي نهت عنه الشريعة الإسلامية، فالغش أو الاحتيال على حقوق الآخرين، بغير وجه مشروع في التجارة الإلكترونية، وكذلك أساليب الحيل والخداع، والاعتداء على الأموال بغير وجه حق مشروع - كل هذا يتنافى مع الشريعة الإسلامية[٣].

ومن واجبات التجارة الإلكترونية في الشريعة الإسلامية ترك الشبهات والإعلانات الكاذبة، والالتزام بالصدق، بالإضافة إلى التحلي بمعالي الأخلاق، وقد تجلت صور حماية الشريعة للمعاملات الإلكترونية بما نصت عليه اللجنة الدائمة للبحوث العلمية، والإفتاء في المملكة العربية السعودية في فتواها رقم (١٨٤٥٣) في ١٤١٧/١/٢هـ التي بينت فيها عدم جواز نسخ البرامج الحاسوبية التي يمنع أصحابها نسخها إلا بإذنهم لقوله ﷺ: "المسلِمون على شُروطِهم"[٤]؛

---

(١) التفريع في فقه الإمام مالك بن أنس، عبيد الله بن الحسين بن الحسن أبو القاسم ابن الجَلَّاب المالكي (ت٣٧٨هـ)، دار الكتب العلمية، بيروت – لبنان، الطبعة الأولى، ١٤٢٨هـ - ٢٠٠٧م، (١٦٧/٢).

(٢) التمهيد، لابن عبد البر (٩٤/٥).

(٣) ينظر: العلامة التجارية وحق استغلالها، وحي لقمان، صحيفة الوطن السعودية، العدد (٨٨٦)، ١ محرم ١٤٢٤هـ، (ص: ٢٤).

(٤) رواه الترمذي في سننه، (٦٣٤/٣-٦٣٥)، كتاب: الأحكام، باب: ما ذكر عن رسول الله في الصلح بين الناس، حديث رقم: (١٣٥٢)، وقال الترمذي: "حديث حسن صحيح"، =

ولقوله ﷺ: «لا يَحِلُّ مالُ امْرِئٍ إلّا بِطيبِ نَفسِهِ»[١].

وقوله ﷺ: «مَنْ سبق إلى ما لم يَسْبقْه إليه مسلمٌ فهو له»[٢]، سواء أكان صاحب هذا البرنامج مسلمًا أم غير مسلم؛ لأن حق غير المسلم محترم كحق

ورواه الدارقطني (٤٢٧/٣)، كتاب: البيوع، حديث رقم: (٢٨٩٤)، والحاكم في المستدرك (٤/ ١١٣)، كتاب: البيوع، باب: وأما حديث أبي هريرة، حديث رقم: (٢٣٠٩)، والبيهقي في السنن الصغرى (٣٠٧/٢)، كتاب: البيوع، باب: الشركة، حديث رقم: (٢١٠٥).

قال ابن تيمية في القواعد النورانية (ص: ٢٢٠): "وهذه الأسانيد وإن كان الواحد منها ضعيفا فاجتماعها من طرق يشدّ بعضها بعضا"، وصححه الألباني بمجموع طرقه في الإرواء، (٥/ ١٤٢ - ١٤٦).

(١) رواه أحمد في المسند (٥٦٠/٣٤)، مسند: البصريين، من حديث: عمرو بن يثربي، حديث رقم: (٢١٠٨٢)، وأبو يعلى في مسنده (٣/ ١٤٠)، مسند: عم أبي حرة الرقاشي، حديث رقم: (١٥٧٠)، والدارقطني في سننه (٣/ ٤٢٤)، كتاب: البيوع، حديث رقم: (٢٨٨٥)، والبيهقي في السنن الكبرى، (١٦٦/٦)، كتاب الغصب، باب: من غصب لوحًا فأدخله في سفينة أو بنى عليه جدارًا، حديث رقم: (١١٥٤٥)، وقال الهيثمي في مجمع الزوائد (٤/ ١٧٢): "وأبو حرة وثَّقهُ أبو داود، وضعَّفهُ ابن معين"، واعتمد ابن حجر توثيق أبي داود له في التقريب، (٢٥٠/١)، فقال: "ثقة"، وقوَّاه الألباني بشواهده في إرواء الغليل في تخريج أحاديث منار السبيل، (٢٤٩/٥-٢٧٩)، المكتب الإسلامي، الطبعة: الثانية، ١٤٠٥هـ - ١٩٨٥م، برقم: (١٤٥٩).

(٢) رواه أبو داود، (٦٧٩/٤)، كتاب: الفرائض، باب: ما جاء في إقطاع الأرضين، حديث رقم: (٣٠٧١)، والبيهقي في الكبرى، (٢٣٦/٦)، كتاب: إحياء الموات، باب: مَن أحيا أرضًا ميتة ليست لأحد، ولا في حق لأحد، فهي له، حديث رقم: (١١٧٧٩)، وضعفه الألباني في ضعيف الجامع (٥٧١٦)، وقال: "قلت: إسناده ضعيف، مظلم؛ منْ دون أسْمر بن مُضرِّس؛ أربعتهم مجهولون، ولذلك استغربه المنذري"، ينظر: ضعيف أبي داود، (٤٥٩/٢)، تأليف: ناصر الدين الألباني، مؤسسة غراس، الكويت، الطبعة: الأولى، ١٤٢٣ه.

المسلم ومعاملاته الإلكترونية على وفق ما يُسمَّى في الوقت المعاصر بالحقوق المعنوية مصونة شرعًا، وقرر ما يلي:

الاسم التجاري والعنوان التجاري والعلامة التجارية والتأليف والاختراع أو الابتكار هي حقوق خاصة لأصحابها، أصبح لها في العرف المعاصر قيمة المالية معدودة لتمول الناس لها وهذه الحقوق يعتد بها شرعا فلا يجوز الاعتداء عليها.

ويجوز التصرف في الاسم التجاري أو العنوان التجاري أو العلامة التجارية ونقل أي منها بعوض مالي إذا انتفى الغرر والتدليس والغش باحتساب أن ذلك حقًا ماليًا.

التحلي بالمصداقية والوضوح؛ فلا يستخدم على هذه المنصات اسمًا غير اسمه أو صورة غير صورته فينتحل شخصية إنسان آخر، سواء أكان من باب الجد أم الهزل، فما أكثر عمليات النصب والاحتيال التي تحدث جراء انتحال أسماء أشخاص أو شركات، وهو ما يرفضه الشرع الشريف؛ لأنه من باب الغش والخداع، وفي الحديث: «مَنْ غَشَّنَا فَلَيْسَ مِنَّا»(١).

ومن صور حماية الشريعة الإسلامية للتجارة الإلكترونية إيقاع عقوبة حد السرقة بشروطها، أو التعزير لمَن يشرع، أو يرتكب اختلاس الأموال بالطريقة الإلكترونية، أو أخذ وسائل إلكترونية للغير البطاقات الائتمانية، أو تزوير التوقيع الإلكتروني فيها؛ كل ذلك محرم في الشريعة الإسلامية، ويستحق مرتكبه العقاب الشرعي لحرمة الأموال شرعًا، وقد يصدر بحق من فعل ذلك بطريقة منظمة تنفيذ حد الحرابة بخاصة جرائم الإنترنت: كالتخريب، أو إزالة للمواقع، أو السرقة، أو

(١) رواه مسلم (١/٩٩)، كتاب: الإيمان، باب: قول النبي ﷺ: «مَنْ غَشَّنَا فَلَيْسَ مِنَّا»، من حديث أبي هريرة I، حديث رقم: (١٦٤).

الانتهاب، أو الإخافة، أو الترويع[١].

هل تنطبق شروط السرقة الحدية على سرقة الإلكترونية؟:

(المسألة الأولى): مدى انطباق شروط السرقة الحدية على سرقة البيانات الإلكترونية:

لبحث مسألة إقامة عقوبة الحد، أو التعزير على سرقة البيانات الإلكترونية يتوجب علينا أولًا معرفة شروط تطبيق حد السرقة التقليدية على السرقة الإلكترونية، وبيان ذلك بالتالي:

الشرط الأول: أن يكون المسروق مالا مُتَقَوّما شرعًا، وفي هذا الشرط اختلف العلماء على قولين:

القول الأول: للحنفية، حيث أنهم حصروا معنى المال في الأعيان؛ لأنه عندهم: "مَا يَمِيلُ إِلَيْهِ الطَّبْعُ وَيُمْكِنُ ادْخَارُهُ لِوَقْتِ الْحَاجَةِ"[٢]، وهذا غير متصور في المنافع التي لا يمكن ادخارها[٣]،فالبيانات الإلكترونية لا تعتبر أموالًا.

القول الثاني: ذهب إليه الجمهور من المالكية[٤] والشافعية[٥] والحنابلة[٦]،

---

(١) ينظر: مجلة الفقه الإسلامي، العدد الخامس، الجزء الثالث، (ص: ٢٦٧)، رقم (١٨٤٥٣) في ٢/١/١٤١٧ هـ.

(٢) الدر المحتار لابن عابدين، (١٠/٧)، مرجع سابق.

(٣) ينظر: درر الحكام شرح مجلة الأحكام، (١٠٠/١)، تأليف: علي حيدر، تعريب: المحامي كمال فهمي، دار الكتب العلمية، بيروت – لبنان.

(٤) ينظر: أحكام القرآن، (١٠٧/٢)، تأليف: محمد بن عبد الله ابن العربي، تحقيق: محمد عبد القادر عطا، دار الكتب العلمية، بيروت – لبنان، الطبعة: الثالثة، ٢٠٠٣م.

(٥) ينظر: حواشي تحفة المحتاج بشرح المنهاج، (٢٣٨/٤)، تأليف: عبد الحميد الشرواني، وأحمد بن قاسم العبادي، مطبعة مصطفى البابي الحلبي، القاهرة – مصر.

(٦) ينظر: شرح منتهى الإيرادات المُسمَّى دقائق أولي النهى لشرح المنتهى، (١٦٢/٣)،

=

في توسعة مفهوم المال؛ ليشمل الأشياء المعنوية التي يمكن تقويمها بالمال، وعليه فإن البيانات الإلكترونية تعتبر حقوقًا مالية معتبرة عندهم.

الترجيح:

ما ذهب إليه الجمهور في توسعة مفهوم المال، وهو الصحيح المعمول به عرفًا[١]، فإطلاق وصف المال على المنافع أحق من إطلاقه على الأعيان، إذ لولا المنافع لما صارت الأعيان أموالًا، إذ لا يصح بيع الأعيان من دونها[٢]، والقول بعدم انطباق وصف المال على البيانات الإلكترونية يخرجها من مجال الحماية الجزائية والشرعية للأموال، ويفتح الباب أمام قرصنة البيانات[٣].

ومما يؤكد هذا الترجيح ما قرره مجمع الفقه الإسلامي بأن: "حقوق التأليف والاختراع أو الابتكار مصونة شرعا، ولأصحابها حق التصرف فيها، ولا يجوز الاعتداء عليها"[٤].

الشرط الثاني: أخذ المال خُفْيَة: وهذا الشرط متوفر في سرقة البيانات

مرجع سابق.

(١) ينظر: الفقه الإسلامي وأدلته للزحيلي، (٤٢/٤)، وقضايا فقهية معاصرة في المال والاقتصاد، (ص: ٣٥)، تأليف: نزيه حماد، دار القلم، دمشق – سوريا، الطبعة: الأولى، ٢٠٠١م.

(٢) ينظر: تخريج الفروع على الأصول، (٢٢٥/١)، تأليف: محمود بن أحمد الزنجاني، تحقيق: الدكتور محمد أديب صالح، مؤسسة الرسالة، بيروت – لبنان، الطبعة: الثانية، ١٣٩٨ه.

(٣) ينظر: جرائم الحاسب الآلي والإنترنت، (ص: ١١٦)، تأليف: أسامة أحمد المناعسة وآخرون، دار وائل، عمّان – الأردن، الطبعة: الأولى، ٢٠٠١م.

(٤) قرار رقم: (٥)، (٢٢٦٧/٣)، بشأن: الحقوق المعنوية، مجلة مجمع الفقه الإسلامي، العدد: الخامس.

الإلكترونية؛ لأن السارق يقوم بالاستيلاء على البيانات دون أن يتنبه المسروق منه.

وبالرغم من اعتبار المال الإلكتروني مالًا متقومًا شرعًا إلا أنه لا تنطبق عليه حد السرقة لوجود الفروق بينهما، تتمثل فيما يلي:

من شروط السرقة الحدية أن يعلم السارق بتحريم الفعل الذي اقترفه، فالجهالة بالتحريم شبهة تدرأ الحد، وقد ذهب بعض العلماء المعاصرين إلى جواز الانتفاع بالبيانات الإلكترونية دون إذن أصحابها، قال الشيخ عبد الرزاق عفيفي -رحمه الله-: "يجوز نسخ حزم البرامج الخاصة بالحاسبات بصفة عامة، وبصرف النظر عن الغرض من النسخ، فيجوز النسخ حتى لو كان الغرض منه الإتجار"(١).

من شروط السرقة الحدية إخراج المال من حيازة المسروق منه وإدخاله في حيازة السارق، وهذا الشرط غير منطبق على سرقة البيانات.

مناقشة الشرطين السابقين:

الشرط الثاني يفسر الشرط الأول؛ كون السرقة الحدية واقعة على ما فيه إضرار بأموال الغير، وأما القول المنقول عن الشيخ عبد الرزاق عفيفي -رحمه الله- فهو في باب المباحات، ومعلوم بأن البيانات الإلكترونية المترتب عليه الإضرار والتعدي على أموال الغير لا تدخل في قول الشيخ عبد الرزاق؛ إذ إن الشيخ قد أحال بعد الفتيا لبحث الشيخ بكر بن عبد الله أبو زيد – رحمه الله- والذي يقول فيه: "أما حق التصنيف: فليس بمال، ولا يصلح أن يكون ملكًا لأحد، بل إن الحكومة كما أنها قررت أن يكون حقًا للأشياء الكثيرة التي ليست

(١) حقوق الإنتاج الذهني، (ص:١٩)، تأليف: الدكتور طلعت رفعت، مجلة الحاسب الآلي، السعودية، العدد: الأول، ١٤١٣هـ.

بقابلة أن تكون حقًا. فهكذا قررت أن يكون هذا الشيء حقًا"[١]، وقال في موضع آخر: "وخلاصة الأمر أن حق التصنيف والابتكار ليس بشيء قابل أن يكون ملكًا لأحد، فلو طبع أحد كتابًا أو نقله أو قلد صناعة بجهوده فالمنع عن ذلك ليس بأمر مباح"[٢].

وعليه: فإن سرقة البيانات يمكن أن تكيف على أنها غصب لمال متقوم أو منفعة مقومة بمال، ومن ثمة فهي جريمة تعزيرية، يُترك تقديرها للقاضي بما يحفظ به حقوق الأفراد والمؤسسات.

(المسألة الثانية): مدى انطباق شروط السرقة التقليدية على سرقة الأموال الإلكترونية:

تعتبر هذه المسألة من النوازل الفقهية المعاصرة، وبالرغم من ذلك فلم تُعطَ حقها بحثًا ومناقشةً، والتي تكاد تُجمع الآراء الفقهية على تجريم مرتكب هذا الفعل، وإن اختلفت آراؤهم حول تكييفها، على النحو الآتي:

الرأي الأول: يرى أصحاب هذا الرأي أن سرقة الأموال الإلكترونية عن طريق الاختراق، أو سرقة بطاقات الائتمان - سرقة حدية مكتملة الأركان؛ وذلك لكون المسروق مالًا بلغ النصاب، ووقعت السّرقة خفْية عن صاحب المال، وأُخِذَتْ من الحرز، وهو الحساب البنكي.

وممن نحى هذا المنحى: الدكتور سالم بن حمزة مدني[٣]، ومال إليه بعض

---

(١) ملكية التأليف تاريخًا وحكمًا، (ص: ٢١٧)، الباحث: الدكتور بكر بن عبد الله أبو زيد، مجلة المجمع الفقهي الإسلامي، العدد الثاني، ١٤٠٨ه.

(٢) المرجع السابق، (ص: ٢١٩).

(٣) ينظر: مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية، (ص: ٧٣-٧٨)، مجلة الحجاز العالمية المحكمة للدراسات الإسلامية والعربية، السعودية، العدد: السادس، فبراير/٢٠١٤م.

الباحثين المعاصرين[١].

أدلة أصحاب الرأي الأول:

الدليل الأول: أركان السرقة التقليدية جميعها متوفر جميعها في السرقة الإلكترونية، ولم يتغير فيها سوى الأسلوب الذي تمت به السرقة.

الدليل الثاني: الحكمة من إقامة حد السرقة هي: حفظ الأموال، وهذه الحكمة تنطبق على سرقة الأموال إلكترونيًا، بل هي أسوأ من السرقة التقليدية، إذ يمكن للسارق سرقة مبالغ ضخمة، وسرقة عدة أشخاص في آنٍ واحد، فتطبيق حد السرقة هنا من باب أولى[٢].

الرأي الثاني: السرقة الإلكترونية ينطبق عليها حد الحرابة، وإلى هذا الرأي مال الدكتور عطا عبد العاطي محمد السنباطي[٣].

أدلة أصحاب الرأي الثاني[٤]:

---

(١) ينظر: السرقة الإلكترونية – دراسة فقهية، (ص: ١٦٤-١٦٩)، تأليف: ضياء مصطفى عثمان، دار النفائس، عمّان – الأردن، الطبعة: الأولى، ٢٠١١م، والسرقة الإلكترونية بين الحد والتعزير، (ص: ١١٠-١١١)، الباحث: تركي بن عبد العزيز بن تركي آل سعود، رسالة ماجستير مقدمة لأكاديمية نايف العربية للعلوم الأمنية، الرياض – السعودية، ٢٠١١م.

(٢) ينظر: مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية، (ص: ٧٨)، الباحث: الدكتور سالم بن حمزة مدني، مجلة الحجاز العالمية المحكمة للدراسات الإسلامية والعربية، السعودية، العدد: السادس، فبراير/٢٠١٤م.

(٣) ينظر: موقف الشريعة الإسلامية من الإجرام الدولي – جرائم الحاسب الآلي والإنترنت، (٣/٣٣٦-٣٣٨)، بحث منشور، مؤتمر: الوقاية من الجريمة في عصر المعلوماتية، كلية الشريعة، جامعة الإمارات العربية، ٦-٨/مايو/٢٠٠١م.

(٤) ينظر: المرجع السابق، (٣/٢٢٦-٢٢٩)، و (٣/٣٣٦-٣٣٨).

الدليل الأول: السرقة الإلكترونية لا تنطبق على السرقة التقليدية التي توجب الحد؛ لأنها ربما تمت بسبب إهمال المالك للمال المسروق، كما أن شرط الحرز غير متوفر فيه، إذ الحاسب الآلي لا يعتبر حرزًا، فهو كَبَيْتٍ في الصحراء، ولا حافظ له يتهيَّب منه اللصوص، كما لم يطالب مالك المال المسروق منه بماله، وهو شرط في الحد.

مناقشة الدليل الأول: من عدة أوجه:

الوجه الأول: دعوى أن صاحب المال تمت سرقته بسبب إهماله؛ دعوى باطلة، كونه لم يضطر لوضعها في البنوك إلا رغبةً في حفظها، بل وأشد مما لو حفظها هو بنفسه.

الوجه الثاني: الحرز أمر معنوي أكثر من كونه حسيًا، بمعنى أن الحرز ينطبق على كل ما فيه أمان للممتلكات، فجعل الحاسب الآلي ليس بحرز أمر لا وجه له، ومن باب أولى لا وجه لقياس التكنولوجيا الحديثة في حفظ الأموال ببيت ناء في الصحراء.

الوجه الثالث: أنه من غير المتصوّر؛ بل يكاد يكون الاحتجاج بعدم مطالبة صاحب المال بأمواله، أمر لا وجود له في الواقع.

وعليه فهذا استدلال ضعيف من جميع الأوجه.

الدليل الثاني: السرقة الإلكترونية تتم عادة من المنظمات الإجرامية على وجه المجاهرة والمغالبة والمحاربة لولي الأمر، وتُستخدم في نطاق أمور سياسية أو عسكرية.

مناقشة الدليل الثاني: كون السرقات الإلكترونية تتم غالبًا عن طريق منظمات وهيئات مختصة في هذا العمل الإجرامي؛ لا يعني هذا عدم وجود المخترقين للحسابات الإلكترونية بأنواعها -مالية وغير مالية.

الرأي الثالث: ذهب بعض المعاصرين إلى التعزير في عقوبة السرقة

الإلكترونية، على اعتبار أن شروط السرقة التقليدية غير متوفرة فيها، فشرط الحرز غير متوفر، بالإضافة إلى وجود شبهة في المال المسروق، وعدم مطالبة المسروق منه بحقه؛ ولأن يخطئ الإمام في العفو خير من أن يخطئ في العقوبة.

مناقشة احتجاج أصحاب الرأي الثالث:

يناقش بمثل ما نوقشت به أدلة أصحاب الرأي الثاني.

الترجيح:

يرجع سبب اختلاف الفقهاء في هذه المسألة إلى الخلاف حول انطباق السرقة الإلكترونية على السرقة التقليدية من عدمه، وللترجيح بين هذه الأقوال ينبغي البحث في توفر شروط السرقة الحدية في السرقة الإلكترونية، على النحو التالي:

شرط أن يكون المسروق مالًا متقومًا مملوكًا للغير: لا شك أن بطاقات السحب الآلي، والحسابات البنكية؛ تعتبر أموالًا متقوّمة مملوكة لأصحابها؛ كونها تمكّن صاحبها من شراء السلع، والخدمات، والحصول على النقود، والهدف من قرصنة الحسابات البنكية أو بطاقات السحب الآلي هو سرقة الأموال التي تحتوي عليها، ولم يختلف في ماليتها أي من الآراء السابقة[1].

شرط أن يؤخذ المال من حرزه: اتفق أصحاب المذاهب الأربعة إلى أن حد السرقة لا يقام إلا إذا أخذ السارق النصاب من حرزه؛ لأن المال غير المحرز ضائع بتفريط صاحبه، وقد اختلفت عبارات المذاهب الأربعة في تعريف الحرز على النحو التالي:

الحرز عند الحنفية: "مَا يُحْفَظُ فِيهِ الْمَالُ عَادَةً كَالدَّارِ وَإِنْ لَمْ يَكُنْ لَهَا

(١) ينظر: موقف الشريعة الإسلامية من الإجرام الدولي، (٣/٣١٥)، الباحث: الدكتور عطا عبد العاطي محمد السنباطي، مرجع سابق.

بَابٌ"[١].

الحرز عند المالكية: "كُلُّ مَا لَا يُعَدُّ صَاحِبُ الْمَالِ فِي الْعَادَةِ مُضَيِّعًا لِمَالِهِ بِوَضْعِهِ فِيهِ"[٢]، "وَلَيْسَ لَهُ ضَابِطٌ شَرْعِيٌّ، وَحِرْزُ كُلِّ شَيْءٍ بِحَسَبِهِ فَالْحِرْزُ يَخْتَلِفُ بِاخْتِلَافِ الْأَشْخَاصِ وَالْأَمْوَالِ"[٣].

وعند الشافعية: "فَإِنَّهُ لَمْ يُحَدَّ فِي الشَّرْعِ وَلَا فِي اللُّغَةِ، فَرَجَعَ فِيهِ إِلَى الْعُرْفِ، كَالْقَبْضِ وَالْإِحْيَاءِ، وَلَا شَكَّ أَنَّهُ يَخْتَلِفُ بِاخْتِلَافِ الْأَمْوَالِ وَالْأَحْوَالِ وَالْأَوْقَاتِ، فَقَدْ يَكُونُ الشَّيْءُ حِرْزًا فِي وَقْتٍ دُونَ وَقْتٍ، بِحَسَبِ صَلَاحِ أَحْوَالِ النَّاسِ وَفَسَادِهَا، وَقُوَّةِ السُّلْطَانِ وَضَعْفِهِ، وَضَبَطَهُ الْغَزَالِيُّ بِمَا لَا يُعَدُّ صَاحِبُهُ مُضَيِّعًا"[٤].

وأما الحرز عند الحنابلة: "مَا عُدَّ حِرْزًا فِي الْعُرْفِ فَإِنَّهُ لَمَّا ثَبَتَ اعْتِبَارُهُ فِي الشَّرْعِ مِنْ غَيْرِ تَنْصِيصٍ عَلَى بَيَانِهِ عُلِمَ أَنَّهُ رَدَّ ذَلِكَ إِلَى أَهْلِ الْعُرْفِ؛ لِأَنَّهُ لَا طَرِيقَ إِلَى مَعْرِفَتِهِ إِلَّا مِنْ جِهَتِهِ، فَرُجِعَ إِلَيْهِ"[٥].

ومن خلال هذه التعريفات للحرز عند الفقهاء، نجد أنهم قد اتفقوا على أن الحرز هو الموضع الحصين الذي يُحفظ فيه المال عادةً، بحيث لا يُعدّ صاحبه مضيعًا له بوضعه فيه، ومرجع ذلك هو العرف؛ إذ لم يرد عن الشارع تحديد له، ومن المعلوم أن الحرز تختلف أحواله باختلاف الزمان، والمكان، ونوعية المال،

---

(١) رد المحتار لابن عابدين، (١٥٩/٦)، مرجع سابق.

(٢) التاج والإكليل لمختصر خليل، (٣٠٨/٦)، تأليف: محمد بن يوسف المواق، تحقيق: زكريا عميرات، دار الكتب العلمية، بيروت – لبنان، الطبعة: الأولى، ١٩٩٥م.

(٣) حاشية العدوي على كفاية الطالب الرباني، (٤٣٤/٢)، تأليف: علي بن ناصر الدين بن محمد العدوي، تحقيق: محمد عبد الله شاهين، دار الكتب العلمية، بيروت – لبنان، الطبعة: الأولى، ١٩٩٧م.

(٤) مغني المحتاج للشربيني، (٢١٥/٤)، مرجع سابق.

(٥) المغني لابن قدامة، (٤٢٧/١٢)، مرجع سابق.

وبيان نوع الحرز موكول في كل قضية لم يرد فيها نص إلى الحاكم، فيستعين على تعيين ذلك بأهل الخبرة[١].

وبتطبيق ذلك على الحسابات البنكية حيث إن الناس قد تعارفوا على أنها موضع للمال بقصد الحفظ والصون من الاعتداء أو الضياع، وأن استعمالها قاصر على ملاكها، وبالتالي يعتبر اختراق البنوك وقرصنة البطاقات المصرفية المملوكة للغير انتهاكًا للحرز.

شرط الأخذ خفية: وذلك من خلال أخذه استتارًا، فإن أخذ الشيء على سبيل المجاهرة سُمِّي: مغالبةً، أو نهبًا، أو خلسةً، أو اغتصابًا، أو انتهابًا، لا سرقة[٢].

كما لا تكتمل صورة الأخذ خفية إلا إذا أخرج السارق الشيء المسروق من حيازة المسروق منه، وأدخله في حيازته[٣].

(مسألة): اختلفت المذاهب الأربعة على طريقة الأخذ التي تؤدي إلى إقامة الحد:

فذهب الحنفية[٤]: إلى أن الأخذ لا يتحقق إلا إذا كان هتك الحرز هتكًا

---

(١) ينظر: حد السرقة في الشريعة الإسلامية، (ص: ٥١-٥٢)، الباحث: محمد بن عبد الله بن سبيل، مجلة المجمع الفقهي الإسلامي، مكة المكرمة، العدد: ١٢، الطبعة: الثانية، ٢٠٠٦م.

(٢) ينظر: الاختيار لتعليل المختار للموصلي، (١٠٩/٤)، ومنح الجليل لعليش، (٢٩١/٩-٢٩٢)، مغني المحتاج للشربيني، (٢٢٤/٤)، والمغني لابن قدامة، (٤١٦/١٢)، مراجع سابقة.

(٣) ينظر: بدائع الصنائع للكاساني، (٧٧/٧)، والشرح الكبير للدردير، (٣٣٨/٤)، والحاوي للماوردي، (٢٩٢/١٣)، مراجع سابقة، ومطالب أولي النهى في شرح غاية المنتهى، (٢٣٥/٦)، تأليف: مصطفى الرحيباني، المكتب الإسلامي، دمشق – سوريا، ١٩٦١م.

(٤) ينظر: الاختيار للموصلي، (١١٣/٤)، وبدائع الصنائع للكاساني، (٦٦/٧)، مراجع سابقة.

كاملًا تحرزًا عن شبهة العدم، وذلك بأن يدخل الحرز فعلًا، إذا كان مما يمكن دخوله، فإذا كان مما لا يمكن دخوله كصندوقٍ، وجيبٍ، فلا يشترط الدخول.

وذهب أبو يوسف(١)، والمالكية(٢)، والشافعية(٣)، والحنابلة(٤): إلى أن دخول الحرز ليس شرطًا لتحقق الأخذ وهتك الحرز؛ فدخول الحرز ليس مقصودًا لذاته، بل لأخذ المال.

وبتطبيق شرط الأخذ خفية على سرقة الحسابات المصرفية نجده منطبقًا عليها؛ فالسرقة الإلكترونية تتم بأخذ المال خفية، وإخراجه من حساب المسروق منه بانتهاك حرز الحاسب الإلكتروني، وإدخاله في حساب الغير خفية.

الخلاصة: أن السرقة الإلكترونية للأموال تطابق السرقة الموجبة لإقامة الحد على السارق بشرطين:

الشرط الأول: أن يتخذ القائمون على المصارف احتياطاتهم الأمنية، من خلال اتخاذ الإجراءات اللازمة لحفظ الحسابات البنكية من الاختراق، والقرصنة؛ حتى لا يُعتبروا مفرّطين، كما يتعيّن على عميل البنك أن يتخذ جميع الاحتياطات التي تحول دون استحواذ الغير على معلوماته البنكية، وإلا فيُعدُّ

---

(١) ينظر: الاختيار للموصلي، (١١٣/٤)، مرجع سابق.

(٢) ينظر: منح الجليل لعليش، (٣٠٩/٩)، مرجع سابق.

(٣) ينظر: الحاوي الكبير في مذهب الإمام الشافعي، (٢٩٤/١٣)، تأليف: علي بن محمد بن محمد البصري الماوردي، تحقيق: علي محمد معوض، وعادل أحمد عبد الموجود، دار الكتب العلمية، بيروت – لبنان، الطبعة: الأولى، ١٩٩٤م.

(٤) ينظر: شرح الزركشي على مختصر الخرقي، (١٢١/٣)، تأليف: محمد بن عبد الله الزركشي، تحقيق: عبد المنعم خليل إبراهيم، دار الكتب العلمية، بيروت – لبنان، ٢٠٠٢م.

مُخلًا في حفظ ماله[١].

الشرط الثاني: أن يقوم السارق بإخراج المال من حيازة مالكه إلى غيره، وأما إذا اكتفى بسرقة البطاقة، أو الدخول إلى الحساب دون الاستيلاء على المال، فلا يمكن تطبيق حد السرقة عليه؛ لأن شرط الأخذ خفية يستلزم إخراج المال من حيازة مالكه -كما بيّنا في شرط الأخذ خفية-، وهذا الشرط غير متوفر هنا.

(١) ينظر: الإجراءات اللازم اتخاذها لحماية بطاقات الائتمان من القرصنة، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض – السعودية، الطبعة: الأولى، ٢٠٠٢م.

المبحث الثاني

خطر الاختراقات الإلكترونية

المطلب الأول

مفهوم الاختراقات الإلكترونية

يقصد بالاختراقات الإلكترونية: "الدخول غير المشروع إلى المعلومات والبيانات الموجودة في المواقع على شبكة الإنترنت بما فيها البريد الإلكتروني"(١).

وهذا السلوك غير المشروع يمكن أن يرتكبه أحد العاملين في الأنظمة أو الجهات المالكة لها، والذي لا تسمح له طبيعة عمله بالولوج إلى تلك المعلومات، كما قد ترتكب من أشخاص خارج تلك الجهات بمساعدة أو دون مساعدة أحد من الداخل، كما يمكن أن يكون الاختراق عن بعد باستغلال الإنترنت(٢).

أو هو: "القدرة على الوصول لأجهزة وبيانات الآخرين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة بهم"(٣).

والاختراق: "مجموعة من الأعمال التي تؤدي إلى الإخلال بنظام وسرية الجهاز، ويقوم بالاختراق شخص أو أكثر عن طريق شبكة الإنترنت باستخدام

---

(١) الحماية المدنية للمعلومات الحاسوبية الشخصية (التعويض) في الفقه الإسلامي وأنظمة المملكة العربية السعودية، د. مسفر القحطاني. ط- ١٤٢٦هـ - ٢٠٠٥م. (ص: ٦١).

(٢) ينظر: الحماية المدنية للمعلومات الحاسوبية الشخصية (التعويض) في الفقه الإسلامي وأنظمة المملكة العربية السعودية، د. مسفر القحطاني. ط- ١٤٢٦هـ - ٢٠٠٥م. (ص: ٦١)..

(٣) أساسيات أمن المعلومات، د. محمد القاسم، د. عبد الرحمن الحمدان، تصميم/ ديجتال ديزايين، الرياض، ط٢ – ١٤٢٩هـ - ٢٠٠٨م. (ص: ١٤٦).

برامج متخصصة (سكانرز) تعمل على فك الرموز والكلمات السرية، وكسر الحواجز الأمنية باستكشاف نقاط الضعف في المواقع التي لا تحدث أنظمتها بشكل دوري، ثم مهاجمتها واختراق نظامها الأمني، والتسلل هو السلوك المصاحب لهذا الفعل"[١].

والاختراق الإلكتروني يمثل التحدي الأكبر الذي يواجه الأفراد والشركات والمواقع الإلكترونية، وهو يبدو أشبه بحرب مفتوحة لا قاعدة ثابتة لها سوى استفادة كل طرف من ثغرات الطرف الآخر، وهي تتم عادة عبر برامج معقدة وأشكال مختلفة، قد تصل إلى حد رصد تحركاتنا الشخصية، عبر اختراق أجهزة الكومبيوتر المحمولة، وربما مراقبتنا داخل منازلنا.

وفي هذا الصدد قال جيمس بولارد[٢] -رئيس بنك الاحتياطي الفيدرالي في سانت لويس-: "إنه يتعين على الجهات الرقابية في الولايات المتحدة تسريع الجهود الرامية لمعالجة المخاطر التي تتسبب فيها شركات التكنولوجيا المالية داخل القطاع المصرفي".

كما حذّر من أن المنظمين إذا لم يكونوا أكثر مكافحة لتلك التكنولوجيا؛ فإنهم سيستيقظون في يوم ويجدون معظم البنوك الكبيرة قد انتزعت، مما يتسبب في أزمة مالية.

وعلى الرغم من الملاحقة القانونية التي تطارد العملات الإلكترونية، فإن

---

(١) أمن الإنترنت من الاختراق وأخصه طروادة، (ص: ٥٦)، تأليف: د. عبد الله القحطاني، مجلة أحوال المعرفة، ربيع الآخر، ١٤٢٣هـ - ٢٠٠٢م، مكتبة الملك عبد العزيز، الرياض - السعودية.

(٢) أمن الإنترنت من الاختراق وأخصه طروادة، (ص: ٥٦)، تأليف: د. عبد الله القحطاني، مجلة أحوال المعرفة، ربيع الآخر، ١٤٢٣هـ - ٢٠٠٢م، مكتبة الملك عبد العزيز، الرياض - السعودية.

التكنولوجيا المالية (**Fintech**) لاتزال بعيدة عن تلك العقوبات.

وهذه الخروقات تحدث إما بسبب جدتها وحداثتها أو بسبب جهل الشركة بها، وتنتج عما يلي من الأسباب[١]:

فيروسات غير معروفة: رغم وجود أنظمة حماية من الفيروسات على أنظمة المؤسسة، إلا أن هنالك فيروسات غير معروفة بعد للنظام الحمائي للمؤسسة، قد تتمكن من دخول نظام الشبكة وإحداث تلف كبير دون الشعور به إلا بعد فوات الأوان.

والفيروس: هو وسيلة تكنيكية حديثة تستخدم لارتكاب جرائم معينة[٢]، وهي برامج مشفرة مصممة بقدرة على التكاثر والانتشار من نظام إلى آخر بواسطة قرص ممغنط أو عبر شبكة الاتصالات، بحيث يمكن أن تنتقل عبر الحدود من أي مكان إلى آخر في العالم[٣]، وبرامج الفيروسات لها القدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافها، وقد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات، ثم تقوم بتدمير نفسها ذاتيًا دون أن تترك أثرًا يدل عليها، وعلى الرغم من قدرتها على تدمير البرامج والمعلومات، إلا أنها لا تسبب عادة تدميرًا لمكونات النظام المادي[٤]، والفيروس المعلوماتي له من خصائص

---

(١) ينظر: أثر الألعاب الإلكترونية على السلوكيات لدى الأطفال، مريم قويدر، رسالة ماجستير، جامعة الجزائر، ٢٠١٢، (ص: ٣٠).

(٢) ينظر: الحماية الجنائية للمعلومات عبر الإنترنت، د. رشدي محمد على عيد، رسالة دكتوراه كلية الحقوق – جامعة القاهرة ٢٠٠٩، (ص: ٢٥٠).

(٣) ينظر: قانون العقوبات ومخاطر تقنية المعلومات، د. هشام محمد فريد رستم، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢م، (ص: ١٦١)، وما بعدها.

(٤) ينظر: مشكلات المسئولية المدنية في مواجهة فيروس الحاسب، د. عزة محمود أحمد خليل، دراسة مقارنة في القانون المدني والشريعة الإسلامية، رسالة دكتوراه كلية

=

المجرم الكثير: فهو يختفي كخطوة أولى، ثم يبدأ في التطور كخطوة ثانية ليدمر في خطوة ثالثة، كالمجرم الذي يضع خطته لارتكاب الجريمة[١].

أ. **قراصنة إنترنت ذوي خبرة عالية:** تعد هذه الحالة من أكبر المشاكل التي تواجهها المؤسسات؛ لأن قراصنة بعضهم يملك خبرة ومهارة تفوق كثيرًا من المتخصصين تمكنهم وفي كثير من الأحيان من اختراق أنظمة المؤسسة دون أن يشعر بهم، وغالبًا تتم جرائمهم دون اكتشاف.

ب. **التسارع التكنولوجي:** يصعب في كثير من الأحيان مواكبة التسارع التكنولوجي على المؤسسات في مجال الإنترنت بشكل عام والتجارة الإلكترونية بشكل خاص؛ مما يجعل التكنولوجيا التي تستخدمها المؤسسة قديمة جدًا عاجزة عن التنبؤ والتعامل في حينه وتصور الحلول المناسبة.

صعوبة تعقب الاختراقات التي تتم عبر شبكة الإنترنت: يعد نظام التجارة الإلكترونية بيئة مثالية للسرقات والتلاعب وإخفاء آثار الجريمة بشكل متقن منقطع النظير.

ومن المعروف أن الشركات التجارية الكبرى تعيش هي -أيضًا- فيما بينها حربًا مستعرة، وقد بينت الدراسات الحديثة أن عددًا من كبريات الشركات التجارية يجري عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم[٢].

الحقوق - جامعة القاهرة ١٩٩٤، من (ص: ٣٧) وما بعدها.

(١) ينظر: المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، د. ماجد عمار، دار النهضة العربية، القاهرة، ١٩٨٩م، (ص: ٧٦).

(٢) ينظر: وقد تبين من إحصائية موثقة أن أكبر (٥٦٠) شركة تعتمد في أعمالها على الإنترنت قد تعرض أكثر من نصفها إلى هجوم بواسطة الهاكرز، وأن أكثر من ثلاثة أرباع الذين هوجموا بواسطة الـ hackers قد هوجموا داخلياً. انظر: جرائم الإنترنت =

حيث يعمل المخترق على تعطيل أجهزة الكمبيوتر أو تخريبها عبر إرسال الفيروسات، أو البرامج التي تحوي أنظمة هجومية؛ مما يسبب تلفًا في أنظمة الكمبيوتر يؤدي لشلل كل الأنشطة المرتبطة بهذا الجهاز أو الأنظمة المرتبطة به.

فمثلًا في الولايات المتحدة الأمريكية أصدر مكتب التحقيقات الفيدرالي الأمريكي -إنذارًا عامًا يحذر مستخدمي الإنترنت من مخاطر رسائل إلكترونية جديدة، تنطوي على فخ، يدفع المستخدمين إلى الكشف عن بيانات حساباتهم المالية الشخصية، ليصار لاحقا إلى السطو عليها"(١).

وحذرت دائرة شكاوى جرائم الإنترنت التابعة للمكتب الفيدرالي، من ظهور مجموعة من الرسائل الإلكترونية، التي تزعم أن المتلقي قد قام بعمليات شراء البضائع عبر الشبكة، وتستدرجه للكشف عن بيانات حساباته، وقالت الدائرة إن نموذجين من تلك الرسائل تم رصدهما، تدعي الأولى أن المتلقي قد عقد طلبية لشراء جهاز كمبيوتر عبر الشبكة، وتطلب منه في حال عدم رغبته بإتمام الطلبية الدخول إلى وصلة البيانات الشخصية لإلغائها، وسيجد متصفح البريد الإلكتروني الذي يدخل تلك الوصلة معلومات شخصية حول حساباته المالية يتوجب عليه الكشف عنه لإلغاء عملية الشراء المزعومة؛ وبذلك يحقق أصحاب تلك الرسائل هدفهم، أما النموذج الثاني فيتضمن بيان كشف مشتريات مرسلة كملف **PDF**، تحتوي على فيروس يتسلل إلى جهاز الكمبيوتر الشخصي للمتلقي، ما إن يقوم بالدخول وتشغيل الرسالة **Ready** لقراءتها"(٢).

والحاسب الآلي ووسائل مكافحتها، منير محمد ممدوح محمد الجنبيهي، دار الفكر الجامعي، الإسكندرية، ط١ – ٢٠٠٦م، (ص: ٥١).

(١) الحماية الجنائية للحاسب الآلي، أحمد تمام، دار النهضة العربية، القاهرة، ٢٠٠٩م، (ص: ٢٧)

(٢) الحماية الجنائية للحاسب الآلي، مرجع سابق، (ص: ٢٧١).

المطلب الثاني

وسائل، ونماذج الاختراقات الإلكترونية

أولًا: وسائل الاختراقات الإلكترونية

تختلف الوسائل التي يمكن اللجوء إليها لاختراق النظم المعلوماتية: ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل جهاز الكمبيوتر، أو فتح البرنامج الذي يقوم بتشغيله، وقد يتطلب الحصول على الشفرات الخاصة بالدخول باستخدام جهاز لفك الشفرة.

كما يمكن الدخول عن طريق وسائل أخرى للدخول لأنظمة الحاسبات الآلية تعتمد على ضعف الأنظمة ذاتها أو على بعض الأخطاء الناجمة عن عملية البرمجة(١).

ويمكن تلخيص بعض الوسائل التي يمكن أن يستخدمها المخترقون للحصول على معلومات عن الشبكة أو الأجهزة في النقاط التالية:

١. يقوم المخترقون بمحاولة السيطرة على جدران الحماية (**firewall**) حيث يبدأ هجومهم(٢).

٢. قد يقوم المخترقون -أحيانًا- بمهاجمة خادمات الملفات العامة

---

(١) ينظر: جرائم الحاسب الآلي الاقتصادية، د. نائلة عادل محمد فريد. منشورات الحلبي الحقوقية. ط ٢٠٠٥م، (ص: ٣١٦)، الجرائم المعلوماتية، د. خالد ممدوح إبراهيم. دار الفكر الجامعي، الإسكندرية. ط١ ٢٠٠٩م، (ص: ٢٤٦).

(٢) وفي الفترة الأخيرة أصبح من الصعب على أولئك المخترقين السيطرة على جدران الحماية، خاصة مع ظهور تقنيات جديدة أكثر تقدمًا، أما الحالات التي تكتشف ولم تتم معالجتها فيتم إخبار مديري الأمن بها ليتم تداركها.

(severs)؛ ومن ثم يحصلون على معلومات عن الشبكة بعد اختراق الخادم[١].

٣. من وسائل الاختراق -أيضًا-: أن يقوم المخترق بمحاولة الحصول على معلومات عن الشبكة باستخدام وسائل غير هجومية؛ أي: بالدخول كمستخدم عادي -إن كانت لديه صلاحية- ثم يقوم بمحاولة الحصول على معلومات تمكنه من الوصول مباشرة إلى شبكة المنشأة؛ ومن ثم يتصل مباشرة بالخادم ويحصل على المعلومات المطلوبة[٢].

ومن الوسائل -أيضًا-: حصول المهاجمين على معلومات خاصة عن شبكة المنشأة بواسطة الروابط المستخدمة من قبل مستخدمي الشبكة، ومن المعلوم أن تطبيقات الإنترنت تبين اسم الجهاز الخاص بدلًا من الاسم العام، ومن هنا يقوم المهاجم باستخدام هذه المعلومة للحصول على معلومات أكثر عن الخادمات في الشبكة لاستخدامها في عملية الاختراق[٣].

ثانيًا: نماذج الاختراقات الإلكترونية

سرقة ٣ ملايين يورو بسبب تبديل شرائح الموبايل SIM Swapping:

حيث استطاعت مجموعة من الهاكرز في أوروبا استخدام تقنية للاختراق

---

(١) لم تعد هذه الطريقة مجدية للمخترقين؛ لأن تلك الخادمات العامة تكون محمية في الغالب، وعند اكتشاف حدوث أي أمر غير طبيعي يجري في أحد الخوادم فيتم إبلاغ مسؤولي أمن النظم في الشبكة عنه فيتم بعد ذلك استدراكه.

(٢) تعد هذه الطريقة من أنجع الطرق؛ لأنها لا تثير أي أنشطة غير مألوفة في الشبكة قد تثير انتباه مسؤولي أمن الشبكات، كما أن هذه الطريقة تسمح للمهاجم بالوصول إلى الشبكة والحصول على المعلومات التي يريدها بأسرع وقت ممكن، وتكرارها متى أراد.

(٣) ينظر: أساسيات أمن المعلومات، د. محمد بن عبد الله القاسم، د. عبد الرحمن بن عبد العزيز الحمدان. تصميم ديجتال ديزايين، الرياض. ط٢ – ١٤٢٩هـ - ٢٠٠٨م، (ص: ٤٨).

استبدال شرائح الموبايل" لسرقة حسابات بنكية، من المعلوم أن الهاتف المحمول وخصوصًا رقم الهاتف أصبح مركز العمليات المهمة خصوصًا البنكية منها؛ لهذا يعتبر رقم الهاتف من المعلومات التي يسعى الهاكرز إلى الوصول إليها؛ لاستخدامها في النقاط **PIN Code** أو رموز الدخول بخطوتين **FA٢** التي يتم إرسالها من البنوك إلى رقم الهاتف عبر خدمات **SMS**، تمكنت الشرطة الأوروبية من القبض على العصابة التي تتكون من ١٢ فردًا استطاعوا خداع شركات الهاتف المحمول لاستبدال شرائح محمول خاصة بشخصيات عامة لديها حسابات بنكية، إضافة إلى تحميل المحافظ الإلكترونية على الهاتف المحمول بالرقم الذي تم الحصول على بياناته على **SIM Card** آخر وسحب الأموال من ماكينة الصراف الآلي دون الحاجة إلى بطاقة ائتمانية عن طريق **PIN CODE** ورقم الهاتف والمحفظة الإلكترونية، استطاعت العصابة سرقة ما يقرب من ٣ ملايين يورو في هذه العملية[١].

(١) ينظر: اختراقات الأمن السيبراني، مركز المعلومات واتخاذ القرار، مجلس الوزراء المصري، القاهرة، ديسمبر، ٢٠٢٠م، (ص: ١٢).

المطلب الثالث

تجريم الاختراقات الإلكترونية

يعد الاختراق الإلكتروني المجرم محرمًا في الشرع؛ إذ هو تعدٍ على حقوق الآخرين، والشريعة الإسلامية نهت عن الاعتداء، فتجريم الاختراق لما فيه من انتهاك للغير وتعدي على حقوق الآخرين، والله -تعالى- حرم التعدي: {وَلا تَعتَدوا إِنَّ اللَّهَ لا يُحِبُّ المُعتَدينَ} [سورة البقرة: ١٩٠]، وحرم النبي ﷺ الاعتداء على أموال الغير، فقال: «لا يَحِلُّ مالُ المُؤمِنِ إلّا بِطيبِ نَفسِهِ»(١).

وقد نظمت دولة الكويت استخدام وسائل التقنية الحديثة وتجريم الانتهاكات التي تحدث منها أو عليها بإصدار حزمة من التشريعات كان من بينها: قانون مكافحة جرائم تقنية المعلومات رقم ٦٣ لسنة (٢٠١٥).

جاء في المادة (٢) ما نصه:

الجريمة: الدخول غير المشروع إلى جهاز حاسب آلي أو نظام معلوماتي أو شبكة معلوماتية".

العقوبة: الحبس مدة لا تجاوز ستة أشهر + غرامة (٥٠٠ - ٢٠٠٠) دينار أو إحداهما.

الجريمة: إذا ترتب على الدخول إلغاء أو حذف أو تدمير أو تغير أو إعادة نشر بيانات أو معلومات.

العقوبة الحبس مدة لا تتجاوز سنتين + الغرامة (٥٢) ألف دينار أو إحدى هاتين العقوبتين.

إذا كانت البيانات أو المعلومات شخصية تكون العقوبة ثلاث سنوات حبس

---

(١) تخريج: تقدّم تخريجه.

+ غرامة (٣) - (١٠) ألف دينار أو أحدهما".

وفي المادة (٤/٢):

الجريمة: الإدخال العمدي عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات ما من شأنه تعطيلها أو إيقافها عن العمل أو دخول موقع؛ لتغيير تصميمه أو إلغاء أو تعديل أو إيقافه.

العقوبة: الحبس مدة لا تتجاوز سنتين + الغرامة (٢-٥) ألف دينار أو إحدى هاتين العقوبتين.

ويعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار، ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين، كل مَن ارتكب أيًا من هذه الجرائم أو سَهَّل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته".

□

المطلب الرابع

طرق حماية المعاملات المالية الإسلامية من هذه المخاطر

إن التعاملات الإلكترونية تنطوي على العديد من المخاطر التي تحيط بها وبجميع صورها، لكون هذه التعاملات تفتقد الثقة والمصداقية عن غيرها من التعاملات غير الإلكترونية.

وقد تكون المعاملة الإلكترونية تتم بين أطراف تقع في دول مختلفة؛ ولذلك فهي تتضمن كافة المخاطر التقليدية المصاحبة لعمليات التجارة الدولية، وفي حالة إتمام الصفقة على الإنترنت تكون تلك المخاطر أكثر صعوبة.

ولهذا من الضروري حماية المعاملات المالية الإسلامية من هذه المخاطر، والعمل على التصدي لها؛ ولهذا حمت الشريعة الإسلامية المعاملات التجارية من كل أنواع التدليس والكذب والغش، وحرمت كافة أنواع غسيل الأموال التجارية، وأوجبت وسائل السلامة في التعامل التجاري؛ حتى يكسب المال حلالًا، وهي أسس شرعية ينبغي أن يتحلى بهما التاجر، وأوجبت طلب الإذن من صاحب العمل التجاري والالتزام بالأمانة،

والابتعاد عن الغش؛ للحديث: «مَنْ غَشَّنَا فَلَيْسَ مِنَّا»[(١)].

وضرورة التحلي بالأخلاق الحميدة المنبثقة من العقيدة الإسلامية، وضرورة ارتباط النية في البيع والصدق والوفاء بالعقود التجارية والابتعاد عن اليمين المنفقة للسلعة، والالتزام بالشروط العقدية[(٢)].

---

(١) تقدّم تخريجه.

(٢) ينظر: المدخل، لابن الحاج ٤/٩١-٩٣، وشرح النووي على صحيح مسلم (٢/١١٤)، وأخلاقيات مهنة الوراقة في الحضارة الإسلامية، د. عابد سليمان الشوخي، بحث منشور في مجلة جامعة الملك سعود، المجلد ١٥، ١٤٢٣ه، (ص: ٣٤٦).

من طرق حماية المعاملات المالية الإسلامية من هذه الإلكترونية المختلفة، ما يلي:

أولًا: الحماية التقنية: تكون هذه الحماية منصبة على المعاملات المالية من جهة، وعلى جهاز الحاسب من جهة أخرى، ومنها:

١. **حماية المعاملات المالية الإلكترونية**[(١)]: ولها عدة نطاقات نذكر منها حافظة النقود الإلكترونية والافتراضية التي يقصد بها تجميع وحدات للقيمة؛ وذلك في أداة مستقلة عن الحسابات البنكية تعرف بحافظة النقود الإلكترونية وحافظة النقود الافتراضية، فبالنسبة للأولى، فإنها تشحن مسبقًا برصيد مالي ويتم تسجيل هذا الرصيد المالي في بطاقة أما بالنسبة لحافظة النقود الافتراضية، فإنها تشحن برصيد مالي على القرص الصلب لجهاز الكمبيوتر الخاص الذي يستعمل الشبكة، وبالتالي فقطع النقود أو النقود الافتراضية تمثل من الناحية الفنية تلك المعاملات المختزلة على ذاكرة جهاز الكمبيوتر ويستطيع بذلك العميل الذي يرغب في التعامل بهذه النقود أن يحصل من أحد البنوك أو أحد المؤسسات الوسيطة على رخصة تسمح له باستعمال النقود الإلكترونية بالمقابل الذي يتفق عليه، ويكون بدءًا مفتاح عام وخاص من أجل تأمين معاملاته وتحققها.

٢. والهدف من هذه التقنية هو تفادي اختراق البيانات التي يتم تداولها عبر شبكة الإنترنت والتغلب على إمكان استخدامها غير المشروع من قبل الغير؛ لأنه بهذه التقنية يصبح لوحدات القيمة الإلكترونية ذاتية مستقلة حيث يمكن نقلها من محفظة إلكترونية إلى أخرى على نحو يؤدي إلى الوفاء من قبل المدين بمجرد

---

(١) ينظر: نوال عبد الكريم الأشهب: التجارة الإلكترونية، المنهل: https: //www. syja. org/ar/sl/٣١٠٤١.

نقل هذه الرموز الإلكترونية، ويمكن المتلقي هذا الوفاء على حافظة إلكترونية أن يقوم بتحويل هذه النقود الإلكترونية إلى نقود رقمية من خلال البنك المصدر لها.

٣. ومن سلبيات هذه التقنية فرض عمولات كبيرة على البنوك المتعاملة بهذا النظام، مقابل تحويلات النقود الإلكترونية إلى نقود حقيقية، كما أن تطور نظام النقد الإلكتروني ينطوي على تهديد احتكار مركزية عملية إصدار النقود.

٤. كما أن عدم إمكانية تتبع العمليات التي تتم من خلال النقود الإلكترونية يخشى منه ازدياد فرص التهرب الضريبي، وربما يفتح بابا جديدا لعمليات غسل الأموال، كما أن استخدام هذه التقنية لا يخلو من مخاطر فنية متمثلة في إمكانية تعطل القرص الصلب وضياع ما عليه من مبالغ نقدية إلكترونية.

حماية المواقع الخاصة بالإنترنت: وتتجلى حماية المواقع الخاصة بالإنترنت من خلال نظام التشفير ونظام الجدران النارية، والتشفير هو إجراء يؤدي إلى توفير الثقة في المعاملات الإلكترونية؛ وذلك باستخدام أدوات ووسائل تحويل المعلومات، تهدف إلى إخفاء محتواها والحيلولة دون تعديلها أو استخدامها غير المشروع(١).

ويعرف كذلك بأنه عملية تحويل المعلومات إلى رموز غير مفهومة، تبدو غير ذات معنى بحيث يمنع الأشخاص غير المرخص لهم من الاضطلاع على المعلومة أو فهمها، فعملية التشفير تنطوي على تحويل النصوص العادية أو نصوص مشفرة، ومن المعلوم أن الإنترنت تشكل الوسيط الأضخم لنقل المعلومات(٢).

---

(١) ينظر: المعاملات التجارية والمالية عبر الإنترنت وسبل تأمينها، بركان أمينة، مجلة الاقتصاد الجديد، العدد (٣)، ماي ٢٠١١م، (ص: ١١٠).

(٢) ينظر: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، هدى حامد قشقوش، دار =

ولا بد من نقل المعلومات الحساسة للحركات المالية والتواقيع الإلكترونية بصيغة مشفرة؛ للحفاظ على سلامتها من عبث القراصنة يسمح نظام التشفير بتلافي بعض المخاطر المتوقعة من استخدام الطرق الإلكترونية في المعاملات التجارية، حيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها، فالتشفير يساعد على حفظ سرية المعلومات، والتوقيع الإلكتروني الذي يتطلب الحفاظ على الأرقام والرموز لحمايته داخل التجارة الإلكترونية.

كما أن الغاية من التشفير هي إيجاد وسيلة للمحافظة على سرية البيانات وحمايتها؛ حتى لا يستطيع أي شخص الاطلاع على هذه البيانات دون المتعاقدين أو من يصرح له قانونا بذلك، ويهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات، ومن ثم منع وصولها مشوهة للطرف الآخر في المعاملات التجارية على نحو يعرقلها[١].

وتعتبر الجدران النارية وسيلة لحماية المحتوى تستعمل لحماية الشبكات الخاصة من دخولها، وتمنع الوصول الغير مشروع للشبكة فتحمي وحدات التحكم والإرسال في الإنترنت[٢].

وتتجلى أهمية الجدران النارية في حماية الشبكات الخاصة من هذه المشكلات؛ ذلك أن الإنترنت تعمل على بث متعدد الأطراف باستعمال الأجهزة السمعية والبصرية ومؤتمرات الفيديو المجموعة من المضيفين؛ ليرى ويسمع كل

النهضة العربية، القاهرة طبعة ١٩٩٢م، (ص: ٦١).

(١) ينظر: الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية، علي كحلون، بدون ذكر المطبعة والطبعة (ص: ٢٨٢).

(٢) ينظر: إنشاء جدار ناري لحماية الإنترنت من الاختراق، زينة هلال، مجلة واسط للعلوم الإنسانية، المجلد (١١)، العدد (٣٣)، السنة ٢٠١٦م، (ص: ٢٢١).

منهم الآخر ويوفر الهيكل الإذاعي المتكامل على الإنترنت، عن طريق برنامج يتيح المجال لأي مستعمل آخر للدخول عليه ومراقبته في الإنترنت، ولكن في ظل الجدران النارية يتم توفير الحماية اللازمة للشبكة والمعلومات والحد من تعرضها للأخطار ومتابعة المستخدمين للشبكة ومن يحاول العبث بها، وتسجيل وقائع الاستخدام بدقة طالما أن كل الرسائل والأوامر تمر به عند خروجها إلى الإنترنت أو قدومها منها وتسجيل كافة المعلومات عن حركة المرور والدخول والخروج.

ثانيًا: آلية الحماية التوعوية: تقوم هذه الحماية على رفع وعى المستهلك وتبصيره بحقوقه وواجباته، بما يضبط قراراته ويوجهه إلى ما يحقق له القدر الأكبر من الحماية، حيث تقوم مواقع حماية المستهلك بتقديم خدمات التوعية للمستهلك للوقاية من الوقوع في مخاطر التجارة الإلكترونية، وذلك من خلال منتديات لتبادل الخبرات أون لاين، والقيام بعرض قصص واقعية لتجارب المشترين مع السلع الرديئة، وتحديث مستمر لنشرات إخبارية تتضمن حوادث الغش التجاري مدعمة بآراء الخبراء والمتخصصين، كما توفر هذه المواقع أيضا خدمة استقبال الشكاوى عبر البريد الإلكتروني، من خلال ما يسمى مركز الشكاوى، وتفرد بعض الصفحات التي تحتوي على المعلومات التي تساعد المستهلك على تجنب الوقوع في احتيال أو غش.

وترتبط معظم الاحتيالات في التعاملات التجارية التي تتم عبر الإنترنت بممارسات التضليل والخداع التي تحاكي وتعكس الأنشطة المشابهة التي تحدث باستخدام التقنيات الورقية التقليدية، ويتمتع المحتالون على الإنترنت بالقدرة على الوصول المباشر للملايين من الضحايا في العالم وبأقل تكلفة ممكنة، على سبيل المثال مكائد المكافآت العالية، مثل: مكائد الاحتيال الهرمي **Pyramid scheme** واحتيال **Ponzi** التي تستخدم سلسة خطابات ورسائل إلكترونية،

ومكائد فرص التجارة، ومزادات الاحتيال والجوائز الخادعة والاستثمارات النقدية ببنوك وهمية[١].

استخدام المواقع المرخصة والمقصود بالمواقع المرخصة، تلك المواقع التي تم تقييمها وتأهيلها من قبل طرف ثالث مؤهل بأمور الحماية، وهذه المواقع تكون ممهورة بتوقيع إلكتروني خاص من طرف ثالث مهني متخصص معتمد دوليا، كمعهد المحاسبين القانونيين الأمريكي.

استخدام برنامج أمن للدخول إلى شبكة الإنترنت: من المعروف أن كل جهاز كمبيوتر يحتوي على برنامج خاص للدخول إلى شبكة الإنترنت، وفي الغالب، فإن هذه البرامج تحتوي على آليات معينة تحفظ في ذاكرة الجهاز جميع المعلومات التي تم تداولها في الشبكة من خلاله وفي كثير من الأحيان يستطيع المخترق وعبر الإنترنت الدخول لذاكرة هذا البرنامج والحصول على جميع المعلومات الخاصة بالمستخدم ودون أن يستشعر بذلك، ولهذا ينصح بشراء برنامج خاص يتمتع بحماية عالية لمنع أي مخترق من الدخول إلى ذاكرته.

ثالثا: الحماية الاحترازية[٢]: لا بد من اتخاذ وسائل الحيطة والحذر في تعامل البنوك مع الأنشطة المصرفية التي

---

(١) ينظر: حماية المستهلك في التعاقد الإلكتروني، أسامة أحمد بدر، دار الجامعة الجديدة للنشر، مصر، الطبعة الأولى، ٢٠٠٥م، (ص: ١٠٨).

(٢) ينظر: المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، محمد الألفي، المكتب المصري الحديث القاهرة، ٢٠٠٥م، (ص: ٢٠٣-٢٠٤)، ومشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، محمد محيي الدين عوض، دار الفكر العربي، القاهرة، ٢٠١١م، (ص: ١٥٣-١٥٥)؛ وجرائم المعلوماتية والإنترنت – الجرائم الإلكترونية، عبد الله عبد الله عبد الكريم، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠١١، (ص: ٥٤-٥٥).

تتم عبر الإنترنت؛ نظرًا لأن تركيز غاسلي الأموال يتم على هذه البنوك، وبهذه الأساليب باعتبارها مرتعًا خصبًا لتجارتهم خصوصًا إذا كانت الدول التي ترعى هذه البنوك أو التي في ضيافتها تعاني من عجز في النظام الرقابي العام للدولة.

رابعًا: إصدار القوانين: من خلال اصدار قوانين واضحة وصارمة تلزم جميع المصارف بوضع الخطوات العملية الضرورية لمنع غسل الأموال فيها خاصة تلك الأموال التي يتم التعامل بها عبر الإنترنت.

كذلك ضرورة قيام المصارف بتدابير عملية من شأنها تكشف محاولات غسل الأموال فيها، ومراقبة جميع التعاملات الإلكترونية.

ومن آلية الحماية الاحترازية -أيضًا-: ضرورة قيام المصارف بإنشاء أجهزة أو إدارات تتولى مراقبة ومتابعة البلاغات التي تصلها عن أي عملية أو نشاط مشبوه؛ وبالتالي الإبلاغ عنها للجهات المختصة في الدولة خاصة إن كانت تلك العمليات المصرفية تتعلق بأنشطة تتم عبر الإنترنت.

إضافة إلى ضرورة تدريب المحققين على القيام بالكشف عما تحتويه أجهزة الكمبيوتر من برامج مخزنة عند الضرورة؛ مما ييسر عمليات التفتيش التي تتم على كمبيوتر المتهم.

وضرورة الاستعانة بخبراء في الكمبيوتر والشبكات أثناء عمليات التقصي والتحقيق في الجرائم المعلوماتية والإنترنت.

خامسًا: تفعيل دور حماية الذكاء الاصطناعي: يمكن استخدام الذكاء الاصطناعي للكشف عن التهديدات وغيرها من الأنشطة الضارة المحتملة، لا يمكن للأنظمة التقليدية مواكبة العدد الهائل من البرامج الضارة التي يتم إنشاؤها. يقوم الذكاء الاصطناعي بالتدخل ومعالجة هذه المشكلة، وتقوم شركات الأمن السيبراني بتعليم أنظمة الذكاء الاصطناعي للكشف عن الفيروسات والبرامج الضارة باستخدام خوارزميات معقدة؛ حتى يتمكن الذكاء الاصطناعي من تشغيل

التعرف على الأنماط في البرامج، يتم تدريب أنظمة الذكاء الاصطناعي على تحديد حتى أصغر سلوكيات هجمات الفدية والبرمجيات الخبيثة قبل أن تدخل النظام ثم تعزلهم عن هذا النظام، يمكنها -أيضًا- استخدام الوظائف التنبؤية التي تتجاوز سرعة الأساليب التقليدية(١).

ويسعى الذكاء الاصطناعي بزيادة القدرة على التفكير الفائق وتحليل البيانات، إلى تعزيز القدرات والمساهمات البشرية بشكل كبير، بل قد يتفوق مستقبلًا على الذكاء البشري، ويحدث ثورة كبيرة في تعزيز قوة الأمن السيبراني، ومع تزايد الهجمات الهائلة على المعلومات التي يصعب على فرق الأمن السيبراني ملاحقتها بالدقة المتناهية المطلوبة كان من الضروري استخدام الذكاء الاصطناعي وتطويعه في التصدي لتلك التهديدات؛ لما يتميز به الذكاء الاصطناعي من سرعة هائلة وقدرة فائقة على مراقبة البيانات، والكشف عن القيم المتطرفة التي تشير إلى احتمال وجود اختراقات معلوماتية، مما جعل الذكاء الاصطناعي حليفا لبرامج الأمن السيبراني(٢).

سادسًا: الحماية القانونية: إن مواجهة الجرائم الإلكترونية قد لاقت اهتمامًا عالميًا، فقد عقدت المؤتمرات والندوات المختلفة، وصدرت من خلالها قوانين وتشريعات تجرم مَنْ يقدم على ارتكاب هذه الجرائم، وتعد السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والإنترنت، حيث صدر قانون البيانات السويدي عام ١٩٧٣م، الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على

---

(١) ينظر: الذكاء الاصطناعي وتحديات الأمن السيبراني، جاسم حجي، جريدة أخبار الخليج البحرينية، الأحد ٢٦ أبريل ٢٠٢٠م.

(٢) ينظر: الذكاء الاصطناعي من أجل الصالح العام، هولين جاو، الاتحاد الدولي للاتصالات، ٢٠٢٠م، (ص: ٤).

البيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها، وجاءت الولايات المتحدة الأمريكية بعد السويد حيث شرعت قانونًا خاصًا بحماية أنظمة الحاسب الآلي في الفترة من ١٩٧٦- ١٩٨٥م، وفي عام ١٩٨٥م حدد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية، وهي: جرائم الحاسب الآلي الداخلية، وجرائم الاستخدام غير المشروع عن بعد، وجرائم التلاعب بالحاسب الآلي، ودعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب، وفي عام ١٩٨٦م، صدر قانون تشريعي عرَّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت المتطلبات الدستورية اللازمة التطبيقية، وعلى أثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم، ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي، وقد خولت وزارة العدل الأمريكية في عام ٢٠٠٠م، خمسة جهات منها مكتب التحقيقات الفيدرالية (**fb١**) للتعامل مع جرائم الحاسب الآلي والإنترنت(١).

وحيث إن الجرائم الإلكترونية تميّزت بالعالمية، وبكونها عابرة للحدود، فإن مكافحتها تتحقق بتعاون دولي، وقد أسس «الإنتربول» عدة من مراكز الاتصالات الإقليمية في كل من (طوكيو، ونيوزلندا، ونيروبي، وأذربيجان، وغيرها)؛ لتسهيل مرور الرسائل المختلفة، بالإضافة لقيام المجلس الأوروبي في لكسمبورج عام ١٩٩١م، بإنشاء شرطة أوروبية لملاحقة الجناة في الجرائم العابرة للحدود، ومنها الجرائم المتعلقة بالإنترنت(٢).

---

(١) ينظر: بحوث فقهية في الجريمة المادية والجريمة الإلكترونية، د. إبراهيم عطايا، (ص: ١٤٠، ١٤١).

(٢) ينظر: الجرائم الإلكترونية وطرق الحد منها، تامر علي النويران، (ص: ١٧٨)، بحث مقدم للمؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC- كلية علوم

=

وعلى مستوى الدول العربية نجد أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية، والتي تفرض نوعًا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة التقليدية، ومن ذلك مثلًا أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، كما تم تطويع نصوص قانون حماية الحياة الخاصة، وقانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض الجرائم المعلوماتية، وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية[1].

وفي المملكة العربية السعودية تم إصدار نظام مكافحة جرائم المعلوماتية ١٤٢٨هـ، ويتكون النظام من ست عشرة مادة نصت المواد من الثالثة إلى العاشرة، ثم المادة الثالثة عشر على العقوبات المحددة لأصناف الجرائم المعلوماتية.

بينما نظمت دولة الكويت استخدام وسائل التقنية الحديثة وتجريم الانتهاكات، التي تحدث منها أو عليها بإصدار حزمة من التشريعات كان من بينها:

- القانون رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية.

- والقانون رقم ٩ لسنة ٢٠٠١ بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت، والقوانين المعدلة له.

الحاسب والمعلومات، بجامعة الإمام محمد بن سعود.

(١) ينظر: الجرائم الناشئة عن استخدام الحاسب الآلي، أحمد حسام طه، (ص: ١٠٤)، دار النهضة العربية القاهرة، نقلًا عن: بحوث فقهية في الجريمة المادية والجريمة الإلكترونية، د. إبراهيم عطايا، (ص: ١٤٠، ١٤١).

- القانون رقم ٣ لسنة ٢٠٠٦ بشأن المطبوعات والنشر.
- القانون رقم ٦١ لسنة ٢٠٠٧ بشأن الإعلام المرئي والمسموع.
- القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.
- القانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات.
- قانون مكافحة جرائم تقنية المعلومات رقم ٦٣ لسنة (٢٠١٥)[١].

(١) ينظر: الجرائم الإلكترونية، إعداد اللجنة العلمية، بمعهد الكويت للدراسات القضائية والقانونية، وزارة العدل، دولة الكويت، ٢٠١٨ – ٢٠١٩م، (ص: ٣٥)، وما بعدها.

الخاتمة

أحمد الله رب العالمين، وأصلي وأسلم على نبيه الكريم سيدنا محمد صلى الله عليه وسلم، وعلى آله وصحبه أجمعين، وبعد:

فقد جاء البحث في مقدمة ومبحثين، وانتهى إلى عدة نتائج وهي:

النتائج

١- الجريمة الإلكترونية أصبحت أمرا واقعا، ولها صور عديدة.

٢- لا بد من التحذير والتثقيف والتوعية من الوقوع في فخ الجريمة الإلكترونية.

٣- سن القوانين الرادعة يقلل من مخاطر واحتمال وقوع الجريمة الإلكترونية.

٤- تتعدد صور الجريمة الإلكترونية من استغلال وسرقة وغش واحتيال واختراق وغيرها.

٥- موقف الشريعة الإسلامية واضح ومحدد من كافة أنواع الجرائم أو الاعتداء على الخصوصية والأموال والأعراض.

٦- تبذل معظم الدول الجهود الكافية للحماية من الجريمة الإلكترونية عبر سن القوانين.

التوصيات

١- ضرورة قيام المؤسسات المعنية بالتحذير من وقوع الأشخاص في فخ الجريمة سواء كان جانيًا أم مجنيًا عليه.

٢- نشر ثقافة التعامل الصحيح على الإنترنت ووسائل التكنولوجيا المعاصرة.

٣- نشر أخلاقيات التعامل عبر الإنترنت، وتقوية الوازع الديني والضمير الإنساني السوي.