المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 7 - الإصدار 78
تاريخ النشر: 20 أبريل 2026 م

جريمة الإختراق المالي للمصارف الإلكترونية (معالجة النظام السعودي والضوابط الشرعية)

The crime of financial hacking targeting electronic banks

(Addressing it within the Saudi legal system and Sharia regulations)

إعداد الدكتور/ عبد الله بن إبراهيم المعمر

أستاذ مساعد، قسم القانون، كلية العلوم والدراسات النظرية، الجامعة السعودية الإلكترونية، المملكة العربية السعودية

Email: a.almuammar@seu.edu.sa

الملخص:

هدفت هذه الدراسة إلى التعرف على ماهية جريمة الاختراق المالي للمصارف الإلكترونية وكيفية معالجة النظام السعودي لها وذلك وفقاً لنظام مكافحة جرائم المعلوماتية ونظام الاتصالات. ولتحقيق هذا الهدف، اعتمد الباحث منهجًا وصفيًا استقرائيًا تحليليًا. استكشفت الدراسة الإطار المفاهيمي للجريمة، ووضّحت المفاهيم ذات الصلة، وحدّدت تصنيفها الفقهي والقانوني، وحلّلت الآليات القانونية والأحكام التشريعية المستخدمة لمكافحتها، بالإضافة إلى استعراض الجهود الدولية في مواجهة الجرائم الإلكترونية، وقد تم تناول الموضوع بتقسيمه إلى مبحث تمهيدي وثلاثة مباحث.

خلصت الدراسة إلى أن الاختراق المالي للبنوك الإلكترونية يُشير إلى الوصول غير المصرح به إلى الأنظمة الإلكترونية، أو المواقع الإلكترونية، أو الحسابات المصرفية، أو حسابات الائتمان بأي وسيلة، بما في ذلك استخدام برامج اختراق متخصصة، بهدف الحصول على بيانات العملاء السرية واستغلالها في عمليات احتيال أو أنشطة غير مشروعة أخرى. ويشمل ذلك أيضًا التحويل غير القانوني للأموال من حساب إلى آخر بغرض الحصول على أموال بطريقة غير مشروعة أو سرقة المعلومات المالية. وأظهرت النتائج كذلك أن القانون السعودي يُجرّم الوصول غير المصرح به والاختراق، لا سيما عندما يُرتكب بهدف الاستيلاء على الأموال أو الوصول إلى بيانات البنوك وبطاقات الائتمان. ولذلك، يُمكن تطبيق الإطار القانوني السعودي الحالي على الأفعال التي تُشكّل جريمة الاختراق المالي للبنوك الإلكترونية، بما في ذلك التحويلات المالية غير المشروعة.

كما أكدت الدراسة على ضرورة وجود إطار قانوني شامل وواضح يُنظّم هذه الجريمة تحديدًا. ويجب أن يُحدّد هذا الإطار طبيعتها القانونية بوضوح، ويُبيّن عناصرها، ويُحدّد الأفعال التي تُشكّل عنصرها المادي، وينص على عقوبات مناسبة. بالإضافة إلى ذلك، أكدت الدراسة على أهمية وضع قواعد إجرائية حديثة تحكم التحقيق والملاحقة القضائية والتفتيش والفحص الفني في قضايا الجرائم الإلكترونية، وذلك لمواكبة التطورات التكنولوجية والطبيعة الخاصة للأدلة الرقمية. كما سلطت الضوء على ضرورة تنظيم اختصاصات الأفراد والسلطات المسؤولة عن التوقيف والتحقيق وإنفاذ القانون فيما يتعلق بهذا النوع الناشئ من الجرائم.

الكلمات المفتاحية: الإختراق المالي، المصارف الإلكترونية، النظام السعودي، الضوابط الشرعية

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 7 - الإصدار 78
تاريخ النشر: 20 أبريل 2026 م

The crime of financial hacking targeting electronic banks (Addressing it within the Saudi legal system and Sharia regulations)

Dr. Abdullah bin Ibrahim Al-Muammar

Assistant Professor, Department of Law, College of Science and Theoretical Studies, Saudi Electronic University, Saudi Arabia

Abstract:

This study aimed to identify the nature of the financial hacking crime targeting electronic banks and how the Saudi system addresses it, in accordance with the Anti-Cybercrime Law and the Telecommunications Law. To achieve this objective, the researcher adopted a descriptive, inductive, and analytical approach. The study explored the conceptual framework of the crime, clarified its related concepts, identified its jurisprudential and legal classification, and analyzed the legal mechanisms and statutory provisions used to combat it, in addition to reviewing international efforts in confronting cybercrime. The study was divided into a preliminary section and three main sections. The study concluded that financial hacking of electronic banks refers to unauthorized access to electronic systems, websites, bank accounts, or credit accounts by any means, including the use of specialized hacking software, in order to obtain confidential customer data and exploit it in fraud or other unlawful activities. It also includes the illegal transfer of funds from one account to another for the purpose of unlawfully obtaining money or stealing financial information. The findings further showed that Saudi law criminalizes unauthorized access and hacking, especially when committed to seize funds or gain access to banking and credit card data. Therefore, the current Saudi legal framework can be applied to conduct constituting the crime of financial hacking of electronic banks, including illegal fund transfers. The study also stressed the need for a comprehensive and explicit legal framework specifically regulating this crime. Such regulation should clearly define its legal nature, identify its constituent elements, determine the acts forming its material element, and prescribe appropriate penalties. In addition, the study emphasized the importance of developing modern procedural rules governing investigation, prosecution, inspection, and technical examination in cybercrime cases, in order to keep pace with technological developments and the special nature of digital evidence. It also highlighted the need to regulate the competence of the individuals and authorities responsible for arrest, investigation, and enforcement in relation to this emerging form of crime.

Keywords: Financial Hacking, Electronic Banks, Saudi Legal System, Sharia Regulations

1. المقدمة:

شهد العالم تطوراً ملحوظاً ومستمراً في مختلف القطاعات وخاصة المجال الاقتصادي والذي يعتبر قطاعاً حيوياً، حيث ظهر الاقتصاد الرقمي وتبعه ظهور المصارف الإلكترونية والتجارة الإلكترونية الأمر الذي استوجب استحداث العديد من الأدوات الإلكترونية (مشري، رياض، لمزاودة، قاجة، د.ت، ص. 2)، حيث تعد التطورات التي شهدها العالم في الحقبة الأخيرة وعلى رأسها التقدم التكنولوجي من أهم التغيرات التي ساهمت في إحداث تحول جذري في الأنماط الخاصة بالعمل المصرفي في عصر العولمة، فقد عملت البنوك على تطوير الخدمات الخاصة بها وابتكار خدمات مصرفية مستحدثة، وذلك من خلال استخدام شبكات الإتصال الإلكترونية لإجراء العمليات المصرفية وبهدف تمكين العميل من الحصول على الخدمات المطلوبة في أي وقت وأي مكان وكذلك مواكبة التزايد الكبير في حجم المعاملات المالية (شناف وبودربالة، 2022/2021، ص. 1)، ويعتبر العمل المصرفي الالكتروني من الأمور التي أفرزها التقدم التكنولوجي الهائل في مجال الاتصالات، فالمعاملات المصرفية الإلكترونية وفرت العديد من المزايا بالنسبة للعملاء وظهور فرص جديدة لأعمال البنوك وتوزيع واسع الانتشار إلا أنه بالرغم من المزايا العديدة التي وفرتها تلك المعاملات، إلا أنها في نفس الوقت تواجه العديد من المخاطر تميزها عن مخاطر البنوك التقليدية غير الإلكترونية، والتي أثارت الخوف والقلق لدى المصرفيين والسلطات الإشرافية حيث أن الجريمة لم تكن بمنأى عن التطور التكنولوجي، فقد تزايدت مخاطر التعرض للاختراقات الأمنية التي تستهدف الحسابات البنكية كما أصبحت قضايا اختراق الحسابات وجرائم الإختراق المالي للمصارف الإلكترونية من التحديات الأمنية التي تواجه الأفراد والمؤسسات في المملكة العربية السعودية، وظهرت العديد من الجرائم المستحدثة والتي يطلق عليها الجرائم الإلكترونية أو الجرائم المعلوماتية فهناك ارتباط وثيق بين العمليات الإلكترونية وأمن المعلومات والذي قد يؤدي إلى العبث في البيانات والأرصدة الخاصة بالعملاء (الشبول، 2023، ص. 51–52؛ الحاج، 2014/2013، ص. 1)، الأمر الذي يتطلب تبنى إدارة مخاطر شاملة لتحديد هوية هذه التحديات والمخاطر واستحداث الطرق والوسائل العديدة للوقاية منها، وكذلك وضع العديد من الأحكام والقواعد والأنظمة لمكافحة تلك الجرائم، وفي إطار ما تقدم تسعى هذه الدراسة للبحث في جريمة الإختراق المالي للمصارف الإلكترونية من حيث بيان الإطار المفاهيمي لتلك الجريمة والبحث في الأركان الخاصة بتلك الجريمة والوقوف على الآليات النظامية والجهود الدولية لمكافحة تلك الجريمة.

1.1. مشكلة الدراسة:

تثير الدراسة العديد من الإشكاليات التي تكمن في المخاطر التي أفرزها التطور التكنولوجي الهائل في مجال الاتصالات والعمل المصرفي الالكتروني، فبالرغم من المزايا العديدة التي وفرتها التكنولوجيا إلا أنها أدت إلى ظهور العديد من المخاطر التي ترتبط بأمن المعلومات والتي تحول دون تحقيق أهدافها، ونظراً لتزايد استخدام الحاسبات فقد نشبت الحروب الإلكترونية وهي حروب من نوع جديد تنتهك سرية المعلومات وتستهدف أمن المعلومات ولعل أخطر ما أفرزته تلك الحروب جريمة الاختراق حيث تمكن إشكالية موضوع الدراسة في مدى كفاية النصوص الحالية لمواجهة هذه الجريمة، وذلك بالنظر إلى كونها عملية تتم من أي مكان بالعالم وذلك دون أهمية لوجود الشخص المخترق في نفس المكان الذي يتم فيه الاختراق، بالإضافة إلى التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي، والتطور الهائل الذي تشهده التقنية الأمر الذي لا تزال نسبة كبيرة من الاختراقات لم تكتشف، وهو ما يؤدي إلى أخطاراً مضاعفة فالمجني عليه لا يشعر بالاختراق ولا يكاد يكتشفه إلا إذا وقع ضرر جراء حدوثه وبالنظر إلى ما تتمتع به الدول العربية ودول الخليج على وجه الخصوص من طفرة في مجال الحاسبات، فقد أصبحت موطناً لارتكاب هذه الجريمة الأمر الذي يستلزم استحداث أساليب وآليات جديدة ونظم رقابة فعالة للحد من ارتكاب تلك الجريمة، والعمل على مواجهتها بالعديد من الأساليب التي تتناسب مع التطور السريع لهذا النوع من الجرائم، وذلك بالنظر إلى قلة الدراسات التي تناولت هذا الموضوع حيث تناولت العديد من الدراسات هذه

الجرائم ولكن بشكل غير مباشر وهذا ما تشير إليه في الدراسات السابقة.

2.1. تساؤلات الدراسة:

يرتكز البحث حول الإجابة على التساؤل الرئيسي والذي يتمثل في ماهية جريمة الإختراق المالي للمصارف الإلكترونية وكيفية معالجة النظام السعودي لتلك الجريمة؟

ويتفرع الإجابة عن هذا التساؤل الرئيسي الإجابة على مجموعة من التساؤلات الفرعية، والتي يمكن صياغتها على النحو التالي:

1. ما هو الإطار المفاهيمي لجريمة الإختراق المالي للمصارف الإلكترونية؟
2. ما هو التأصيل الفقهي والنظامي لجريمة الإختراق المالي للمصارف الإلكترونية؟
3. ما هي أركان جريمة الإختراق المالي للمصارف الإلكترونية؟
4. ما هي آليات مكافحة جريمة الإختراق المالي للمصارف الإلكترونية؟

3.1. أهمية الدراسة:

يمكن إبراز أهمية الدراسة من الناحيتين النظرية والعملية، حيث تظهر الأهمية النظرية من خلال بيان التأصيل الفقهي والنظامي لجريمة الإختراق المالي للمصارف الإلكترونية، حيث تعتبر جريمة الاختراق المالي للمصارف الإلكترونية من الجرائم المستحدثة والتي ظهرت مع التقدم التكنولوجي في كافة المجالات، كما أنها تعكس السلوك السلبي الإنساني وتعتبر مظهراً سلبياً من مظاهر المجتمع يتطلب البحث في تكييفها من الناحية الفقهية والقانونية للوصول إلى الوصف الصحيح لتلك الجريمة، وتحقيق الحماية القانونية اللازمة لها.

كما تظهر الأهمية العملية فيما يثيره موضوع الإختراق المالي للمصارف الإلكترونية من إشكاليات عملية في المملكة العربية السعودية، وكيفية معالجة النظام السعودي لجريمة الإختراق المالي لتلك المصارف، وتسليط الضوء على النصوص القانونية ومدى كفايتها لمواجهة هذا النوع من الجرائم، وكذلك المساهمة في إبراز أهمية التصدي التشريعي لتلك الجريمة، وبيان أحدث طرق ووسائل المواجهة وكذلك الآليات النظامية والجهود الدولية لمكافحة جريمة الإختراق المالي للمصارف الإلكترونية.

4.1. أهداف الدراسة:

تهدف الدراسة إلى ما يلي:

1. بيان وتحديد المفاهيم الأساسية لجريمة الإختراق المالي للمصارف الإلكترونية.
2. تحديد أسباب ودوافع ارتكاب جريمة الاختراق المالي للمصارف الإلكترونية.
3. بيان خصائص جريمة الاختراق المالي للمصارف الإلكترونية.
4. البحث في التكييف الفقهي والنظامي لجريمة الإختراق المالي للمصارف الإلكترونية.
5. الوقوف على الركن المفترض لجريمة الإختراق المالي للمصارف الإلكترونية.
6. تحديد الركن المادي والمعنوي لجريمة الإختراق المالي للمصارف الإلكترونية.
7. بيان الآليات النظامية لمكافحة جريمة الإختراق المالي للمصارف الإلكترونية.
8. الوقوف على الآليات والجهود الدولية لمكافحة الجرائم المعلوماتية.
9. معالجة مشكلة الدراسة والبحث في مدى كفاية النصوص النظامية لمواجهة هذا النوع من الجرائم.

5.1. منهج الدراسة:

اعتمد الباحث في بيان أهداف الدراسة وتحقيق النتائج المرجوة منها على المنهج الوصفي والمنهج الاستقرائي التحليلي، حيث اعتمد على المنهج الوصفي في بيان الإطار المفاهيمي لجريمة الإختراق المالي للمصارف الإلكترونية وتحديد المفاهيم الأساسية المرتبطة بها بالإضافة إلى تحديد خصائص جريمة الإختراق المالي للمصارف الإلكترونية والوقوف على دوافع ارتكاب تلك الجريمة.

كما اعتمد على المنهج الاستقرائي التحليلي في استنباط واستقراء الأسس الفقهية والنظامية للوقوف على التكييف الفقهي والقانوني لجريمة الإختراق المالي للمصارف الإلكترونية، وتحليل النصوص القانونية لبيان وتحديد أركان جريمة الإختراق المالي للمصارف الإلكترونية، والوقوف على الركن المفترض لهذه الجريمة، بالإضافة إلى بيان الآليات والنصوص النظامية لمواجهة هذه الجريمة، والجهود الدولية لمكافحة الجرائم المعلوماتية، وتحديد مدى كفاية تلك النصوص لمواجهة هذا النوع من الجرائم المستحدثة ومدى كفايتها في تحقيق الردع وتحقيق الرقابة اللازمة للحد من ارتكاب تلك الجرائم.

6.1. حدود الدراسة:

تعتمد حدود الدراسة بشكل رئيسي على المملكة العربية السعودية، وذلك من خلال توضيح الإطار المفاهيمي لجريمة الإختراق المالي للمصارف الإلكترونية، وتحديد المفاهيم الأساسية المرتبطة بها، وبيان التأصيل الفقهي والنظامي لتلك الجريمة، وتحديد أركانها والبحث في أساليب وآليات مواجهتها في الأنظمة السعودية، وذلك في نطاق تطبيق أحكام نظام مكافحة جرائم المعلوماتية ونظام الاتصالات والوقوف على مدى كفاية تلك النصوص لمواجهة هذا النوع من الجرائم.

2. الدراسات السابقة:

في إطار البحث في موضوع جريمة الإختراق المالي للمصارف الإلكترونية تجدر الإشارة إلى العديد من الدراسات التي تناولت هذا النوع من الجرائم وذلك على النحو التالي:

دراسة عمايره، محمد منذر. (2023م/1445هـ) بعنوان: "التعاون الدولي في مواجهة الجريمة الإلكترونية"

حيث قسم الباحث دراسته إلى قسمين تناول في القسم الأول الجريمة الإلكترونية بشكل عام مع التطبيق على التشريع الفلسطيني، حيث تناول الباحث ماهية التعاون الدولي في مجال مواجهة الجريمة الإلكترونية، من حيث بيان المفهوم العام للجريمة الإلكترونية في التشريع الفلسطيني والمفهوم العام للتعاون الدولي في مجال الجريمة الإلكترونية، كما تناول الباحث في القسم الثاني أشكال التعاون الدولي وصعوباته في مواجهة الجريمة الإلكترونية بالشرح والتفصيل وذلك من حيث بيان أوجه التعاون الدولي في مواجهة الجريمة الإلكترونية، وتوضيح التعاون الأمني والقضائي كما تناول الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الإلكترونية، وقد خلصت الدراسة إلى ضرورة حث المشرع الفلسطيني لتعديل قانون مكافحة الجرائم الإلكترونية حتى يتواكب مع كل ما هو جديد في هذا المجال وبما يتوافق مع الاتفاقات الدولية التي وقعت عليها دولة فلسطين.

2- دراسة فشي، فرفي، ورملي، (2018). بعنوان: "البنوك الإلكترونية مخاطرها وطرق الحماية منها- مع الإشارة إلى حالة الجزائر"

حيث قسم الباحث دراسته إلى ثلاثة محاور تناول في المحور الأول ماهية البنوك الإلكترونية من خلال البحث في تعريفها وتطورها التاريخي وبيان أهميتها ومميزاتها كما تطرق في المحور الثاني إلى البحث في مخاطر البنوك الإلكترونية، وطرق الرقابة والحماية للحد من تلك المخاطر أما المحور الثالث فقد تناول الباحث التطبيق العملي وعرض تجربة الجزائر في هذا المجال، وذلك من خلال التعرض إلى واقع المعاملات البنكية في الجزائر وكذلك بيان الطرق القانونية للحماية من مخاطرها حيث توصلت الدراسة إلى أن

تطوير نظام الصيرفة الإلكترونية في الجزائر يقتضي الالتزام بالعديد من العوامل منها تطوير البنية التحتية للاتصالات للدولة ومختلف القطاعات والتحكم بتقنية المعلومات وكذلك العمل على سلامة سياسات السوق الاتصالي وغير ذلك من العوامل التي تعتبر بمثابة قواعد للعمل الالكتروني.

3- دراسة الحاج (2013-2014). بعنوان: "مخاطر العمليات المصرفية الإلكترونية – دراسة مقارنة".

قسم الباحث دراسته إلى قسمين بواقع مبحثين تناول في المبحث الأول الإطار القانوني للعمل المصرفي من حيث بيان وتوضيح ماهية العمليات المصرفية الإلكترونية، والبحث في الأهمية العملية والاقتصادية للمعاملات المصرفية الإلكترونية، كما تناول التكييف القانوني للعمل المصرفي الالكتروني وتوضيح الأسس القانونية للعمليات المصرفية الإلكترونية والأسس المحاسبية التي تطبق عليها، وكذلك موقف المشرع الجزائري من العمليات المصرفية الإلكترونية، أما فيما يتعلق بالمبحث الثاني فقد تناول الباحث إدارة المخاطر المصرفية، وذلك من حيث بيان أنواع المخاطر المصرفية والبحث في مخاطر العمليات المصرفية الإلكترونية وكذلك مبادئ إدارة المخاطر المصرفية ورقابتها حيث خلصت الدراسة إلى أن " عدم قدرة تشريعات الكثير من البلدان العربية والتي منها الجزائر مسايرة التطورات الحديثة يؤثر على قدرة البنوك على الاستمرار في ظل المنافسة الشديدة التي يشهدها القطاع البنكي وخصوصا بعد تحرير السوق البنكية مما يؤثر كذلك في ثقة العملاء تجاه المنظومة التشريعية من جهة قدرتها على حمايتهم من الأخطار الناجمة عن التعامل مع البنوك مما يؤدي إلى عزوفهم عن التعامل مع البنوك وبالتالي الإضرار بالاقتصاد الوطني".

4- دراسة القاسمي (2018). بعنوان: "جرائم الدخول غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون اتحادي رقم (5) لسنة (2012) في شأن مكافحة جرائم تقنية المعلومات)"

حيث قسم الباحث دراسته إلى قسمين تناول في القسم الأول البنيان القانوني لجرائم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية، من حيث بيان أركان جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة، وكذلك أركان جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية، بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية بينما تناول الباحث في القسم الثاني بيان العقوبات والتدابير المقررة لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية، حيث تناول بالشرح والتفصيل العقوبات المقررة لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية في صورتها المجردة كما تناول العقوبات المقررة لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، بالإضافة إلى ما أشار إليه الباحث وتضمنه من بيان التدابير المقررة لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات الإلكترونية، وقد خلصت الدراسة إلى أن المشرع قد شدد العقوبة الخاصة بجريمة الدخول غير المشروع بقصد الحصول على بيانات حكومية أو معلومات سرية تتعلق بمنشآت مالية أو تجارية أو اقتصادية وذلك من جنحة يعاقب عليها بالحبس والغرامة إلى جناية يعاقب عليها بالسجن المؤقت والغرامة وذلك لأهمية المعلومات السرية الخاصة بالمنشآت المالية أو التجارية أو الاقتصادية وأهمية البيانات الحكومية وتعلقهما بالاقتصاد القومي أو الأمن القومي أو المصالح العليا للدولة.

5- دراسة العنزي (2022م). بعنوان: "معاينة الجانب الموضوعي الإحتيال من خلال المواقع المواقع الإلكترونية في النظام السعودي مقارناً بالقانونين المصري والكويتي.

تناول الباحث في هذه الدراسة ماهية الاحتيال المالي من خلال المواقع الإلكترونية، من خلال توضيح التعريف بالاحتيال من خلال المواقع الإلكترونية في القسم الأول من البحث وبيان أوجه الشبه والاختلاف بين جريمة الاحتيال المالي والاحتيال التقليدي وبيان المشكلات التي تثيرها جريمة الاحتيال من خلال المواقع الإلكترونية وبيان صورها ثم تناول في القسم الثاني بيان أركان جريمة

الاحتيال من خلال المواقع الإلكترونية، والعقوبة المقررة لتلك الجريمة، وقد توصل الباحث إلى تزايد جرائم الاحتيال بشكل يومي وذلك من خلال المواقع الإلكترونية بسبب تنوع الطرق الاحتيالية التي يلجأ إليها الجناة مستغلين بذلك صعوبة الوصول إليهم والتطور والتقدم التكنولوجي الحاصل الأمر الذي يستوجب تتضافر الجهود لمواجهة تلك الجريمة.

6- دراسة الطويلي (2019م). بعنوان: "التكييف الفقهي والقانوني لجريمة السرقة الإلكترونية (البطاقة الائتمانية نموذجاً للتطبيق).

قسم الباحث دراسته إلى ثلاثة مباحث، حيث تناول في المبحث الأول التعريف بالسرقة عموماً والسرقة الإلكترونية خصوصاً، من حيث التعريف بالبطاقة الائتمانية ومزاياها وبيان التكييف الفقهي والقانوني، كما تناول الباحث في المبحث الثاني تكييف جريمة سرقة البطاقة الائتمانية بالشرح والتوضيح، من حيث بيان المقصود بها والتكييف الفقهي والقانوني لها، أما فيما يتعلق بالمبحث الثالث فقد تناول الباحث توضيح الحماية الجزائية لبطاقة الصراف الآلي في الشريعة الاسلامية والقوانين العربية والاتفاقيات الدولية، وقد خلص الباحث في دراسته إلى أنه في حالة عدم وجود نصوص خاصة بتنظيم جريمة السرقة الإلكترونية عموما وجريمة سرقة بطاقة الائتمان خصوصا فإن النصوص العامة الواردة في الشريعة الاسلامية بشأن جريمة السرقة تكون كافية لتنظيم ذلك.

7- دراسة شناف (2022/2021). بعنوان: "الخدمات الإلكترونية للبنوك-أخطارها وطرق الحماية منها -دراسة حالة المؤسسة العربية المصرفية (ABC) الأردن.

قسم الباحث دراسته إلى ثلاثة أقسام تناول في القسم الأول عميات حول البنوك من حيث بيان ماهيتها ووظائفها وأهميتها، ثم تناول في القسم الثاني الخدمات الإلكترونية للبنوك وذلك من حيث بيان البنوك الإلكترونية بالشرح والتفصيل وذلك من خلال توضيح المفهوم الخاص بها والمتطلبات المتعلقة بها، وبيان المزايا والتحديات التي تواجهها البنوك الإلكترونية، أما فيما يتعلق بالقسم الثالث فقد تطرق الباحث إلى الدراسة التطبيقية والتي تضمن فيها حالة المؤسسة العربية المصرفية (ABC) الأردن وقد توصل الباحث إلى عدة نتائج في دراسته ومنها، ضرورة العمل باستمرار على تطوير إستراتيجية تأهيل الموارد البشرية حتى تكون مستمدة من مفهوم جديد ومتطور بهدف تعزيز الكفاءة الادارية والانتاجية وكذلك توفير موارد بشرية مؤهلة مع التركيز على تنويع النشاط التدريبي وذلك حتى يكون منسجماً مع متطلبات العمل المصرفي الحديث.

2.2. التعليق على الدراسة:

بالنظر إلى الدراسات السابقة نجد أنها لم تتناول في أغلبها جريمة الاختراق المالي للمصارف الالكتروني في المملكة العربية السعودية بشكل مباشر فالبعض منها قد تناول المصارف الإلكترونية والبعض أشار إلى المخاطر التي تتعرض لها ومنها، الإحتيال المالي والمخاطر التي تتعلق بانتهاك سرية البيانات وأمن المعلومات، وأشار البعض الآخر إلى الجريمة ولكن بشكل غير مباشر وذلك من خلال الإشارة بوجه عام إلى الجرائم المعلوماتية ومنها الجرائم التي تتعلق بالمصارف الإلكترونية، والبعض الآخر من الدراسة تتناول الجوانب المتعلقة بجريمة الدخول غير المشروع بوجه عام دون تخصص في جريمة الاختراق التي تتعلق بالمصارف الإلكترونية، وبالإضافة إلى ما تقدم فقد أشارت بعض الدراسات إلى الجريمة ولكن دون معالجتها في النظام السعودي، كما أن هناك مراجع تناولت الجانب الموضوعي للاحتيال عبر المواقع الإلكترونية إلا أنها لم تتطرق بشكل متخصص لجريمة الاختراق المالي للمصارف الإلكترونية، وقد تميزت هذه الدراسة عن الدراسات السابقة في كونها تعتبر دراسة متخصصة في موضوع جريمة الاختراق المالي للمصارف الإلكترونية حيث جاءت شاملة للمفاهيم الخاصة بالجريمة والمفاهيم المتعلقة بالمصارف الإلكترونية، كما جاءت شاملة للأركان الخاصة بها، فضلاً عن معالجتها لتلك الجريمة في إطار الأنظمة الصادرة في المملكة العربية السعودية مع الإشارة إلى الجهود والآليات الدولية الخاصة بمكافحة هذا النوع من الجرائم.

3. تقسيم الدراسة

المبحث التمهيدي: الإطار المفاهيمي لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الأول: المفاهيم الأساسية لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الثاني: خصائص جريمة الإختراق المالي للمصارف الإلكترونية ودوافع ارتكابها

المبحث الأول: التأصيل الفقهي والنظامي لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الأول: التأصيل الفقهي لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الثاني: التأصيل النظامي لجريمة الإختراق المالي للمصارف الإلكترونية

المبحث الثاني: أركان جريمة الإختراق المالي للمصارف الإلكترونية:

المطلب الأول: الركن المفترض لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الثاني: الركن المادي لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الثالث: الركن المعنوي لجريمة الإختراق المالي للمصارف الإلكترونية

المبحث الثالث: آليات مكافحة جريمة الإختراق المالي للمصارف الإلكترونية

المطلب الأول: الآليات النظامية لمكافحة جريمة الإختراق المالي للمصارف الإلكترونية

المطلب الثاني: الآليات والجهود الدولية لمكافحة الجرائم المعلوماتية

المبحث التمهيدي: الإطار المفاهيمي لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الأول: المفاهيم الأساسية لجريمة الإختراق المالي للمصارف الإلكترونية

لتوضيح مفهوم جريمة الإختراق المالي للمصارف الإلكترونية لغة واصطلاحاً، ينبغي تقسيم هذا المطلب إلى فرعين نعرض في أولهما تعريف جريمة الإختراق المالي للمصارف الإلكترونية لغة، ونتناول في الثاني جريمة الإختراق المالي للمصارف الإلكترونية اصطلاحاً وذلك على النحو التالي:

الفرع الأول: تعريف جريمة الإختراق المالي للمصارف الإلكترونية لغة.

أولاً: تعريف الجريمة لغة.

الجرم في اللغة هو القطع، ومما يرد إليه قولهم جرم، أي كسب وذلك لأن الذي يحوزه فكأنه اقتطعه، ومنه فلان جريمة أهله بمعنى كاسبهم، والجرم والجريمة الذنب وهو من الأول وذلك لأنه كسب والكسب هو اقتطاع ومنه قوله تعالى﴿ وَلَا يَجْرِمَنَّكُمْ شَنَآنُ قَوْمٍ عَلَى أَلَّا تَعْدِلُوا ﴾(سورة المائدة، الآية 8)، أي لا يحملنكم ولا يكسبنكم بغض قوم على مخالفة أحكام الله تعالى، وقوله تعالى﴿لَا يَجْرِمَنَّكُمْ شِقَاقِي أَنْ يُصِيبَكُمْ مِثْلُ مَا أَصَابَ قَوْمَ نُوحٍ أَوْ قَوْمَ هُودٍ أَوْ قَوْمَ صَالِحٍ وَمَا قَوْمُ لُوطٍ مِنْكُمْ بِبَعِيدٍ ﴾(سورة هود، الآية 89)، أي لا يحملنكم خلافي وبغضي على تكذيبي، وقالوا في قولهم لا جرم هو من قولهم جرّمت وذلك بمعنى كسبت ومنه قوله تعالى﴿ لَا جَرَمَ أَنَّ لَهُمُ النَّارَ﴾ (سورة النحل، الآية 62)، فقيل جرم بمعنى كسب وقيل أيضا حقّ ووجب، ومنه أيضاً جرم الشيء أي قطعه، وأجرم بمعنى أذنب، والجريمة لغة الذنب والجمع جرائم (رضا، 1958، ص. 515؛ الطناحي، 2008، ص. 230–231؛ ابن فارس، 1979، ج1، ص. 445–446).

ثانياً: تعريف الإختراق لغة.

الخاء والراء والقاف أصل واحد، وذلك بمعنى مزق الشيء، وخرق يخرق خرقاً فهو خرق وأخرق ويقال خرقت الأرض بمعنى جبتها، واخترقت الأرض، وذلك إذا جابتها، والخرق المفازة، وذلك لأن الرياح تخترقها، والخرق هو نقيض الرفق، كأن الذي يفعله مخترق، والمخترق هو الموضع الذي يخترقه الرياح، ومنه قوله تعالى﴿ وَلَا تَمْشِ فِي الْأَرْضِ مَرَحًا إِنَّكَ لَنْ تَخْرِقَ الْأَرْضَ وَلَنْ تَبْلُغَ الْجِبَالَ طُولًا﴾(سورة الإسراء، الآية 37)، وقوله تعالى ﴿ وَجَعَلُوا لِلَّهِ شُرَكَاءَ الْجِنَّ وَخَلَقَهُمْ وَخَرَقُوا لَهُ بَنِينَ وَبَنَاتٍ بِغَيْرِ عِلْمٍ سُبْحَانَهُ وَتَعَالَى عَمَّا يَصِفُونَ﴾(سورة الأنعام، الآية 100)، ويقال مررت بخريق من الأرض بين مسحاوين وهي التي تّسعت واتسع نباتها، أي مزقه وخرق الاتفاق أي خالفه ونقضه وخرق الحصار بمعنى نفذ منه ومرّ من خلاله ومنه اخترق يخترق اختراقاً فهو مخترق، واخترق الصفوف أي خرقها ونفذ منها واخترق الجيش الحصار بمعنى خرقه ونفذ منه، واخترق العدو الحدود أي عبرها مهاجماً وخرق القانون هو الخروج عنه وعدم احترامه، واختراق هو مصدر اخترق وذلك بمعنى خاصية النفوذ وإمكان الخرق وقيل " أحسن وسيلة للتغلب على الصعاب اختراقها"، ومعنى اختراق هو تجاوز حاجز أو معيق والتغلب عليه والاختراق هو هجوم يخترق مناطق العدو أو جبهة عسكرية (ابن فارس، 1979، ج2، ص. 172–173؛ عمر، 2008، ص. 634–635).

ثالثاً: تعريف المال لغة.

الميم والواو واللام كلمة واحدة، وتمول الرجل، بمعنى اتخذ مالاً، ومنه مال يمال أي كثر ماله، والمال هو كل ما يملكه الفرد، أو ما تملكه الجماع من عروض التجارة، أو المتاع أو النقود أو العقار قل أو كثر ماله، وتوظيف المال، هو استثماره والمال المنقول، هو الشيء المملوك الذي يمكن نقله كالاثاث أو البضائع أو السيارات، والمال غير المنقول، هو الشيء المملوك الذي لا يمكن نقله من العقارات والأبنية، ورأس المال هو جملة المال المستثمر في عمل ما، كما يقابلها الدخل الذي ينتج منها، والأوراق المالية فهي الورق النقدي (ابن فارس، 1979، ج5، ص. 285؛ عمر، 2008، ص. 2139–2140)

رابعاً: تعريف للمصارف الإلكترونية لغة.

الصاد والراء والفاء، يدل على رجع الشيء في معظم بابه، ومنه صرفت القوم صرفاً وانصرفوا، بمعنى رجعتهم فرجعوا، وقيل الصرف، هو فضل الدرهم على الدرهم في القيمة، ومعنى الصرف، هو أن شيء صرف إلى شيء، كأن الدينار صرف إلى الدراهم، وذلك بمعنى رجع إليها إذا أخذت بدله، ومنه اسم الصيرفي، وذلك لتصريفه أحدهما إلى الآخر، وهو اسم منسوب إلى صيرف وصراف، وهو من يبدل نقداً بنقد، أو هو المستأمن على أموال الخزانة يقبض ويصرف ما يستحق، وصيرفة هي مهنة صرف العملات، وهي تبديل عملة وطنية بعملة أجنبية أو العكس، ومصرف مفرد مصارف، وهو اسم مكان من صرف، وهو مهرب أو ملجأ، والمصرف المركزي، هو مؤسسة رسمية تتولى إصدار النقد والرقابة على النشاط المالي للدولة، وكذلك الإشراف على المصارف الأخرى، ومصرفي، هو اسم منسوب إلى مصرف، وصاحب بنك، والبنك هو المنشأة التي تقوم بعمليات الإئتمان كتقديم القروض وقبول الودائع، وتسهيل عمليات الدفع، وإصدار النقود، والحساب المصرفي هو الأموال التي يتم إيداعها في أحد المصارف وتكون قابلة للسحب من قبل المودع (ابن فارس، 1979، ج3، ص. 342–343؛ عمر، 2008، ص. 1291–1292).

الفرع الثاني: جريمة الإختراق المالي للمصارف الإلكترونية اصطلاحاً

لتوضيح مفهوم جريمة الإختراق المالي للمصارف الإلكترونية اصطلاحاً، لابد من تعريف جريمة الإختراق اصطلاحاً، وتعريف المصارف الإلكترونية اصطلاحاً، وصولاً إلى تعريف جريمة الإختراق المالي للمصارف الإلكترونية، وذلك على النحو التالي:

أولاً: تعريف جريمة الإختراق اصطلاحاً.

يمكن التعبير عن الجريمة بأنها "كل فعل غير مشروع صادر عن إرادة جنائية يقرر له الشارع جزاءً جنائياً، وذلك بالنظر لما يشكله هذا الفعل من مساس بمصلحة قانونية محمية يعرضها لخطر أو يصيبها بضرر" (حسني، 1962، ص.35–36؛ محمد، 2016، ص. 93).

فالجريمة تعبر عن السلوكيات السلبية للشخص، حيث تعرف بأنها انحراف الإنسان عن الطبيعة الإيجابية الخاصة به، والإنتقال إلى طبيعة سلبية، بسبب العديد من العوامل المختلفة، والتي يعد من أهمها طبيعة البيئة التي يعيش فيها الإنسان والتي يتأثر بها ويؤثر فيها، فالجريمة التقليدية تختلف عن المستحدثة، وذلك من حيث الأدوات والتي تكون عادة برامج معينة كما أن الشبكة الإلكترونية تكون مسرحاً للجريمة المستحدثة.

أما فيما يتعلق بالإختراق فيعبر عنه بالقدرة على الدخول للحاسب الآلى أو إلى أي جزء منه، ويعرف بأنه محاولة الدخول إلى الجهاز المشترك في شبكة الإنترنت، وذلك من قبل شخص لا يحق له الدخول إلى الجهاز أو تلك الشبكة، بغرض الاطلاع على المعلومات أو البيانات أو تدمير تلك البيانات أو القيام بزرع فيروسات، وغالباً ما يكون الإختراق باستخدام برامج متخصصة لاختراق المواقع، كما يشبه جانب من الفقه الجنائي الفرنسي عملية الإختراق أو الدخول غير المشروع إلى نظام الحاسوب أو الموقع الإلكتروني باختراق ذاكرة الإنسان (عياش، 2024، ص. 94–95؛ العنزي، 2022، ص. 7).

ويرى الباحث أن الإختراق يمكن تعريفه بالقدرة التي يستطيع من خلالها المخترق الولوج أو الدخول إلى نظام الحاسوب أو الموقع الإلكتروني من خلال برامج متخصصة للإختراق، بهدف تحقيق النتيجة التي يهدف إليها من هذا الهجوم وهي حدوث الأضرار، وذلك بصرف النظر عن قيمتها والآثار المترتبة عليها.

وبالتالي يمكن تعريف جريمة الإختراق في إطار تعريف جريمة الدخول غير المشروع، والتي تعتبر من أهم صور الجرائم المعلوماتية، والتي يطلق عليها تسمية الجرائم المعلوماتية، حيث تعرف جريمة الدخول غير المشروع بأنها عبارة عن ظاهرة معنوية تعني الدخول والولوج إلى العمليات التي يقوم بها النظام المعلوماتي، أو الولوج أو الدخول بشكل غير مشروع أو غير مصرح به إلى نظام معالجة البيانات باستخدام الحاسوب، كما تعرف بأنها كافة الأفعال التي تسمح بالدخول إلى النظام المعلوماتي والسيطرة أو الإحاطة بالخدمات التي يقوم بتقديمها أو المعطيات التي يتكون منها أو الخدمات التي يقدمها (الحذيفي، 2022، ص. 34–35).

وتجدر الإشارة إلى أن جريمة الدخول غير المشروع تتطلب الولوج والانتقال إلى داخل النظام المعلوماتي، وبالتالي لكي تتحقق تلك الجريمة لابد من حدوث اتصال فعلي من قبل الجاني ببيانات ومعلومات النظام المعلوماتي، فلا يكفي محاولة إقامة الاتصال فقد يكون الحاسوب في وضع الحماية رغم تشغيله، والتالي لا يمكن أن يتحقق الدخول غير المشروع للنظام المعلوماتي إلا بعد الحصول على كلمة السر وكذلك التمكن من السيطرة والتسلل إلى النظام المعلوماتي والاطلاع على كافة المعلومات والبيانات أو الخدمات التي يقدمها النظام المعلوماتي (الحذيفي، 2022، ص. 34–35).

وقد أشار المنظم السعودي في اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه، إلى تعريف الإختراق من خلال ما تضمّنه من النص في المادة الأولى منها على أن الأختراق هو " الدخول غير المشروع بأي طريقة، من قبل أي شخص على أي جزء من شبكة اتصالات أو محتوياتها، لأي هدف أو غرض، سواء نتج عن ذلك تخريب أو تعطيل أو لم ينتج عنه شيء"، كما أشار إلى تعريف المخترق بأنه "أي شخص أو مقدم خدمة أو مستخدم قام بعملية اختراق لأي سبب من الأسباب"[1].

[1] المادة الأولى من اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب قرار وزير الإتصالات وتقنية المعلومات رقم (4) بتاريخ 29 / 1 / 1442ه.

كما أشار المنظم السعودي في نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428هـ، إلى الجريمة المعلوماتية من خلال ما تضمّنه من النص في المادة الأولى منه على أنها " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" كما عرف الدخول غير المشروع بأنه" دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"[2].

ويرى الباحث بناء على التحليل السابق أن تعريف المنظم السعودي للجريمة المعلوماتية والدخول غير المشروع قد اعتمد على معيار الوسيلة التي يتم من خلالها ارتكاب الجرائم المعلوماتية، ولم يشترط لقيام الجريمة أن يكون النظام المعلوماتي أو الموقع الألكتروني أو الحاسب الآلي، محمياً بحظر الدخول عليه، كما أن المنظم قد اقتصر في تعريفه لجريمة الدخول غير المشروع على الحالة الخاصة بالجاني الذي لا يتمتع بتصريح الدخول، وبالتالي لم يشير إلى باقي الحالات الأخرى التي تتمثل في البقاء بشكل غير مشروع عند وجود تصريح سابق أو الحالة التي يتم فيها تجاوز التصريح، الأمر الذي يعني فتح المجال لإباحة الطرق الأخرى أما فيما يتعلق باللائحة التنفيذية لنظام الاتصالات فقد تضمن المنظم الإشارة إلى الدخول غير المشروع بأي طريقة كانت والإشارة إلى الحالة التي يتم فيها مجرد الدخول غير المشروع والبقاء بدون حدوث تخريب أو تعطيل.

ثانياً: تعريف المصارف الإلكترونية اصطلاحاً.

يستخدم اصطلاح المصارف والبنوك الإلكترونية كتعبير شامل ومتطور للمفاهيم التي تبلورت مع بداية التسعينات، والتي تتمثل في مفهوم الخدمات المصرفية عن بعد، والخدمات المصرفية الذاتية والبنوك الإلكترونية عن بعد، والتي تُمكن الشخص من إدارة حساباته وانجاز أعماله المتصلة بالبنك عن طريق المكتب أو أي مكان آخر، وإتمام معاملاته في الوقت الذي يريده الأمر الذي يعبر عنه بالخدمة المالية عن بعد (الحاج، 2014، ص 9).

وهناك العديد من المصطلحات التي تطلق على البنوك المتطورة والتي تتمثل في بنوك الانترنت، البنوك الإلكترونية، البنوك الإلكترونية عن بعد، البنك المنزلي، وبنوك الويب حيث يمكن تعريف المصارف والبنوك الإلكترونية بأنها البنوك الافتراضية التي تنشئ لها مواقع الكترونية على الانترنت فهي وسيلة إلكترونية يمكن من خلالها نقل الخدمات والمنتجات البنكية التقليدية والحديثة، وكذلك مباشرة العملاء عبر الانترنت، وإنجاز مختلف العمليات المصرفية التي تنجزها البنوك التقليدية، وكذلك تمكين العملاء من الوصول لحساباتهم، والحصول على المعلومات وإجراء العمليات دون الحاجة إلى التنقل بين فروع البنوك (شناف وبودربالة، د.ت، ص. 32؛ منصوري وعبد المالك، 2014/2013، ص. 34؛ قشي، قرفي، ورملي، 2018، ص. 3).

ثالثاً: تعريف الإختراق المالي للمصارف الإلكترونية.

يرى الباحث بالنظر إلى التحليل السابق لمفهوم الاختراق ومفهوم جريمة الدخول غير المشروع وكذلك التطرق لمفهوم المصارف الإلكترونية يمكن تعريف جريمة الإختراق المالي للمصارف الإلكترونية بأنها الدخول غير المشروع للأنظمة والمواقع الإلكترونية بأي طريقة كانت، باستخدام برامج متخصصة للإختراق والوصول غير المصرح به إلى الحسابات البنكية أو بطاقات الائتمان والحصول على بيانات العملاء السرية، لاستخدمها بالتحايل على المواقع الإلكترونية أو القيام بعمليات التحويل من حساب إلى آخر بشكل غير مشروع، وذلك بهدف الحصول على أموالهم وسرقة بياناتهم المالية. ويعد هذا النوع من أنواع الإختراق من أبرز الجرائم الإلكترونية الشائعة والتي تتم بهدف سرقة البيانات المالية ويعبر عنه بالاحتيال المالي عبر الإنترنت.

[2] المادة الأولى من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

المطلب الثاني: خصائص جريمة الإختراق المالي للمصارف الإلكترونية ودوافع ارتكابها.

لتوضيح خصائص جريمة الإختراق المالي للمصارف الإلكترونية ودوافع ارتكابها ينبغي تقسيم هذا المطلب إلى فرعين نعرض في أولهما خصائص جريمة الاختراق المالي للمصارف الإلكترونية، ونتناول في الثاني دوافع ارتكاب جريمة الاختراق المالي للمصارف الإلكترونية وذلك على النحو التالي:

الفرع الأول: خصائص جريمة الاختراق المالي للمصارف الإلكترونية.

نظراً لارتباط جريمة الإختراق المالي للمصـارف الإلكترونية بالأنظمة وشـبكة الإنترنت واعتبارها من الجرائم المعلوماتية فهناك مجموعة من الخصائص المميزة لها عن الجرائم التقليدية وتتمثل في:

أولاً: جريمة عابرة للحدود

أعطى انتشار شبكة الإنترنت الإمكانية لربط العديد من الأجهزة والأنظمة من غير الخضوع لحدود الزمان والمكان فغالباً ما يكون المجرم في دولة والمجني عليه مقيم في دولة أخرى، حيث تتلاشى الحدود الجعرافية عند ارتكاب الجرائم المعلوماتية كما تظهر العديد من الإشكاليات حول تحديد الجهة صاحبة الإختصاص القضائي للجرائم المعلوماتية ومنها جريمة الإختراق المالي للمصارف الإلكترونية (العجمي، 2014، ص. 20–21؛ عمايره، 2023، ص. 22).

ثانياً: خصوصية المجرم المعلوماتي

يكون المجرم المعلوماتي عادة من ذوي المعرفة والإختصاص، حيث يتم ارتكاب هذا النوع من الجرائم من خلال وسائل تقنية المعلومات ومواكبة التطور والتقدم التكنولوجي، كما يعتبر المخترقون بارعون في استخدام الحاسب الآلي، ولديهم الفضول دائماً في استخدام الحسابات الخاصة بالآخرين بطرق ووسائل غير مشروعة الأمر الذي يدل على أنهم أشخاص غير مرحب بهم لدى الغير وأشخاص متطفلون، وغالباً ما يرتكبون هذا النوع من الجرائم لإثبات الذات والقدرات الخاصة بهم (العجمي، 2014، ص. 20–21).

ثالثاً: صعوبة اكتشاف الجريمة وقياس حجم الأضرار الناتجة عنها

يوصف هذا النوع من الجرائم بالجرائم الخفية والمستترة فالجاني يتميز بقدرة فائقة تمكنه من تنفيذ جريمته بدقة عالية بدون ملاحظتها والقيام بإرسال فيروسات أو سرقة الأموال والبيانات الخاصة بها باستخدام برامج مخصصة للإختراق والدخول غير المشروع، كما تعتبر الأضرار الناتجة عن الجرائم المعلوماتية والتي تعد منها جريمة الاختراق أضراراً غير قابلة للقياس، وذلك في حالة إثبات تلك الجريمة فالمجني عليهم في الغالب لا يعرفون ولا يعلمون شيئاً عنها إلا بعد وقوعها وغالباً ما يفضلون الكتمان تجنباً نشر سر انتهاك النظام المعلوماتي (شريهان، 2020، ص. 10).

رابعاً: صعوبة إثبات الجريمة

هذه الجرائم غالباً لا تترك أثراً لها بعد ارتكابها كما أنه يصعب الإحتفاظ بالآثار الخاصة بها وبالتالي يعد إثباتها من الأمور التي لا تتم بالسهولة حيث أنها تفتقر إلى الدليل المادي، كما أن اكتشافها يكون بعد ارتكاب الجريمة وبمحض الصدفة في بعض الأحيان بالإضافة إلى أن مرتكب الجريمة يعتمد على العديد من وسائل التحايل والتضليل عند ارتكاب تلك الجريمة وإخفاء هويته الحقيقية فضلاً عما يتطلبه التعقب والتحقق منها من خبرة فنية وكفاءة عالية (السكر، 2022، ص. 16).

الفرع الثاني: دوافع اتكاب جريمة الاختراق المالي للمصارف الإلكترونية.

هناك العديد من الأهداف والدوافع التي يسعى الجاني لتحقيقها من خلال ارتكابه لجريمة الإختراق المالي للمصارف الإلكترونية،

ويمكن تقسيمها إلى الدوافع الشخصية، والدوافع الخارجية لارتكاب تلك الجريمة وذلك على النحو التالي:

أولاً: الدوافع الشخصية:

هناك العديد من الدوافع الشخصية التي تؤدي بدورها إلى ارتكاب جريمة الاختراق المالي للمصارف الإلكترونية والتي تتمثل في الدوافع الذهنية والدوافع المالية:

1. الدوافع الذهنية

الدوافع الذهنية قد تكون سبباً في ارتكاب تلك الجريمة إذ تنطوى النفس الإنسانية على بواعث نفسية متعددة، كما تتجه الإرادة إلى تحقيق غايات متناهية واستخدام النظام لمصالح وأغراض شخصية، فالمجرم المعلوماتي يقوم بارتكاب تلك الجريمة، حيث يكون لديه شعور بالبحث عن القوة، والقدرة على القيام بذلك الفعل والرغبة في إثبات الذات، ومواجهة التطور العلمي والتقدم التقني في الحاسوب والإنترنت من خلال وضع بصماته وإظهار تفوقه، وإثبات قدراته على الدخول واختراق الأنظمة في أي لحظة والحصول على البيانات والمعلومات التي يريد الحصول عليها، حيث يكون لديه الشغف والرغبة في اختراق الأنظمة والمواقع عند ظهور أية تقنية مستحدثة، ويحاول بكافة الوسائل والبرامج التي يمكن من خلالها تحطيمها والتفوق عليها الأمر الذي يؤدي إلى الشعور بالرغبة في الاختراق وارتكاب تلك الجريمة بهدف لفت الانتباه وتوجيه الانظار إليه، وكذلك إظهار التفوق على التطور والتقدم التكنولوجي ومستوى ارتقاء براعته في كسر حواجز الأمن للأنظمة والشبكات المعلومات (عياش، 2024، ص. 98؛ القحطاني، 2016، ص. 20).

2. الدوافع المالية

فقد يرتكب العديد من الأشخاص تلك الجريمة بدافع الحصول على الأموال وذلك لإشباع غريزتهم من حب التملك والحصول على المال بأسهل الطرق،حيث تعد الدوافع المالية من أهم الدوافع التي تحفز المجرم لارتكاب العديد من الجرائم ومنها جريمة الاختراق المالي للمصارف الإلكترونية فالإنسان بطبيعته لديه حب كبير للمال، وهذا ما ورد في قوله تعالى﴿ وَتُحِبُّونَ ٱلۡمَالَ حُبّٗا جَمّٗا﴾ (سورة الفجر، الآية 20)، فالشخص عندما يشعر أنه سوف يحصل على مال كثير من خلال ارتكابه لتلك الجريمة فإنه يشعر بالتحفيز، كما يجعله يعمل على مواكبة التقدم والتطور التكنولوجي وإيجاد الثغرات التي يمكن من خلالها الحصول على الأموال، وتحقيق مكاسب مالية من خلال هذا التطور الأمر الذي يدفعه إلى ارتكاب هذا النوع من الجرائم والقيام بالإختراق والدخول غير المشروع، والقيام بسرقة البيانات والمساومة عليها والقيام بعمليات التحويل غير المشروعة، وذلك بهدف تحقيق الربح والكسب المالي بطرق غير مشروعة وارتكاب العديد من الجرائم ومنها جريمة الاختراق المالي للمصارف الإلكترونية (عياش، 2024، ص. 98–99؛ غنام، 2023، ص. 18).

ثانياً: الدوافع الخارجية:

هناك العديد من العوامل الخارجية والتي تعتبر بدورها دافعاً لارتكاب العديد من الجرائم المعلوماتية ومنها جريمة الإختراق المالي للمصارف الإلكترونية وقد تتمثل في الدوافع السياسية والدينية بالإضافة إلى دافع الإنتقام ويمكن الإشارة إليها فيما يلي:

1. الدوافع السياسية والدينية

تعتبر الدوافع السياسية والدينية من أهم الدوافع لارتكاب الجرائم المعلوماتية ومنها جريمة الإختراق المالي للمصارف الإلكترونية، فالخلافات السياسية بين الدول أو بين الأحزاب أو بين المعارضة والدولة نفسها قد تؤدي إلى ارتكاب الجرائم، حيث يعد هذا الدافع أحد الدوافع التي ظهرت بشكل كبير، وذلك بسبب انتشار الظلم وغياب الديموقراطية، وعدم وجود القوانين التي تكفل احترام المواطن وتحقيق مصالحهم، الأمر الذي أدى إلى ارتكاب العديد من الجرائم وتبني العديد من المنظمات أفكار ووجهات نظر سياسية أو أيدلوجية

معينة أو دينية، وبالتالي قد ترتكب الجريمة للدفاع عن هذه الآراء ووجهات النظر والقيام بأفعال إجرامية ضد معارضيها (القحطاني، 2016، ص. 19؛ عياش، 2024، ص. 98–99).

2. دافع الإنتقام

يعتبر دافع الإنتقام من الدوافع الأكثر خطورة في ارتكاب هذا النوع من الجرائم كما تزيد خطورته أيضاً عندما يمتلك هؤلاء الأشخاص البيانات والمعلومات الكبيرة عن تلك المصارف حيث يعتبر دافع الإنتقام من أخطر الدوافع التي تجبر المجرم على ارتكاب الفعل الإجرامي، فقد يتعرض موظف للفصل التعسفي من وظيفته، مع العلم أن لديه الكفاءة والخبرة بالعمل والقيام بمهام وظيفته فيقوم ذلك الموظف بالرد على هذا الفصل التعسفي بالقيام بالإنتقام، وذلك من خلال الدخول والإختراق والوصول إلى بيانات العملاء السرية وسرقة الأموال، والقيام بعمليات تحويل الأموال بطرق غير مشروعة وسرقتها وذلك بدافع الإنتقام أو غير ذلك من دوافع الانتقام الأخرى التي تؤدي إلى ارتكاب الجريمة (غنام، 2023، ص. 17؛ عياش، 2024، ص. 98–99).

المبحث الأول: التأصيل الفقهي والنظامي لجريمة الإختراق المالي للمصارف الإلكترونية

المطلب الأول: التأصيل الفقهي لجريمة الإختراق المالي للمصارف الإلكترونية.

الجريمة في الاصطلاح الشرعي هي إتيان فعل من الأفعال المحرمة المعاقب على فعلها أو ترك فعل من الافعال المأمور بها والتي يعاقب على تركها، فالجرائم في الشريعة الإسلامية هي المحظورات الشرعية التي زجر الله تعالى عنها بحدٍ أو تعزير (عوده، 1968، ج1، ص. 66؛ أبو زهرة، 1998، ص. 20؛ الماوردي، 1989، ص. 285).

ويعد مقصد حماية الأموال من مقاصد الشريعة الإسلامية، حيث نهت عن الإعتداء عليه وذلك بأي صورة من صور الإعتداء، كما قررت الشريعة الإسلامية العقوبات الرادعة للإعتداء على تلك الأموال بالسرقة والإستيلاء عليها، وشرعت حد السرقة والعقوبة الرادعة لارتكاب جريمة السرقة وهي القطع وذلك وقوله تعالى ﴿وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَٰلًا مِّنَ ٱللَّهِۗ وَٱللَّهُ عَزِيزٌ حَكِيمٌ﴾ (سورة المائدة، الآية 38).

كما أكدت السنة النبوية الشريفة على حرمة الدماء والأموال والأعراض، وبالتالي حرمت الإعتداء على الأموال بأي صورة من صور الإعتداء، فالإعتداء على الأموال المحرزة وسرقتها توجب الحد، فالحرز هو ما يصير به المال محرزاء أي ما يصير به محفوظاً ومصوناً من الضياع، وقد جرى العرف على اعتبار البطاقة حرزاً وذلك لأن البنك والمصرف الذي أصدر البطاقة يقوم بتسديد الأموال التي تم التعامل بها وذلك من خلال هذه البطاقة (الطويلي، 2019، ص. 22).

ولما كانت الشريعة الإسلامية هي التي تحكم المعاملات في المملكة العربية السعودية ولما كانت السلطة قد وضعت القواعد والأنظمة التي تحكم التعاملات الإلكترونية وكذلك التجارة الإلكترونية وأجاز علماء الأمة التعاملات الإلكترونية من خلال البطاقة الإلكترونية، وذلك باعتبارها وكالة أو كفالة بأجر أو وساطة تجارية بأجر، ولما كانت تشمل الأموال وغيرها فإن سرقة البطاقات الائتمانية تعد جريمة بالمفهوم الشرعي حيث يظهر ذلك من تعريف السرقة عند فقهاء المسلمين والذي لم يحدد نوع المال المسروق بل هي عبارة عن أخذ الشيء خفية من الغير بغير إذنه مالاً كان أو غيره (الطويلي، 2019، ص. 18–19).

كما اختلف العلماء المعاصرين حول تكييف سرقة البطاقات الائتمانية عبر الانترنت فأشار البعض منهم إلى كونها تعد جريمة سرقة مكتملة الاركان، وذلك لتوافر شروط السرقة الحدية حيث أنها مال مسروق خفية قد بلغ النصاب مأخوذ من حرز وهو الحاسب الآلي، كما أشار البعض الآخر إلى أن شروط السرقة الحدية غير مكتملة فهي إما أن تعتبر جريمة سرقة غير حدية أو عملية نصب أو احتيال أوخيانة (الطويلي، 2019، ص. 18–19).

ويرى الباحث أن جريمة الإختراق المالي للمصارف الإلكترونية والتي قد يتم من خلالها اختراق الحسابات البنكية وبطاقات الإئتمان وسرقة البيانات المالية وتحويل الأموال بطرق غير مشروعة تعتبر جريمة من الجرائم المعاقب عليها في الشريعة الإسلامية ويمكن تكييفها على أنها جريمة سرقة وتعبر من الجرائم الحدية التي يقام الحد على مرتكبها إذا توافرت الشروط وتم الحصول على المال الذي بلغ النصاب كما أن قيام شخص بالاختراق واتجاه إرادته إلى الدخول غير المشروع للمصارف والقيام بعمليات تحويل الأموال بطريقة غير مشروعة وسرقة البيانات البنكية والبطاقات البنكية والقيام بالاحتيال المالي، يعتبر جريمة سرقة حيث تعتبر البطاقات مالاً متقوماً وذلك باعتبارها وسيلة للحصول على الأموال، بالإضافة إلى أنها مأخوذة من حرز وهو الحاسب الآلي وبالتالي لا يجوز انتهاكها أو الاعتداء عليها بأي شكل من الأشكال. كما أن السرقة تنطبق على كافة أنواع السرقة مما هو معروف ومما هو حديث ويتم ارتكابه بوسيلة من وسائل تقنية المعلومات وفي إطار المعاملات الإلكترونية طالما تحققت الشروط الخاصة بها.

المطلب الثاني: التأصيل النظامي لجريمة الإختراق المالي للمصارف الإلكترونية

انتشرت أفعال الدخول غير المشروع إلى الأنظمة والمواقع الإلكترونية وكذلك الاختراقات صورة واسعة وذلك بسبب عدم اهتمام العديد من الأفراد والمؤسسات بتوفير الحماية والأمن للأنظمة المعلوماتية التي يتعاملون بها، لمواكبة التطور والتقدم التكنولوجي بالإضافة إلى أن برامج الاختراق والأدوات والأساليب الخاصة به متاحة عبر الانترنت الأمر الذي يؤدي إلى تزايد عدد من يرتكبون تلك الجريمة.

وبالنظر إلى موقف المنظم السعودي من جريمة الاختراق المالي للمصارف الإلكترونية نجد أنه قد تضمن في الأنظمة الصادرة في المملكة العربية السعودية تجريم أفعال الدخول غير المشروع والاختراقات، حيث أشار في اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه، إلى تجريم الإختراقات، وذلك من خلال ما تضمّنه من النص في المادة الأولى منه على أنه " يعتبر الإختراق إحدى صور إساءة استخدام شبكة الاتصالات ويكون بذلك مخالفة وفقاً للمادة السابعة والثلاثون من النظام وتنطبق عليها الإجراءات المنصوص عليها في هذه اللائحة لمعالجة المخالفات.

- تقوم الهيئة وفقاً لأنظمتها بوضع الإجراءات الضرورية الهادفة إلى تحقيق الحماية والحد من الإختراقات وإصدار التعليمات اللازمة لذلك.
- يجب على أي شخص أو مقدم خدمة أو مستخدم الإلتزام بالإجراءات والتعليمات التي تضعها وتصدرها الهيئة وفقاً للفقرة (87 - 2) من هذه المادة"[3].

حيث تضمن المنظم السعودي الاشارة إلى المخالفات الخاصة بأحكام النظام في المادة السابعة والثلاثون من نظام الاتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه، وأشار إلى إساءة استخدام شبكة الاتصالات، وذلك من خلال النص على أنه " يعد مخالفة كل مشغل أو شخص طبيعي أو معنوي يقوم بأحد الأعمال الآتية:

14- إلحاق ضرر بشبكات الاتصالات العامة أو التعدي عليها أو قطعها أو الإستفادة غير المشروعة منها أو تعطيل الاتصالات أو منع تبادل المعلومات بشكل عام"[4].

---

[3] المادة السابعة والثمانون من اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب قرار وزير الإتصالات وتقنية المعلومات ال رقم (4) بتاريخ 29 / 1 / 1442ه.

[4] المادة السابعة والثلاثون من نظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب المرسوم الملكي رقم (74) بتاريخ 5 / 3 / 1422ه وتعديلاته.

كما أشار المنظم السعودي إلى تجريم فعل الدخول غير المشروع وذلك ضمن النصوص الواردة في نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه، وذلك من خلال النص على أن " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1. الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
2. إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
3. إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت"[5].

كما تضمن النص على أن " يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:.....2. الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني" [6]..

بالإضافة إلى ما تضمنه المنظم ضمن النصوص الواردة في نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه، من تجريم الاختراق المالي للمصارف الإلكترونية، وتجريم الوصول دون مسوغ نظامي صحيح إلى البيانات البنكية، وذلك من خلال النص على أن "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:.....2. الوصول - دون مسوغ نظامي صحيح إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات[7].

ويرى الباحث بناء على النصوص التي تم الإشارة إليها والتي تضمنها المنظم السعودي أن المنظم السعودي قد جرم فعل الإختراق والذي يتمثل في الدخول غير المشروع بأي طريقة، على أي جزء من شبكة اتصالات أو محتوياتها، من قبل أي شخص لأي غرض أو هدف، سواء نتج عن ذلك تعطيل أو تخريب أو لم ينتج عنه شيء، وذلك باعتبارها إحدى صور إساءة استخدام شبكة الاتصالات، وأشار ضمن النصوص الواردة في اللائحة التنفيذية لنظام الاتصالات إلى اعتبارها مخالفة من المخالفة الواردة في المادة السابعة والثلاثون من نظام الإتصالات حيث تضمن المنظم تجريم أفعال الاختراقات والتي تمثل خطراً على مصالح المؤسسات وأموالها والإعتداء عليها، مما يزعزع الثقة في المعاملات الإلكترونية.

كما جرم فعل الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها والدخول غير المشروع إلى نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو موقع إلكتروني، أو أحد أجهزة الحاسب الآلي بهدف الحصول على البيانات التي تمس الاقتصاد الوطني، حيث تمثل جريمة الدخول غير المشروع إلى النظام المعلوماتي أو الشبكة المعلوماتية تهديداً وانتهاكاً صارخاً للخصوصية الإلكترونية.

---

[5] المادة الخامسة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

[6] المادة السابعة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

[7] المادة الخامسة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

كما اعتبر المنظم جريمة الدخول غير المشروع جريمة من الجرائم المعلوماتية التي يتم العقاب عليها وبالتالي فإن المنظم السعودي أشار إلى تجريم أفعال الدخول غير المشروع والاختراقات، وأشار إلى تجريم الدخول غير المصرح به بغرض الإستيلاء على الأموال أو الدخول إلى البطاقات البنكية، أو الإئتمانية وهو ما ينطبق بدوره على جريمة الاختراق المالي للمصارف الإلكترونية، وتحويل المبالغ المالية بطرق غير مشروعة والحصول على بيانات الحسابات البنكية، وبطاقات الائتمان وذلك نظراً لخطورة تلك الأفعال والآثار التي تترتب على ارتكابها.

المبحث الثاني: أركان جريمة الإختراق المالي للمصارف الإلكترونية:

المطلب الأول: الركن المفترض لجريمة الإختراق المالي للمصارف الإلكترونية

جريمة الإختراق كغيرها من الجرائم الأخرى تتطلب توافر الأركان الخاصة بها من ركن مادي وركن معنوي بالإضافة إلى الركن القانوني والذي يتمثل في كون الفعل معاقباً عليه ضمن النصوص النظامية في المملكة العربية السعودية، فالركن القانوني هو ما يسميه بعض الحقوقيين بالركن الشرعي، والذي يعبر عنه بأنه لا جريمة ولا عقوبة إلا بنص، فالقواعد الجنائية هي التي تحدد الأفعال التي يمكن اعتبارها جريمة وكذلك تقرر العقوبات المناسبة لها (عياش، 2024، ص95)، وهذا ما أشار إليه المنظم السعودي في النظام الأساسي للحكم الصادر بالأمر الملكي رقم أ/19 بتاريخ 27 / 8 / 1412ه من خلال النص على أن" العقوبة شخصية، ولا جريمة ولا عقوبة إلا بناء على نص شرعي، أو نص نظامي، ولا عقاب إلا على الأعمال اللاحقة للعمل بالنص النظامي"[8].

وهذا ما أشارنا إليه في التأصيل القانوني لجريمة الاختراق المالي للمصارف الإلكترونية، حيث أشار المنظم السعودي إلى تجريم تلك الأفعال وتقرير العقوبة المناسبة لها وذلك من خلال ما تضمنه من تجريم أفعال الإختراق في اللائحة التنفيذية لنظام الإتصالات الصادرة بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه[9].

وكذلك تجريم فعل الدخول غير المشروع ضمن النصوص الواردة في نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه[10].

وتجدر الإشارة إلى أن هناك أنواع خاصة من الجرائم التي تستلزم لقيامها بالإضافة إلى الركنين المادي والمعنوي ركناً خاصاً يعرف بالشرط المفترض، وهو شرط يفترض القانون توافره حتى يتحقق قيام الجريمة، كما أنه شرط سابق لتحقق الركن المادي للجريمة، بالرغم من أن هذا الشرط لا يعتبر من الأركان العامة إلا أنه شرط من الشروط الضرورية لقيام الجريمة، ويعتبر بمثابة ركناً خاصاً من أركان الجريمة حيث عرف الفقه المصري الشرط المفترض بأنه عنصر سابق على السلوك يلزم وجوده لثبوت الصفة الجرمية لهذا السلوك، أو العنصر الذي يفترض قيامه وقت مباشرة الفاعل لنشاطه، أو يعرف بأنه حالة قانونية أو واقعية يحميها القانون (القاسمي، 2018، ص. 10).

وبالنسبة لهذه الجريمة وباعتبارها جريمة من الجرائم المعلوماتية والتي يعد منها الدخول غير المشروع فإنها تستلزما ركناً خاصاً

---

[8] المادة الخامسة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

[9] المادة السابعة والثمانون من اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب قرار وزير الإتصالات وتقنية المعلومات ال رقم (4) بتاريخ 29 / 1 / 1442ه.

[10] المادة الخامسة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

وهو المحل الذي ينصب عليه السلوك الإجرامي والذي يتمثل في النظام المعلوماتي والمواقع الإلكترونية أو شبكة المعلومات أو أنظمة المعلومات الإلكترونية ووسيلة تقنية معلومات، فلا تتحقق تلك الجريمة إلا بتوافر الشرط المفترض والركن الخاص لها ولا يلزم أن يقع هذا السلوك على جميع صور المحل التي نص عليها المنظم، بل يكفي أن ينصب على إحداها فقط لتحقق الجريمة وقيامها (القاسمي، 2018، ص. 10–11).

ويرى الباحث بالنظر لما تقدم من تجريم أفعال الدخول غير المشروع والاختراقات وبالتطبيق على جريمة الإختراق المالي للمصارف الإلكترونية، فإن هذه الجريمة لها طبيعة خاصة تستلزم لقيامها توافر الشرط المفترض وذلك بالقياس على مفهوم الاختراق الوارد في اللائحة التنفيذية لنظام الاتصالات والقياس على الجرائم المعلوماتية ومنها جريمة الدخول غير المشروع إلى النظام المعلوماتي، فإن جريمة الاختراق المالي للمصارف الإلكترونية تتطلب شرطاً مفترضاً يتمثل في محل الجريمة، ويتضمن وجود الكيان المادي للنظام الآلي لمعالجة المعلومات والنظام المعلوماتي والبيانات المالية للمصارف الإلكترونية والبطاقات البنكية وبطاقات الائتمان.

المطلب الثاني: الركن المادي لجريمة الإختراق المالي للمصارف الإلكترونية

تعتبر جريمة الإختراق المالي للمصارف الإلكترونية من أخطر جرائم الاعتداء على الأموال، والتي ينبغي لقيامها وتحققها توافر الركن المادي والذي يتمثل في النشاط أو الفعل الذي يقوم به الجاني من خلال الاعتداء على حق كفله القانون، والوجه الخارجي للنشاط الإجرامي، ويتمثل الركن المادي في جريمة الإختراق المالي للمصارف الالكترنية، في الدخول إلى النظام الآلي لمعالجة البيانات، والوصول إلى البيانات المالية للمصارف الإلكترونية والحصول عليها، ويتحقق ذلك من خلال توافر السلوك الإجرامي والنتيجة الإجرامية وعلاقة السببية وذلك على النحو التالي:-

اولاً: السلوك الإجرامي

يعد السلوك الإجرامي عنصر من عناصر الركن المادي لجريمة الاختراق المالي للمصارف الإلكترونية، حيث يتمثل السلوك الإجرامي فيما يقوم به الشخص من أفعال تؤدي بدورها إلى تحقيق النتيجة التي يسعى إليها فالجاني في الجرائم المعلوماتية يتمتع بالكفاءة والمهارة التي تميزه عن الجاني في الجرائم التقليدية، وفيما يتعلق بجريمة الإختراق في صورتها المجردة فيكون مجال السلوك الإجرامي يتمثل في إتلاف المعلومات والبيانات الخاصة بالمجني عليه أو تدمير المواقع أو اتلافها حيث تعد الشبكات وسيلة من وسائل نقل المعلومات والبيانات وبالتالي يجب حمايتها وتوفير الضمان لها من الاختراق (القاسمي، 2018، ص. 55/49).

وبالتطبيق على جريمة الإختراق المالي للمصارف الإلكترونية، يتمثل الركن المادي حسب ما تضمنه المنظم السعودي من تعريف الإختراق في اللائحة التنفيذية لنظام الاتصالات في الدخول غير المشروع بأي طريقة، وأي وسيلة من الوسائل على أي جزء من شبكة اتصالات أو محتوياتها[11].

وهذا ما تضمنه المنظم أيضاً في نظام مكافحة جرائم المعلوماتية، حيث يتمثل الركن المادي وفقاً لما أشار إليه في الدخول غير المشروع إلى نظام معلوماتي مباشرة أو موقع إلكتروني، أو أحد أجهزة الحاسب الآلي أو الشبكة المعلوماتية [12]

---

[11] المادة الأولى من اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب قرار وزير الإتصالات وتقنية المعلومات ال رقم (4) بتاريخ 29 / 1 / 1442ه.

[12] المادة السابعة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

وبالتالي يتمثل السلوك الإجرامي في كل فعل من الأفعال التي يقوم بها المخترق من الدخول غير المشروع والقيام بفعل الدخول نفسه وذلك دون تصريح أو رضا من صاحب الحق في الدخول إلى النظام، حيث يمثل مجرد الدخول إلى النظام المعلوماتي أو الشبكة المعلوماتية بدون تصريح جريمة في حد ذاته، وذلك بمجرد القيام بالنشاط أو السلوك التقني الإجرامي.

وبالنظر إلى تطور وسائل تقنية المعلومات والاستعانة بأحد الوسائل لتنفيذ جريمة الإختراق المالي للمصارف الإلكترونية فهناك العديد من الطرق والوسائل التي يمكن تنفيذ الجريمة من خلالها، والتي تتمثل في الدخول إلى النظام المعلوماتي أو الحسابات المصرفية، أو الحصول على أرقام بطاقات الائتمان واستخدام الثغرات الأمنية للوصول إلى الحسابات البنكية أو سرقة كلمات المرور أو تثبيت برامج التجسس (الحذيفي، 2022، ص. 36).

ويرى الباحث بالتطبيق على جريمة الإختراق المالي للمصارف الإلكترونية أن السلوك الإجرامي يتمثل في الدخول غير المشروع واختراق النظام، واختراق المصارف الإلكترونية للحصول على البيانات المالية والحسابات البنكية وسرقة البطاقات الإئتمانية، والوصول على البيانات المالية للعملاء، وتحويل الأموال بطرق غير مشروعة، حيث يتمثل الركن المادي لتلك الجريمة في التصرف الفعلي الذي يقدم به الجاني ويترتب عليه الدخول غير المصرح به إلى الأنظمة وحسابات الآخرين بأي طريقة من خلال وسيلة من وسائل تقنية المعلومات أو برمجيات ضارة أو برامج اختراق متخصصة في ذلك.

ثانياً: النتيجة

بجانب توافر عنصر السلوك الإجرامي، يشترط لتحقق جريمة الإختراق المالي للمصارف الإلكترونية أن تتحقق النتيجة الإجرامية وهي الأضرار التي تترتب على ارتكاب تلك النشاط الإجرامي والهدف الذي يسعى المخترق للوصول إليه، حيث تتحقق النتيجة الجرمية في جريمة الإختراق بمجرد الدخول غير المشروع، وهذا ما تضمنه المنظم السعودي من تجريم الإختراق واعتباره مخالفة في اللائحة التنفيذية لنظام الاتصالات، وما تضمنه من المفهوم الخاص به والذي يتمثل في الدخول غير المشروع بأي طريقة.

وبالتالي يشترط لتحقق جريمة الإختراق المالي للمصارف الإلكترونية تحقق النتيجة الإجرامية من من الدخول غير المشروع، والوصول إلى المعلومات والبيانات المخزنة داخل النظام دون وجه حق، بطريقة متعمدة بقصد الاطلاع على ما تحويه من بيانات أو معلومات سرية خاصة والحصول إلى البيانات المالية للعملاء وتحويل المبالغ المالية بطرق غير مشروعة والتحويل من حساب لآخر (العنزي، 2022، ص. 13؛ عياش، 2024، ص. 96/95).

وذلك وفقاً لما تضمنه المنظم في نظام مكافحة جرائم المعلوماتية من الإشارة إلى النتيجة التي يلزم تحققها على في جريمة الاختراق المالي للمصارف الإلكترونية وهي الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية، أو ائتمانية، أو معلومات، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو أموال، أو ما تتيحه من خدمات[13].

ثالثاً: علاقة السببية.

يقصد بعلاقة السببية أن يكون السلوك الإجرامي هو الذي تسبب في حدوث النتيجة، والتي تعتبر أحد عناصر الركن المادي وبالتالي يلزم أن تكون هناك رابطة أو علاقة سببية بين الفعل والنتيجة، وتجدر الإشارة أن الجرائم المعلوماتية لا تستوجب من الجاني القيام بأي عنف أو بذل أي جهد بشكل عام.

(13) المادة الخامسة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

وبالتطبيق على جريمة الاختراق المالي للمصارف الإلكترونية تتمثل علاقة سببية في جريمة الاختراق في العلاقة بين الفعل والنتيجة، وذلك من خلال الدخول غير المشروع إلى الجهاز أو بالحصول على البيانات أو المعلومات الإلكترونية المخزنة، حيث تتمثل في العلاقة بين فعل الجاني الذي قام به والسلوك الإجرامي الصادر عنه بالدخول غير المشروع دون مسوغ نظامي صحيح وبين الوصول والحصول على بيانات بنكية، أو ائتمانية، أو معلومات، أو بيانات متعلقة بملكية أوراق مالية للحصول على الأموال، ويمكن إثبات علاقة السببية وتوافرها متى ثبت مساهمة السلوك الإجرامي الصادر عن الجاني في إحداث وتحقق النتيجة (عياش، 2024، ص. 95–96؛ القاسمي، 2018، ص. 49–55؛ العنزي، 2022، ص. 13)

المطلب الثالث: الركن المعنوي لجريمة الإختراق المالي للمصارف الإلكترونية

يمثل الركن المعنوي أهمية رئيسية في النظرية العامة للجريمة وهو ركن من الأركان التي يجب توافرها لقيام الجريمة فلا يسأل الشخص عن الجريمة إلا في حالة توافر الركن المعنوي الذي يؤدي إلى تحديد المسؤولية الجنائية على الوجه الدقيق، فلابد لقيام جريمة الاختراق المالي للمصارف الإلكترونية وترتيب المسئولية الجنائية عنها، توافر الركن المعنوي للجريمة والذي يتمثل في القصد الجنائي واتجاه إرادة الجاني إلى السلوك الإجرامي الذي باشره وإلى تحقيق النتيجة المترتبة عليه وذلك مع علمه بكافة العناصر المتطلبة لقيام الجريمة، فلا يكفي أن يكون الجاني عالماً بالركن المادي للجريمة، بل لابد أن تتجه إرادته إلى تحقيق النتيجة وبالتالي يستلزم لتحقق القصد الجنائي توافر العلم والإرادة وذلك على النحو التالي (الحذيفي، 2022، ص. 38–39):

أولاً: العلم

العلم هو أحد عنصري القصد الجنائي، ويقصد به أن ينصرف علم الجاني إلى جميع العناصر الرئيسية التي يقوم عليها كيان الجريمة، فيجب أن يكون الجاني على علم تام بالجريمة التي يقوم بارتكابها، وكافة العناصر القانونية لها بالإضافة إلى إنصراف إرادته لارتكاب ذلك السلوك والنتيجة المترتبة عليه، وبالتالي يستلزم العلم إحاطة مرتكب السلوك الإجرامي بالواقعة الإجرامية وتكييف الفعل نفسه والنتيجة التي تترتب على القيام به وذلك بمعنى أن يأتي الجاني سلوكه التقني الإجرامي وهو عالماً بأنه يقوم بالدخول على النظام المعلوماتي أو الموقع الكتروني، أو الشبكة المعلوماتية، الغير مصرح له الدخول إليها، وأن هذا الدخول المعلوماتي يتم بدون تصريح (القاسمي، 2018، ص. 56).

كما يجب أن يعلم الجاني بالوقائع التي تعد عنصراً في الجريمة، ومنها العلم بمحل الجريمة والمحل الذي يقع عليه الإعتداء فلا يتوافر القصد الجنائي إذا انتفى هذا العلم، فلا تقوم الجريمة إذا كان لا يعلم أنه يدخل على نظام معلومات الكتروني، أو موقع إلكتروني أو شبكة معلوماتية أو كان لديه اعتقاد بأنه يقوم بعمليات حسابية من خلال الحاسب الآلي، وذلك متى كان هذا الاعتقاد مبنياً على مبررات معقولة (الحذيفي، 2022، ص. 38؛ القاسمي، 2018، ص. 58–59).

ثانياً: الإرادة

الإرادة هي العنصر الثاني للقصد الجنائي والتي ينتفي القصد الجنائي بدونها، فهي جوهر القصد الجنائي وهي العنصر الهام الذي يتم التمييز من خلاله بين الجرائم العمدية والجرائم الغير عمدية حيث أنه يصعب في الكثير من الأحيان الوقوف على تحديد ما إذا كان الدخول إلى النظام المعلوماتي قد تم بطريقة عمدية أو عن طريق الخطأ فالإرادة كعنصر من عناصر القصد الجنائي تتمثل في عنصرين أولهما إرادة النشاط الصادر عن مرتكب الجريمة والثاني إرادة تحقيق النتيجة والتي قام الفاعل بارتكاب السلوك الإجرامي بهدف تحقيقها (الحذيفي، 2022، ص. 38–39؛ القاسمي، 2018، ص. 59).

وفيما يتعلق بجريمة الاختراق بصورتها البسيطة فإنها تتطلب توافر القصد الجنائي العام والذي يتكون من العلم والإرادة، ويتمثل في

اتجاه إرادة الفاعل إلى الدخول عمداً دون وجه حق بأية وسيلة نظاماً، أو موقعا الكترونيا، أو شبكة إلكترونية، والاستمرار في التواجد بها وذلك بعد علمه بأن هذا الفعل مجرماً وفقاً للأنظمة واللوائح المعمول بها في المملكة العربية السعودية.

فالركن المعنوي يتطلب إثبات أن الجاني كان على دراية كاملة وعلم بأن فعل الإختراق الذي يقوم به فعلاً مجرماً وغير قانونياً، وأن التصرف الذي يقوم به يترتب عليه العديد من الإضرار التي تتمثل في الإضرار بالضحايا أو الإستفادة بشكل وطرق غير مشروعة.

وفي بعض الأحيان يستلزم القانون توافر القصد الجنائي الخاص للعقاب على الجريمة وذلك في الحالة التي تتجه فيها إرادة الجنائي بتحقيق هدف أو غاية معينة من ارتكاب هذا الفعل المجرم وهو الإختراق والدخول غير المشروع وسيلة نظاماً، أو شبكة إلكترونية، حيث تستلزم جريمة الاختراق المالي للمصارف الإلكترونية توافر قصداً جنائياً خاصاً يتمثل في الحصول على البيانات المالية للعملاء، وسرقة البطاقات البنكية والبطاقات الائتمانية والقيام بعمليات تحويل الأموال من حساب لاخر وبطرق غير مشروعة، حيث يشترط المنظم في القصد الخاص توافر عنصراً إضافياً بجانب عنصري العلم والإرادة والذي يتمثل في النية الخاصة لدى الجاني والتي يسعى إلى تحقيقها من خلال الاختراق والدخول غير المشروع وليس فقط الاختراق والدخول غير المشروع المجرد (الحذيفي، 2022، ص. 39/38؛ القاسمي، 2018، ص61/60).

المبحث الثالث: آليات مكافحة جريمة الإختراق المالي للمصارف الإلكترونية

المطلب الأول: الآليات النظامية لمكافحة جريمة الإختراق المالي للمصارف الإلكترونية

بذلت المملكة العربية السعودية العديد من جهود المكافحة لمواجهة الجرائم المعلوماتية حيث سايرت التطور الدولي في مجال المكافحة كما استفادت من تجارب العديد من الدول في التصدي لهذا النوع من الجرائم سواء من خلال الطرق الفنية أو الطرق القانونية والعمل على تحديث وتطوير الأنظمة التشريعية المتعلقة بمكافحة جرائم المعلوماتية ومن أهمها:

أولاً: إصدار نظام مكافحة جرائم المعلوماتية

أصدرت المملكة العربية السعودية نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428هـ والذي يهدف إلى الحد من وقوع هذا النوع من الجرائم، وذلك من خلال تحديد هذه الجرائم والعقوبات المقررة لكل منها، الأمر الذي يؤدي إلى حفظ الحقوق التي تترتب على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية والمساعدة على تحقيق الأمن المعلوماتي وكذلك حماية الأخلاق، والمصلحة العامة، والآداب العامة بالإضافة إلى حماية الاقتصاد الوطني [14].

حيث تضمن إقرار العديد من الجرائم ومنها جريمة الدخول غير المشروع، وذلك من خلال النص على تعريفها في المادة الأولى منه كما أشار إلى تجريم الإختراق المالي للمصارف الإلكترونية، وذلك من خلال تجريم الوصول دون مسوغ نظامي صحيح إلى البيانات البنكية أو الائتمانية أو الحصول على المعلومات أو الأموال والاستيلاء عليها، وقرر لها عقوبة السجن الذي لا تزيد مدته على ثلاث سنوات والغرامة التي لا تزيد على مليوني ريال أو إحدى هاتين العقوبتين وذلك من خلال النص على أن" يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:.....2. الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات[15].

---

(14) المادة الثانية من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

(15) المادة الخامسة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

كما نص على تجريم الدخول غير المشروع بهدف تسريب البيانات وتقرير عقوبة لهذا الفعل والتي تتمثل في السجن الذي لا تزيد مدته على أربع سنوات والغرامة التي لا تزيد على ثلاثة ملايين ريال أو إحدى هاتين العقوبتين وذلك من خلال النص على أن " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

4. الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
5. إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
6. إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت"[16].

بالإضافة إلى ما تضمنه المنظم من تشديد العقوبة على الجاني وذلك في الحالة التي يكون فيها الهدف من الدخول غير المشروع، الحصول على بيانات تمس الاقتصاد الوطني حيث قرر عقوبة السجن الذي لا تزيد مدته على عشر سنوات والغرامة التي لا تزيد على خمسة ملايين ريال أو إحدى هاتين العقوبتين وذلك من خلال النص أن" يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:.....2. الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني" [17].

فضلاً عما أشار إليه المنظم السعودي في الحالة التي تقترن فيها الجريمة بأي من هذه الحالات والتي تتمثل في شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة أو ارتكاب الجاني تلك الجريمة مستغلاً نفوذه وسلطته حيث تضمن النص على أن " لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:

1. ارتكاب الجاني الجريمة من خلال عصابة منظمة.
2. شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلًا سلطاته أو نفوذه.
3. التغرير بالقُصَّر ومن في حكمهم، واستغلالهم.
4. صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة"[18].

وبالإضافة إلى ما تقدم فقد أقر المنظم السعودي عقوبة المصادرة ضمن نظام مكافحة جرائم المعلوماتية وذلك من خلال النص على أنه "مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها.

كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقًا نهائيًا أو مؤقتًا متى كان مصدرًا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه"[19].

---

(16) المادة الخامسة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

(17) المادة السابعة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

(18) المادة الثامنة من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

(19) المادة الثالثة عشر من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

ويرى الباحث أن المنظم السعودي قد تطرق إلى جريمة الاختراق المالي للمصارف الإلكترونية محل البحث في نظام مكافحة جرائم المعلوماتية وذلك من خلال تجريم الوصول دون مسوغ نظامي صحيح إلى البيانات البنكية أو الائتمانية أو الحصول على المعلومات أو الأموال والاستيلاء عليها، وينطبق ذلك على الإختراق والدخول غير المشروع والحصول على البيانات البنكية أو الائتمانية أو الحصول على البيانات المالية للعملاء، وكذلك تحويل الأموال من حساب لآخر وتحويل المبالغ المالية بطرق غير مشروعة والاستيلاء عليها، حيث يتم ذلك من خلال فعل الدخول غير المشروع وبدون مسوغ قانوني صحيح والحصول على تلك البيانات.

ثانياً: إصدار نظام الاتصالات ولائحته التنفيذية

أصدرت المملكة العربية السعودية نظام الاتصالات بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422هـ، والذي أشار إلى المخالفات الخاصة بأحكام النظام في المادة السابعة والثلاثون والتي يعد منها الإضرار بشبكات الاتصالات العامة أو الإعتداء عليها أو الإستفادة غير المشروعة منها [20] كما أشارت اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه، إلى تجريم الإختراق وذلك من خلال ما تضمّنه من النص في المادة الأولى منه على أنه " - يعتبر الإختراق إحدى صور إساءة استخدام شبكة الاتصالات ويكون بذلك مخالفة وفقا للمادة السابعة والثلاثون من النظام وتنطبق عليها الإجراءات المنصوص عليها في هذه اللائحة لمعالجة المخالفات....."[21].

وقد أشار المنظم إلى العقوبات المقررة لتلك المخالفة أو الشروع فيها أو حتى المساعدة وذلك من خلال ما تضمنه بالنص على أن "..... يعاقب من ارتكب أياً من المخالفات المنصوص عليها في المادة (السابعة والثلاثون) من هذا النظام أو شرع في ارتكابها أو ساعد فيها بغرامة مالية لا تتجاوز خمسة وعشرين مليون ريال ويعاقب المخالف بالعقوبة نفسها إذا لم ينته عن المخالفة أو لم يصححا خلال المهلة التي تحددها اللجنة المنصوص عليها في الفقرة (5) من هذه المادة ويكون تحصيل الغرامة مشمولاً بالنفاذ المعجل ولهيئة استعادة أي عائد مالي حصل عليه المخالف نتيجة المخالفة...." [22].

ويرى الباحث أن المنظم السعودي قد تطرق إلى جريمة الاختراق المالي للمصارف الإلكترونية محل البحث في نظام الاتصالات من خلال تجريم الاختراق والإضرار بشبكات الاتصالات العامة أو الإعتداء عليها أو الإستفادة غير المشروعة، حيث ينطبق ذلك على الدخول غير المشروع والاستفادة غير المشروعة من حيث الحصول على البيانات البنكية أو البطاقات الإئتمانية وتحويل الأموال بطرق غير مشروعة وبالتالي تحقيق الاستفادة غير المشروعة من تلك الدخول.

كما نص على اعتبارها مخالفة من المخالفات التي يتم العقاب عليها بعقوبة الغرامة المالية بالإضافة إلى إقرار النفاذ المعجل لتلك الغرامة فضلاً عن الحق في استعادة العائد المالي الذي حصل عليه المخالف نتيجة المخالفة.

ثالثاً: جهات التحقيق وكذلك الدعم والمساعدة الفنية للجهات الأمنية

تضمن نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428هـ النص على أن تتولى هيئة الاتصالات وتقنية المعلومات الدعم والمساعدة الفنية للجهات الأمنية في العمل على ضبط هذا النوع من الجرائم بالإضافة إلى تقديم

---

[20] المادة السابعة والثلاثون من نظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب المرسوم الملكي رقم (74) بتاريخ 5 / 3 / 1422ه وتعديلاته.

[21] المادة السابعة والثمانون من اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب قرار وزير الإتصالات وتقنية المعلومات ال رقم (4) بتاريخ 29 / 1 / 1442ه.

[22] المادة السابعة والثلاثون من نظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب المرسوم الملكي رقم (74) بتاريخ 5 / 3 / 1422ه وتعديلاته.

الدعم والمساعدة أيضا أثناء مرحلتي التحقيق والمحاكمة وذلك من خلال النص على أن " تتولى هيئة الاتصالات وتقنية المعلومات وفقًا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة "[23].

كما أشار المنظم إلى التحقيق والإدعاء في هذا النوع من الجرائم وذلك من خلال النص على أن" تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام"[24].

وبالتالي يجب على المحقق بمجرد وصـــول البلاغ إليه والعلم بوقوع جريمة معينة من تلك الجرائم أن يبادر بفحص هذا البلاغ وتمحيص المضمون الخاص به والتأكد منه وتسجيل التفاصيل الخاصة به في السجل المعد لذلك ثم بعد ذلك يتم مباشرة الإجراءات الخاصة بالتحقيق والبحث عن الأدلة من خلال الانتقال إلى مكان الحادث وإجراء المعاينة والمحافظة على الأدلة وضبط كل ما يتعلق بتلك الجريمة والقيام إلى الإجراءات اللازمة للتحقق من الجريمة (العامري، 2022 م، ص356/357).

ونشير في هذا المجال إلى لجنة النظر في مخالفات نظام الإتصالات والتي تتولى النظر في المخالفات المنصوص عليها في نظام الاتصالات وكذلك الحق في استدعاء المنسوب إليه المخالفة وسماع أقوله وضبها في محضر مخصص لذلك حيث تضمنت اللائحة التنفيذية لنظام الإتصالات النص على أن " – ينعقد اختصاص اللجنة لنظر المخالفات المنصوص عليها في نظام الاتصالات وإذا كانت المخالفة المرفوعة للجنه لا تقع تحت اختصاصها فعليها ان تصرف النظر عنها....."[25].

وتجدر الإشارة إلى ما تضمنته اللائحة التنفيذية لنظام الإتصالات من الإشارة إلى القيام بوضع الإجراءات الضرورية الهادفة إلى تحقيق الحماية وكذلك العمل على الحد من الإختراقات وإصـدار التعليمات اللازمة التي تكفل تحقيق ذلك، وذلك من خلال النص على أن" تقوم الهيئة وفقاً لأنظمتها بوضـــع الإجراءات الضـــرورية الهادفة إلى تحقيق الحماية والحد من الإختراقات وإصـــدار التعليمات اللازمة لذلك....."[26].

بالإضافة إلى الآليات النظامية في مجال مكافحة جرائم المعلوماتية، هناك العديد من الجهود المبذولة من القطاع الخاص في المملكة العربية السعودية وكذلك قطاع الأفراد والمؤسسات ومنها إنشاء مركز خدمة (رقيب) ويعتبر أول مركز أمني لإدارة أمن المعلومات بالمملكة حيث تم إطلاقه عام 2008 وتجدر الإشارة إلى أنه يقوم بتقديم العديد من الخدمات منها أنظمة منع التطفل والدخول غير المشروع على الأنظمة المعلوماتية، وكذلك الخدمات الخاصة بإدارة الثغرات الأمنية ومخاطر أمن المعلومات وغير ذلك من الخدمات الخاصة بمكافحة جرائم المعلوماتية، ومن الجهود المبذولة أيضاً تأسيس شركة سعودية متخصصة بأنظمة الدفاع والفضاء والأمن السيبراني وهي شركة ريثون العربية السعودية والتي تأسست بموجب اتفاقية تعاون بين شركة ريثون الأمريكية ومع الشركة السعودية للصناعات العسكرية وذلك بغرض تقديم جميع الخدمات المتعلقة بمكافحة جرائم المعلوماتية والأمن السيبراني (المالكي، 2024، ص. 59–60).

---

(23) المادة الرابعة عشر من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

(24) المادة الخامسة عشر من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428ه الصادر بموجب قرار مجلس الوزراء رقم (79) بتاريخ 7 / 3 / 1428ه.

(25) المادة الثامنة والثمانون من اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب قرار وزير الإتصالات وتقنية المعلومات ال رقم (4) بتاريخ 29 / 1 / 1442ه.

(26) المادة الثامنة والثلاثون من اللائحة التنفيذية لنظام الإتصالات الصادر بالمرسوم الملكي رقم م/12 بتاريخ 12 / 3 / 1422ه الصادرة بموجب قرار وزير الإتصالات وتقنية المعلومات ال رقم (4) بتاريخ 29 / 1 / 1442ه.

المطلب الثاني: الآليات والجهود الدولية لمكافحة الجرائم المعلوماتية

هناك العديد من الجهود الدولية المبذولة في مجال مكافحة الجرائم المعلوماتية وجرائم الاختراق والدخول غير المشروع، حيث تطرقت العديد من الاتفاقيات الدولية إلى تجريم أفعال الوصول غير المشروع والسرقة والاحتيال المتعلقان بأنظمة تكنولوجيا المعلومات، بالإضافة إلى وضع العديد من النصوص المتعلقة بالملاحقة والمقاضاة بمكافحة هذا النوع من الجرائم، ونذكر في هذا المجال ما تضمنته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تعتبر من أهم الاتفاقيات التي جاءت كنتيجة للجهود التي قامت بها جامعة الدول العربية في مجال مكافحة جرائم النظم المعلوماتية حيث عنيت بمواجهة العديد من الجرائم وألزمت من خلالها الدول العربية بإدخال العديد من التعديلات على التشريعات الخاصة بها لتجريم تلك الأفعال حيث تضمنت في المادة السادسة منها الإشارة إلى جريمة الدخول غير المشروع، وذلك من خلال النص على أنها " 1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به 2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبينات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

ب- الحصول على معلومات حكومية سرية " (المالكي، 2024، ص. 52–53).

وما تضمنته اتفاقية بودابست والتي تعد أولى الاتفاقيات الدولية لتجريم كافة أشكال الجرائم الإلكترونية والتي تضمنت مكافحة جرائم الحاسبات المعلوماتية والاتصالات، كما تعد من أوئل الاتفاقيات التي واجهت جرائم الدخول غير المشروع، وذلك من خلال ما تضمنته من تجريم النفاذ غير المشروع بالنص في مادتها الثانية على أن " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني إذا ما ارتكب عمداً وبغير حق النفاذ الكامل أو الجزئي لنظام كمبيوتر.

يجوز لطرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية بنية الحصول على بيانات الكمبيوتر أو بأي نية غير صادقة أخرى أو في ارتباط بنظام كمبيوتر متصل بنظام حاسوبي آخر" (اتفاقية بودابست بشأن الجريمة الإلكترونية، 2001، المادة 2؛ المالكي، 2024، ص. 52–53؛ عبد الهادي، 2020/2019، ص. 33؛ زرقان، 2016/2015، ص. 50).

وبالإضافة إلى اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية والتي تهدف إلى تشجيع وتعزيز التعاون الدولي في مجال منع ومكافحة الجريمة السيبرانية وذلك على نحو أكثر فعالية وكفاءة، كما تعمل على دعم وتيسير توفير المساعدة التقنية وبناء القدرات، بهدف منع ومكافحة الجريمة السيبرانية وذلك من خلال ما تضمنته من تجريم الوصول غير المشروع من خلال النص على أن" تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرِّم بموجب قانونها الداخلي الوصول دون وجه حق إلى نظام تكنولوجيا معلومات واتصالات بأكمله أو إلى أي جزء منه، عندما يُرتكب هذا الفعل عمدا.

2 - يجوز للدولة الطرف أن تشترط أن يكون الفعل الإجرامي قد ارتُكب من خلال انتهاك لتدبير أمني، بقصد الحصول على بيانات إلكترونية أو بأي قصد غير نزيه أو إجرامي آخر، أو فيما يتعلق بنظام تكنولوجيا معلومات واتصالات متصل بنظام تكنولوجيا معلومات واتصالات آخر"[27].

وذلك بالإضافة إلى ما تضمنته من الإشارة إلى السرقة أو الاحتيال المتعلقان بنظام تكنولوجيا المعلومات واتصالات وذلك من خلال النص على أن " تعتمد كل دولة طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى لكي تجرّم بموجب قانونها الداخلي التسـبب في

[27] المادة (7) من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية

إلحاق خسارة بممتلكات الغير عندما يُرتكب هذا الفعل عمدا ودون وجه حق، عن طريق:

(أ) أي إدخال أو تحوير أو حذف أو إخفاء لبيانات إلكترونية

(ب) أي تدخل في عمل نظام تكنولوجيا معلومات واتصالات

(ج) أي خداع يتعلق بالظروف الواقعية يحدث عن طريق نظام تكنولوجيا معلومات واتصالات ويحمل شخصا ما على القيام أو الامتناع عن القيام بفعل لم يكن لولا ذلك سيقوم به أو يمتنع عن القيام به وذلك بقصد الاحتيال أو بقصد غير نزيه لكي يحصل من يرتكب ذلك لنفسه أو لشخص آخر، دون وجه حق، على كسب مالي أو على ممتلكات أخرى"[28].

فضلاً عما تضمنته الإتفاقية من الإشارة إلى الملاحقة والمقاضاة والعقوبات الخاصة بمكافحة الجريمة السيبرانية وجرائم تقنية المعلومات، وذلك من خلال النص على أن"1 - تجعل كل دولة طرف ارتكاب أي فعل مجرَّم وفقا لهذه الاتفاقية خاضعا لعقوبات فعالة ومتناسبة ورادعة تُراعى فيها جسامة ذلك الفعل الإجرامي.

2 - يجوز لكل دولة طرف أن تعتمد، وفقا لقانونها الداخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار الظروف المشددة فيما يتعلق بالأفعال المجرمة وفقا لهذه الاتفاقية، بما في ذلك الظروف التي تؤثر في البنى التحتية الحيوية للمعلومات.

3 - تسعى كل دولة طرف إلى ضمان أن أي صلاحيات قانونية تقديرية، يتيحها قانونها الداخلي فيما يتعلق بملاحقة الأشخاص قضائيا لارتكابهم أفعالا مجرَّمة وفقا لهذه الاتفاقية، تمارس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القانون التي تُتخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة الردع عن ارتكابها....."[29].

5. الخاتمة:

الحمد لله الذي بنعمته تتم الصالحات والصلاة والسلام على المبعوث رحمة العالمين سيدنا محمد وعلى آله وصحبه ومن اهتدى بهديه إلى يوم الدين. أما بعد

هذا البحث جاء تحت عنوان جريمة الإختراق المالي للمصارف الإلكترونية - معالجة النظام السعودي والضوابط الشرعية، وتمثلت أهمية موضوعه فيما يثيره موضوع الإختراق المالي للمصارف الإلكترونية من إشكاليات عملية في المملكة العربية السعودية، وكيفية معالجة النظام السعودي لجريمة الإختراق المالي لتلك المصارف، وقد سعى الباحث لحل مشكلته التي تمثلت في ماهية جريمة الإختراق المالي للمصارف الإلكترونية وكيفية معالجة النظام السعودي لتلك الجريمة وذلك من خلال تحديد أسباب ودوافع ارتكاب جريمة الاختراق المالي للمصارف الإلكترونية وبيان التكييف الفقهي والنظامي لها والوقوف على أركان جريمة الإختراق المالي للمصارف الإلكترونية والعقوبات المقررة لها، هذا واقتضت طبيعة موضوع البحث اتباع المنهج الوصفي والمنهج الاستقرائي التحليلي، حيث تناول النصوص النظامية الخاصة بجريمة الإختراق المالي للمصارف الإلكترونية وتوضيح العقوبات المقررة لها، وقد تم تناول الموضوع بتقسيمه إلى مبحث تمهيدي وثلاثة مباحث الأول بعنوان التأصيل الفقهي والنظامي لجريمة الإختراق المالي للمصارف الإلكترونية، والثاني أركان جريمة الإختراق المالي للمصارف الإلكترونية والثالث بعنوان آليات مكافحة جريمة الإختراق المالي للمصارف الإلكترونية وقد تم التوصل إلى بعض النتائج التي تجدر الإشارة إليها في هذا المقام فضلاً عن بعض التوصيات التي نود الإشارة إليها.

[28] المادة (13) من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية

[29] المادة (13) من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.

1.5. النتائج:

1. يمكن تعريف جريمة الإختراق المالي للمصارف الإلكترونية بأنها الدخول غير المشروع للأنظمة والمواقع الإلكترونية بأي طريقة كانت، باستخدام برامج متخصصة للإختراق والوصول غير المصرح به إلى الحسابات البنكية أو بطاقات الائتمان والحصول على بيانات العملاء السرية، لاستخدمها بالتحايل على المواقع الإلكترونية أو القيام بعمليات التحويل من حساب إلى آخر بشكل غير مشروع وذلك بهدف الحصول على أموالهم وسرقة بياناتهم المالية.
2. أن جريمة الإختراق المالي للمصارف الإلكترونية والتي يتم من خلالها اختراق الحسابات البنكية وبطاقات الإئتمان وسرقة البيانات المالية وتحويل الأموال بطرق غير مشروعة، تعتبر جريمة من الجرائم المعاقب عليها في الشريعة الإسلامية ويمكن تكييفها على أنها جريمة سرقة وتعبر من الجرائم الحدية التي يقام الحد على مرتكبها إذا توافرت الشروط وتم الحصول على المال الذي بلغ النصاب.
3. أن المنظم السعودي قد جرم فعل الإختراق والذي يتمثل في الدخول غير المشروع بأي طريقة، على أي جزء من شبكة اتصالات أو محتوياتها، من قبل أي شخص لأي غرض أو هدف، سواء نتج عن ذلك تعطيل أو تخريب أو لم ينتج عنه شيء، وذلك باعتبارها إحدى صور إساءة استخدام شبكة الاتصالات، وأشار ضمن النصوص الواردة في اللائحة التنفيذية لنظام الاتصالات إلى اعتبارها مخالفة من مخالفات أحكام النظام.
4. تتطلب جريمة الإختراق المالي للمصارف الإلكترونية شرطاً مفترضاً يتمثل في محل الجريمة ويتضمن وجود الكيان المادي للنظام الآلي لمعالجة المعلومات والنظام المعلوماتي والبيانات المالية للمصارف الإلكترونية وذلك بالقياس على مفهوم الاختراق الوارد في اللائحة التنفيذية لنظام الاتصالات والقياس على الجرائم المعلوماتية ومنها جريمة الدخول غير المشروع إلى النظام المعلوماتي.
5. أن المنظم السعودي قد تطرق إلى جريمة الاختراق المالي للمصارف الإلكترونية محل البحث في نظام الاتصالات من خلال تجريم الاختراق والإضرار بشبكات الاتصالات العامة أو الإعتداء عليها أو الإستفادة غير المشروعة، كما أشار إلى الجريمة أيضاً في نظام مكافحة جرائم المعلوماتية، من خلال تجريم الدخول غير المصرح به بغرض الإستيلاء على الأموال أو الدخول إلى البطاقات البنكية، أو الإئتمانية وهو ما ينطبق بدوره على جريمة الاختراق المالي للمصارف الإلكترونية.

2.5. التوصيات:

1. لابد أن يتضمن نظام مكافحة جرائم المعلوماتية تعريفاً صريحاً ومفهوماً واضحاً لجريمة الإختراق المالي للمصارف الإلكترونية وأن يتضمن في تعريف الدخول غير المشروع الإشارة إلى باقي الحالات الأخرى التي تتمثل في البقاء بشكل غير مشروع عند وجود تصريح سابق أو الحالة التي يتم فيها تجاوز التصريح وعدم الاقتصار في تعريفه على الحالة الخاصة بالجاني الذي لا يتمتع بتصريح الدخول وذلك حتى لا يكون المجال متاحاً لإباحة الطرق والحالات الأخرى.
2. ضرورة وضع تنظيم شامل ونصوص مباشرة وصريحة تعالج جريمة الإختراق المالي للمصارف الإلكترونية من حيث بيان الكيان القانوني للجريمة وتحديد الأركان الخاصة بها وتحديد الأفعال التي تشكل ركناً مادياً لجريمة الإختراق المالي للمصارف الإلكترونية ووضع العقوبات المناسبة لها والحالات والظروف المشددة لها.
3. ضرورة وضع العديد من النصوص النظامية المستحدثة فيما يتعلق بالتحقيق والإدعاء والإجراءات المتعلقة بالتفتيش والمعاينة حتى تتوافق مع هذا النوع من الجرائم المستحدثة لمواكبة التطور التقني والتكنولوجي وبما يتوافق مع طبيعة الدليل المستمد من الجرائم المعلوماتية وكذلك تنظيم اختيار الأشخاص والجهات التي تقوم بالضبط والتحقيق في هذا النوع من الجرائم المستحدثة.
4. ضرورة تحديث الأنظمة الخاصة بالحماية بشكل دوري وذلك لمراقبة الأنشطة غير الإعتيادية داخل الحسابات ومواكبة التهديدات

الحديثة وكذلك ضرورة توفير قنوات تواصل سريعة وفورية للإبلاغ عن أي محاولة للاحتيال.

5. ضرورة التوثيق الكامل للأدلة والإحتفاظ بالأدلة الرقمية والتي تتمثل في لقطات الشاشة وكذلك تسجيلات الدخول غير المصرح بها وكافة الأدلة التي تساعد في إثبات الجريمة.

6. ضرورة وضع العديد من الضوابط الرقابية للعمليات المصرفية الإلكترونية واتباع العديد من المبادئ الرشيدة لإدارة المخاطر التي تتعلق بتقديم الخدمات من خلال شبكة الاتصال الإلكترونية، والتي تتضمن تقسيم المخاطر والرقابة عليها ومتابعتها.

7. تحسين كفاءة وفعالية الرقابة المصرفية وإمكانية تطبيق نظم رقابية جديدة تعمل على الحد من ارتكاب تلك الجرائم ومواجهة التغييرات والتحديات السائدة في بيئة الأعمال المصرفية الإلكترونية والمخاطر التي تواجهها.

8. ضرورة وضع العديد من القواعد والضوابط لحماية العمليات المصرفية الإلكترونية والعمل على ابتكار وسائل حديثة لحماية أمن وسرية المعلومات والمراسلات عن طريق تشفيرها وكذلك حماية الشبكات الداخلية والمواقع من خلال جدران الحماية.

9. ضرورة التعاون بين السلطات الإشرافية على المستوى الدولي بهدف تقوية الدعائم الرقابية في كافة الأنظمة القانونية الدولية وتوسيع الممارسات الرقابية السليمة والعمل على استحداث أساليب متطورة بشأن إدارة مخاطر العمليات المصرفية الإلكترونية.

10. ضرورة الإهتمام بالتوعية القانونية عبر وسائل التواصل الاجتماعي والمؤتمرات وكذلك ضرورة التوعية والإرشاد والتثقيف بخطورة هذا النوع من الجرائم لتجنب الوقوع فيها.

6. المصادر والمراجع:

1.6. المصادر:

القرآن الكريم

2.6. التشريعات والاتفاقيات:

اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.

اللائحة التنفيذية لنظام الاتصالات. الصادرة بموجب قرار وزير الاتصالات وتقنية المعلومات رقم (4) بتاريخ 1442/1/29هـ.

نظام الاتصالات. الصادر بالمرسوم الملكي رقم (م/12) بتاريخ 1422/3/12هـ، والمعدل بالمرسوم الملكي رقم (74) بتاريخ 1422/3/5هـ.

نظام مكافحة جرائم المعلوماتية. الصادر بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ، وبقرار مجلس الوزراء رقم (79) بتاريخ 1428/3/7هـ.

3.6. الكتب والأبحاث العلمية:

أبو زهرة، محمد بن عبد، (1419 هـ/ 1998 م). الجريمة والعقوبة في الفقه الإسلامي، الجريمة، دار الفكر العربي، القاهرة.

الحاج، شراديد محمد، (2014/2013م). مخاطر العمليات المصرفية الإلكترونية، دراسة مقارنة، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر.

الحذيفي، أمين محمد أحمد، (2022م). جريمة الدخول غير المشروع إلى المواقع الإلكترونية في النظام السعودي، مجلة القانون الدولي للدراسات البحثية.

السكر، سلطان فياض محمد السكر، (2022م). جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير، ع21، جامعة الشرق الأوسط.

الشبول، شاكر أحمد محمود، (2023م). الحماية الجنائية لوسائل الدفع الالكتروني، دراسة مقارنة، مجلة جرش للبحوث والدراسات، المجلد 24، ع2.

الصالح، قشي محمد؛ عمار، قرفي، رملي، حمزة، (2018م). البنوك الإلكترونية مخاطرها وطرق الحماية منها مع الإشارة لحالة الجزائر، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بو الصوف – ميلة.

الطناحي، محمود محمد، (1428 هـ/ 2008 م). من أسرار اللغة في الكتاب والسنة، معجم لغوي ثقافي، ج1، المكتبة المكية، المملكة العربية السعودية.

الطويلي، أحمد أحمد صالح، (2019م). التكييف الفقهي والقانوني لجريمة السرقة الإلكترونية، البطاقة الائتمانية نموذجاً للتطبيق، المجلة الإلكترونية الشاملة، ع15.

العامري، سليمان بن إبراهيم بن أمان، (2022م). جريمة الدخول غير المشروع على المواقع الإلكترونية المتعلقة بأمن الدولة، دراسة تأصيلية تطبيقية في النظام السعودي، المجلة الأكاديمية للأبحاث والنشر العلمي، ع44.

العجمي، عبد الله دغش، (2014م). المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط.

العنزي، ممدوح بن رشيد بن مشرف، (2022م). معاينة الجانب الموضوعي للإحتيال من خلال المواقع الإلكترونية في النظام السعودي مقارناً بالقانونيين المصري والكويتي، المجلة العربية للدراسات الأمنية، عدد38.

القاسمي، إبراهيم محمد، (2018م). جرائم الدخول غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون اتحادي رقم (5) لسنة (2012) في شأن كافحة جرائم تقنية المعلومات) "، رسالة ماجستير، جامعة الإمارات العربية المتحدة.

القحطاني، مداوي سعيد مداوي، (2016م). الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجتهتها، مجلس التعاون لدول الخليج العربية، وزارة الداخلية - قطر، 2016م.

المالكي، محمد خالد، (2024م). التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وجهود المملكة في مكافحتها، المجلة الدولية للعلوم المالية والإدارية والاقتصادية، الاصدار3، ع10.

الماوردي، أبي الحسن علي بن محمد بن حبيب، (1409 هـ/ 1989 م). الأحكام السلطانية والولايات الدينية، مكتبة دار ابن قتيبة، الكويت، ط1.

حسني، محمود نجيب، (1962م). شرح قانون العقوبات، القسم العام- النظرية العامة للجريمة، دار النهضة العربية، القاهرة.

رضا، أحمد، (1377ه/1958م). معجم متن اللغة، المجلد الأول، دار مكتبة الحياة، بيروت.

رقية، منصوري، أسماء، عبد المالك، (2014/2013م). الخدمات المصرفية الإلكترونية مذكرة التخرج لشهادة الليسانس، جامعة أبي بكر بلقايد.

زكريا، أبي الحسين أحمد بن فارس، (1399ه/1979 م). معجم مقاييس اللغة، دار الفكر.

زكرياء، شناف، فؤاد، بودربالة، (2022/2021م). الخدمات الإلكترونية للبنوك- أخطارها وطرق الحماية منها، دراسة حالة المؤسسة العربية والمصرفية (ABC) الأردن، رسالة ماجستير، معهد العلوم الاقتصادية والتجارية وعلوم التسيير، الجزائر.

شريهان، ممدوح حسن، (2020م). الجرائم المعلوماتية وسبل مواجتهها على المستويين الوطني الدولي، المجلة الإلكترونية الشاملة، ع21.

شناف، زكرياء، بودربالة، فؤاد، (2022/2021م). الخدمات الإلكترونية للبنوك-أخطارها وطرق الحماية منها -دراسة حالة المؤسسة العربية المصرفية (ABC) الأردن، رسالة ماجستير، اقتصاد نقدي وبنكي معهد العلوم الاقتصادية والتجارية وعلوم التيسيير.

عبد الهادي، حشيفة، (2020/2019م). التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية.

عمايره، محمد منذر طه، (2023م/1445ه). التعاون الدولي في مواجهة الجريمة الإلكترونية، رسالة ماجستير، جامعة القدس، عمادة الدراسات العليا.

عمر، أحمد مختار، (2008م). معجم اللغة العربية المعاصرة، المجلد الأول، عالم الكتاب، القاهرة.

عوده، عبد القادر، (1968م). التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، ج1، دار الكاتب العربي، بيروت.

عياش، راشـــد، (2024م). جريمة الاختراق وتأثيرها على الشـــبكة الإلكترونية في ظل القانون الفلســـطيني، مجلة القدس للبحوث الأكاديمية، ع3.

غنام، محمد جواد محمد، (2023م). إجراءات التحقيق الإبتدائي في الجريمة الإلكترونية، دراسـة مقارنة، رسـالة ماجسـتير، الجامعة العربية الإمريكية.

محمد، أمين مصطفى، (2016م). قانون العقوبات، القسم العام، دار المطبوعات الجامعية، الإسكندرية.

مشري، فريد، رياض، لمزاودة، قاجة، آمنة، (د.ت). الحماية القانونية لوسائل الدفع الالكتروني – الجزائر نموذجاً، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية 23 و24 أفريل 2018، المركز الجامعي عبد الحفيظ بوالصوف – ميلة.

هشام، زرقان، (2016/2015م). النظام القانوني لبطاقات الدفع الالكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية.

Doi: http://doi.org/10.52133/ijrsp.v7.78.3