الدراسة الرابعة:
الأوصاف القانونية لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية - دراسة مقارنة بين قوانين دول مجلس التعاون الخليجي والقانون الأردني[1]

د. عبدالله محمد خنجر أحجيله[2]
وأميرة سعيد الشماسي

Abstract

The Legal characterizations of unauthorized access to electronic banking and financial information. A comparison between the law in Jordan its counterpart in GCC countries"

This study revolves around the legal characterizations of unauthorized access to electronic banking and financial information under the laws of GCC countries; compared against the Jordanian law. According to the UAE's ICT crime law, intent is not required for the misdemeanor of unauthorized access to banking and financial

[1] جزء من هذا البحث (ما نسبته حوالي 20–30% من محتوى البحث) مستخلص من رسالة ماجستير، بعنوان جرائم الاعتداء على المعلومات المالية والمصرفية في قانون الجرائم الإلكترونية الأردني – دراسة مقارنة، جامعة اليرموك،2021، للطالبة أميرة الشماسي، وإشراف الدكتور عبدالله احجيله.

[2] أستاذ مشاركAssociate Professor جامعة اليرموك– كلية القانون– قسم القانون العام.

information to constitute, while the Bahraini ICT crime law didn't explicitly provide for the offense of unauthorized access to such information.

Additionally, the Qatari Cybercrime Law did not characterize such an offense as a felony. Furthermore, the Saudi cybercrime ordinance have imposed an extenuated penalty for such an offense, while the Jordanian Cybercrime Law; under Article (6) thereof, have imposed a misdemeanor penalty for such an offense, but at the same time, it punished it under Article 7; with reference to Article 6 of the same law, with a felony penalty.

This study adopts a descriptive analytical approach, in addition to a comparative approach between the laws of GCC countries and its counterpart in Jordan. The study has concluded several findings, the most important of which is that: there are some regulatory shortcomings in the Qatari, Bahraini and Saudi laws regarding the offense in question, as such laws omit the criminal characterization of this offense when the banking and financial information in question is stored in a core banking system (banking IT system). Another finding of the study suggests that there is no contradiction between Articles (6 and 7) of the Jordanian Cybercrime Law.

In conclusion, the study makes several recommendations around addressing the legislative shortcomings in some of the GCC countries laws; regarding the offense of unauthorized access to electronic banking and financial information.

Keywords: legal description, felony, misdemeanor, penalties, information system, banking and financial information, Jordanian, Emirati, Kuwaiti, Omani, Qatari, Bahraini, Saudi.

المقدمة

1. موضوع الدراسة:

يُعَدُّ القطاع المصرفي والمالي أحدَ أهمِّ القطاعات في الاقتصاديات الحديثة، ليس فقط لدوره المُهِمِّ في تمويل الاستثمار الذي يُمثل عَصَبَ النشاط الاقتصادي؛ بل لكونه أصبح يُشكل حَلْقَةَ اتصالٍ مُهِمَّةٍ مع العالم الخارجي، لذلك سَعَت البنوك والشركات المالية إلى مواكبة التطور التكنولوجي، وذلك من خلال تقديم خِدْماتِها المصرفية بوسيلةٍ إلكترونية؛ ذلك أنَّ هذه الوسيلة تُتيحُ للعملاء الكثيرَ من المزايا، فهي توفِّرُ لهم الجهد والراحة والوقت. وتحرِصُ هذه البنوك والشركات على أن يكون هناك درجة عالية من الأمان التقني؛ وذلك حمايةً للمعلومات المصرفية والمالية وخصوصية عملائها، إلا أنه وعلى الرغم من ذلك، فإنَّ المعاملات المالية والمصرفية الإلكترونية محفوفةٌ بالمخاطر التقنية.

ومن هنا تنبهت قوانين مكافحة الجرائم الإلكترونية في دول مجلس التعاون الخليجي وقانون الجرائم الإلكترونية الأردني لهذه المخاطر، وحَرِصَت على توفير قدراً من الحماية الجنائية للمعلومات التي تتعلق بالمعاملات المصرفية أو المالية الإلكترونية، وذلك من خلال تجريم فِعْلَ الحصولِ غير المشروع على المعلومات المالية والمصرفية والمعاقبة عليه.

2. إشكاليات الدراسة:

تتمثل إشكاليات الدراسة بما يلي:

- لم تشترط المادة (12) من قانون مكافحة جرائم تقنية المعلومات الإماراتي لقيام جنحة الحصول غير المشروع على المعلومات المالية والمصرفية الإلكترونية توافر القصد.
- لم ينص قانون جرائم تقنية المعلومات البحريني صراحةً على جريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية لا بوصفٍ جنائي ولا بوصفٍ جنحيٍ.
- لم ينص قانون مكافحة الجرائم الإلكترونية القطري على جناية الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية، إذا تم الحصول عليها من نظام معلومات إلكتروني مصرفي.

- عاقبت المادة (4) من نظام مكافحة الجرائم المعلوماتية السعودي على جريمة الحصول غير المشروع بوسيلةٍ إلكترونية، على المعلومات المصرفية والمالية الإلكترونية، بعقوبة مخففة، وذلك حتى ولو تم الحصول عليها من نظام معلومات إلكتروني مصرفي، وذلك خلافاً لبعض القوانين المقارنة التي عاقبت على ذلك، بعقوبةٍ جنائية كالقانون الإماراتي والكويتي والعُماني والأردني.
- جَرَّمَ المُشرِّعَ الأردنيَّ في المادة (6) من قانون الجرائم الإلكترونية، واقِعةَ الحصول غير المشروع بوسيلةٍ إلكترونية، على معلومات تتعلق ببطاقات الائتمان أو بتنفيذ المعاملات المالية أو المصرفية الإلكترونية، وعاقب على هذه الواقعة بعقوبة جُنحية، وفي الوقت ذاته جرَّمَ ذات الواقعة في المادة (7 وبالإحالة على المادة 6) من القانون السالِفِ ذِكْرُه، وعاقب عليها بعقوبةٍ جنائية، لذلك لم تستقِرَّ أحكام القضاء الأردني بشأنِ تكييفِ هذه الواقعة، فتارةً يُكيِّفُها بأنها جُنحة، وتارةً أخرى يُكيِّفُها بأنها جناية.

3. تساؤلات الدراسة:

تثيرُ إشكاليات الدراسة التساؤلاتِ الآتية:

- ما الأوصاف القانونية لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية في قوانين دول مجلس التعاون الخليجي والقانون الأردني؟
- هل سارت قوانين دول مجلس التعاون الخليجي والقانون الأردني على وتيرةٍ واحدة بشأن التجريم والمعاقبة على واقعة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية؟
- ما الأركان المطلوبة لقيام جناية وجنحة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية في قوانين دول مجلس التعاون الخليجي والقانون الأردني؟
- هل ثمَّةَ تنازُعٌ حقيقيٌّ بين نَصَّي المادتين (6 و7) من قانون الجرائم الإلكترونية الأردني؟ أم إنَّ الأمر لا يعدو كونَهُ تنازُعًا ظاهريًّا؟
- ما مدى استقرار أحكام القضاء الأردني، بشأن تكييف واقعة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية؟

4. أهمية الدراسة:

تكمُنُ أهمية هذه الدراسة في أنها حددت الأوصاف القانونية لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية في قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون الخليجي وفي قانون الجرائم الإلكترونية الأردني، كما أنها أوضحت أركان وعقوبات هذه الجريمة في جميع القوانين المقارنة، ورصدت مواطن القصور التشريعي في هذه القوانين، وقدمت مقترحات لمعالجة هذا القصور.

وتبرز أهمية هذه الدراسة أيضاً في أنها تصدت لمعالجة بعض الإشكاليات العملية، ولا سيَّما إشكالية التطبيق القضائي، بشأن تكييف واقعة الحصول غير المشروع بوسيلةٍ إلكترونية، على معلومات تتعلق ببطاقات الائتمان أو تستخدم في تنفيذ المعاملات المصرفية والمالية الإلكترونية.

5. أهداف الدراسة:

تهدف هذه الدراسة إلى بيان الأوصاف القانونية لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية في قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون الخليجي وفي قانون الجرائم الإلكترونية الأردني، ، كما وتهدف إلى بيانِ أركان وعقوبات الجريمة السالف ذكرها بوصفيها الجنائي والجنحي، وتهدف أيضاً إلى رصد مواطن القصور التشريعي بشأن هذه الجريمة في جميع القوانين المقارنة وتقديم المقترحات لمعالجة هذا القصور.

وأخيرًا تهدف الدراسةُ إلى بيانِ مدى استقرار أحكام القضاء الأردني بشأن تكييف واقعة الحصول غير المشروع بوسيلةٍ إلكترونية، على معلومات تتعلق ببطاقات الائتمان أو تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية.

6. منهجية الدراسة:

اتبع الباحثان في هذه الدراسة المنهجين الوصفي والتحليلي، وذلك من خلال استعراض وتحليل نصوص قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون الخليجي ونصوص قانون الجرائم الإلكترونية الأردني التي تتعلق بجريمة الحصول غير المشروع بوسيلةٍ إلكترونية

على المعلومات المصرفية والمالية الإلكترونية، وذلك وفقاً للقواعد الأصولية في تفسير النصوص القانونية وتطبيقها، وقد اتبع الباحثان أيضاً المنهج المقارن، وذلك بالمقارنة بين قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون الخليجي وبين قانون الجرائم الإلكترونية الأردني، وذلك لبيان مواطن القصور في هذه القوانين بشأن موضوع الدراسة، وتقديم بعض المقترحات لمعالجة القصور التشريعي أينما وجد.

7. خطة الدراسة:

تم تقسيم خطة هذه الدراسة إلى مطلبين، المطلب الأوَّلَ – الوصف الجنائي لجريمة الحصول على المعلومات المصرفية والمالية الإلكترونية في القانون الإماراتي والكويتي والعُماني والأردني، والمطلب الثاني، الوصف الجنحي لجريمة الحصول على المعلومات المصرفية والمالية الإلكترونية في جميع القوانين المقارنة.

وقبل الدخول في تفاصيل هذه الدراسة نود أن نشير إلى ملاحظة هامة ألا وهي، أنه وتجنبًا لتكرار كتابة الجمل الطويلة، فحينما يُذكر مصطلح "نظام المعلومات" فإننا نقصد بذلك نظام المعلومات الإلكتروني، والشبكة المعلوماتية والموقع الإلكتروني أيضاً، وسنتطرق لتعريف هذه المصطلحات وتوضيحها في متن هذه الدراسة إن شاء الله.

المطلب الأول: الوصف الجنائي لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية

يتضح من عدة نصوص جاءت في القانون الإماراتي والكويتي والعُماني والأردني أنه يُشترط لقيام جناية الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية وجود ثلاث أركان، وهي ركن المحل، والركنين المادي والمعنوي، وبتوافر هذه الأركان، يتعين الحكم بالعقوبة الجنائية المقررة لهذه الجناية في القوانين السالفة الذكر، وبناءً على ذلك سنوضح أركان هذه الجناية وعقوباتها في هذه القوانين في فرعين الأول هو، أركان جناية الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية في القانون الإماراتي والكويتي والعُماني

والأردني، والفرع الثاني هو العقوبات المقررة لهذه الجناية في القوانين السالفة الذكر، وسنوضح هذين الفرعين كما هو تالٍ:

▪ الفرع الأول: أركان جناية الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية

يُستفاد من نصوص المواد (4 من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012، و 3 من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015، و 6 من قانون مكافحة جرائم تقنية المعلومات العُماني رقم 12 لسنة 2011، و 6 و7 من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015) – أنه يُشترط لقيام جناية الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية توافُر ثلاث أركان، الركن الأول هوُ ركن المحل، ويتمثل بالمعلومات المصرفية والمالية المخزنة في نظام معلومات مصرفي أو مالي، والركن الثاني، هو المادي، ويتمثل بالحصول على المعلومات المصرفية أو المالية الإلكترونية، وسنستعمل في دراستنا هذه، عبارة (الحصول على المعلومات المستهدفة) اختصاراً لعبارة: (الحصول على المعلومات المصرفية أو المالية الإلكترونية)، والركن الثالث هو المعنوي بصورة القصد، وبناءً على ذلك سنوضح أركان هذه الجناية في القوانين سالفة الذكر كما يلي:

أولاً: ركن المحل في جناية الحصول غير المشروع على المعلومات المستهدفةِ

1– ركن المحل في جناية الحصول غير المشروع على المعلوماتِ المستهدفةِ في القانون الإماراتي

نصت المادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي على أنه: "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواءً كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية".

يُستفاد من هذه المادة بأنه يُشترط لقيام جناية الدخول غير المشروع في نظام معلومات خاص بمنشأة مالية بقصد الحصول على معلومات سرية، توافر ركن المحل، وهو (المعلومات المالية المُخزنة في نظام معلومات إلكتروني خاص بمنشأة مالية.

وقد تم تعريف المنُشأة المالية في المادة (1) من قانون مكافحة جرائم تقنية المعلومات الإماراتي بأنها:" أي منشأة تكتسب وصفها المالي بموجب الترخيص الصادر لها من جهة الاختصاص بالدولة".

وتُعرّف المنشآت المالية المرخصة، بموجب المادة(1) من قانون المصرف المركزي وتنظيم المنشآت والأنشطة المالية الإماراتي رقم (14) لسنة 2018 بأنها: "البنوك والمؤسسات المالية الأخرى المرخصة، وفقاً لأحكام هذا المرسوم بقانون لممارسة نشاط أو أكثر من الأنشطة المالية المرخصة، وتشمل تلك التي تمارس كافة أو جزء من أعمالها وفق أحكام الشريعة الاسلامية، وتكون تلك المنشآت إما مؤسسة داخل الدولة أو في مناطق اختصاص أخرى، ويكون لها فروع أو شركات تابعة أو مكاتب تمثيل داخل الدولة".

ومن الجدير بالتنبيه هنا إن وضع تعريفاً جامعاً مانعاً للمعلومات المصرفية أو المالية أو للأعمال المصرفية أو المالية يُعد أمراً بالغ الصعوبة نظراً لتشعب الأعمال المصرفية والمالية من حيث موضوعها وطبيعتها[1]، وتبعاً لذلك تشعب المعلومات المصرفية والمالية، وقد يكون من الصعب أيضاً تعداد حصري لتخصص الشركات المالية التي تقدم خدمات مصرفية أو مالية، والدليل على ذلك، إن قوانين البنوك في غالبية الدول اكتفت بوضع تعداد للأعمال المصرفية والمالية على سبيل المثال، دون وضع تعريف منضبط ومحدد لها[2]، ولكن يمكن

---

[1] بهذا المعنى يُنظر، حسام الخولى، الحماية الجنائية والمدنية لعمليات البنوك الإلكترونية "دراسة مقارنة"، أطروحة دكتوراه، جامعة عين شمس، مصر، 2016، ص 43، ولمزيد من التفاصيل يُنظر، د. اكرم ياملكي، الأوراق التجارية والعمليات المصرفية، دار الثقافة، عمّان، 2009، ص273.

[2] يُنظر المادة (1) من قانون المصرف المركزي وتنظيم المنشآت والأنشطة المالية الإماراتي رقم 14 لسنة2018، والمادتان (54 و77) من قانون النقد وبنك الكويت المركزي وتنظيم المهنة المصرفية الكويتي رقم32 لسنة1968، والمادة (1) من قانون مصرف قطر المركزي وتنظيم المؤسسات المالية رقم 13 لسنة2012، والمادة (5) من القانون المصرفي العُماني رقم 114 لسنة2000، والمادة (1) من نظام مراقبة البنوك السعودي رقم (م/5) لسنة 1966 (1386 هـ)، والمادة (2) من قانون البنوك الأردني رقم 28 لسنة2000والمادة(2/31) من قانون البنوك الموحد المصري رقم (88) لسنة 2003.

الاستفادة أحياناً من تعداد الأعمال المصرفية والمالية لمعرفة وتحديد طبيعة المعلومات كمعلومات مصرفية أو مالية.

كما أنَّ تحديد فيما إذا كانت المعاملة مالية أم مصرفية، يحتاج لخبراء متخصصين في مجال أعمال البنوك والشركات المالية، ولذلك سنذكر بعض المعاملات المالية التي تتم بمقابل مالي على سبيل المثال، فمنها معاملات دفع الفواتير ودفع الرسوم المالية، ومن المعاملات المصرفية على سبيل المثال، فتح الحسابات البنكية، والتعرُّفُ على أرصدة الحسابات البنكية، وتحديث بيانات عملاء البنوك، وطلبات حصولهم على قروض، وتحويل أموالهم، وإجراء التسويات المالية والمقاصات بين البنوك والعملاء من جهة، وبين البنوك في ما بينها من جهة أخرى[1].

وفي تقديرنا لا أهمية تُذكر للتفرقة بين المعلومات المصرفية وبين المعلومات المالية في مجال حديثنا عن جناية الحصول على المعلومات المصرفية والمالية الإلكترونية، لأن جميعها تصلح لأن تكون محلاً لهذه الجناية، متى كانت هذه المعلومات مخزنة في نظام معلومات خاص في مصرف أو في أي منشأة مالية أخرى.

وعليه، إن المعلومات المالية المخزنة في نظام المعلومات الخاص بالمنشآت المالية تتسع لتشمل المعلومات المصرفية، كالمعلومات التي تتعلق بخدمات الصرافة وتحويل الأموال وتقديم القروض، لأنه من الصعب وكما أسلفنا القول وضع تعريفاً جامعاً مانعاً للمعلومات المصرفية أو المالية، وقد يكون من الصعب أيضاً تعداد حصري لتخصص المنشآت المالية التي تقدم خدمات مصرفية أو مالية[2].

---

[1] بهذا المعنى يُنظر: د. عبدالإله النوايسة، جرائم تكنولوجيا المعلومات، دار وائل للنشر والتوزيع، عمَّان، 2017، ص 290.

[2] والدليل على ذلك، إن قانون المصرف المركزي وتنظيم المنشآت والأنشطة المالية الإماراتي، لم يُعرّف الأنشطة المصرفية أو المالية، ولم يُعرف كذلك المعلومات المصرفية والمالية[2]، وقد اكتفى بذكر الأنشطة المالية على سبيل التعداد في المادة (1/65) التي جاء فيها– " تعد الأنشطة التالية أنشطة مالية، خاضعة لترخيص ورقابة المصرف المركزي، وفقا لأحكام هذا المرسوم بقانون أ. تلقي الودائع بكافة أنواعها، بما فيها الودائع المتوافقة مع أحكام الشريعة الإسلامية. ب. تقديم التسهيلات الائتمانية بكافة أنواعها. ج. تقديم تسهيلات التمويل بكافة أنواعها، بما فيها تسهيلات التمويل المتوافقة مع أحكام الشريعة الإسلامية.د. تقديم خدمات الصرافة وتحويل الأموال.هـ. تقديم خدمات الوساطة النقدية.و. تقديم خدمات القيم المخزنة والدفعات الإلكترونية للتجزئة والنقد الرقمي.ز. تقديم خدمات العمليات المصرفية الافتراضية.ح. الترتيب و/أو

وخلاصة القول، إن مصطلح (المنشأة المالية) الذي ورد في المادة (1) من قانون مكافحة جرائم تقنية المعلومات الإماراتي يتسع ليشمل المنشأة المالية المصرفية وغير المصرفية، وثمّة مجموعة متنوعة من الخدمات التي تقدمها المنشأة المالية غير المصرفية، تتداخل مع الخدمات التي تقدمها المنشأة المالية المصرفية، كخدمات الصرافة وتحويل الأموال وتقديم القروض، وبالتالي فإن المعلومات المالية أو المصرفية المخزنة في نظام المعلومات الخاص بالمنشأة المالية، تصلح لأن تكون محلاً لجناية الدخول غير المشروع في نظام معلومات منشأة مالية للحصول على معلومات سرية، المنصوص عليها في المادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

ومن المفيد الإشارة في نهاية هذه الجزئية إلى تعريف (المعلومات الإلكترونية) بشكلٍ عام، كما عرّفتها المادة (1) من قانون مكافحة جرائم تقنية المعلومات الإماراتي بأنها: "أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها "– وبشكلٍ عام، يُقصَدُ بنظام المعلومات الإلكتروني، كما جاء في المادة (1) سالفة الذكر، بأنَّهُ:" مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك"، وعرّفت المادة (1) من ذات القانون الشبكة المعلوماتية بأنَّها: "ارتباط بين مجموعتين أو اكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات"

2– ركن المحل في جناية الحصول غير المشروع على المعلوماتِ المستهدفةِ في القانون الكويتي

تنص المادة (1/3) من قانون مكافحة جرائم تقنية المعلومات الكويتي على أنه: " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من ارتكب دخولاً غير مشروع الى موقع أو نظام

التسويق للأنشطة المالية المرخصة.ط. العمل كأصيل في المنتجات المالية التي تؤثر على المركز المالي للمنشأة المالية المرخصة والتي تشمل ولا تقتصر على الصرف الأجنبي، والمشتقات المالية، والسندات والصكوك، وملكية الحقوق، والسلع، وأية منتجات مالية أخرى يوافق عليها المصرف المركزي".

معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون، فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، تكون العقوبة الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، ويسرى هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية".

يُستفاد من هذه المادة بأنه يُشترط لقيام جناية الدخول غير المشروع في نظام معلومات خاص بمنشأة مصرفية للحصول على حسابات عملاء هذه المنشأة، توافر ركن المحل، وهو (معلومات حسابات عملاء منشأة مصرفية مُخزنة في نظام المعلومات الخاص بهذه المنشأة).

3- ركن المحل في جناية الحصول غير المشروع على المعلوماتِ المستهدفةِ في القانون العُماني

تنص المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني على أنه: " يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمداً ودون وجه حق موقعا إلكترونياً أو نظاماً معلوماتياً بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك، وتكون العقوبة السجن مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني إذا ترتب على الفعل المجرم إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر البيانات أو المعلومات الإلكترونية[1]، وتعد البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات المالية في حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة".

[1] بخصوص معنى أفعال إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر المعلومات الإلكترونية، أنظر، د. عبد الإله النوايسة، جرائم تكنولوجيا المعلومات، مرجع سابق، ص254 وما بعدها.

يُستفاد من هذه المادة بأنه يُشترط لقيام جناية الدخول غير المشروع في نظام معلومات للحصول على معلومات مصرفية أو مالية، توافر ركن المحل، وهو (المعلومات المصرفية أو المالية المُخزنة في نظام معلومات مصرف أو شركة مالية)، ومن المفيد الإشارة هنا أن القانون المصرفي العُماني رقم (114) لسنة2000، لم يُعرّف الأنشطة المصرفية أو المالية، ولم يُعرف كذلك المعلومات المصرفية والمالية، ولكنه اكتفى في المادة (5) بذكر الأعمال المصرفية على سبيل التعداد [1].

4- ركن المحل في جناية الحصول غير المشروع على المعلوماتِ المستهدفةِ في القانون الأردني

يقصد بهذا الركن كما جاء في المادة (7) من قانون الجرائم الإلكترونية، لزومٌ الحصول على معلومات إلكترونية مخزنة في نظام معلوماتي خاص ببنك أو بشركة مالية تقدم خِدْمات مصرفية، وهذا ما عبَّرت عنه المادة (7) بقولها: "يُعاقب كل من قام بأحد الأفعال المنصوص

[1] عرّفت المادة (٥) من القانون المصرفي العُماني رقم (114) لسنة 2000 "الأعمال المصرفية" بأنها: "القيام بصفة رئيسية وكمجال عمل عادي، حسبما يعرف ويفسر ذلك مجلس المحافظين، بواحد أو أكثر من الأنشطة التالية، أو الأنشطة الإضافية التي يرخص بها صراحة بموجب تعديلات تطرأ على هذا القانون، أو تلك التي يصرح بها مجلس المحافظين، في ترخيص يصدره وفقا لأحكام هذا القانون، – استلام الأموال كودائع تحت الطلب أو لأجل أو ودائع توفير، وفتح الحسابات الجارية والاعتمادات، وتقديم قروض بدون ضمان وتمديد الاعتماد، وإقراض الأموال بضمان شخصي أو إضافي أو عقاري، وأعمال بطاقات الائتمان، وإصدار خطابات الضمان وخطابات الاعتماد وتداولها، وصرف الشيكات والحوالات، وأوامر الدفع والأدوات الأخرى القابلة للتداول وتحصيلها، وقبول وخصم وتداول الأوراق المالية والكمبيالات والسندات الإذنية وغيرها من الأدوات القابلة للتداول، وبيع وتوظيف السندات والشهادات وغيرها من الأوراق المالية القابلة للتداول، وقبول المستندات المالية للحفظ، وممارسة الصلاحيات الاستئمانية، والقيام بأعمال الاستثمار وعمليات المصارف التجارية والأنشطة المالية الأخرى، التي يجوز أن تشمل، دون حصر ، تمويل الشركات والمشاريع وأعمال سمسرة الاستثمار والخدمات الاستشارية الاستثمارية وإدارة الاستثمار وتعهد تغطية إصدارات الأسهم وخدمات أمانة العهد والاستئمان والتأجير والوساطة وتمويل الشراء التأجيري وأية أنشطة أخرى مماثلة يوافق مجلس المحافظين على اعتبارها أعمالا مصرفية أو شراء وبيع واستبدال العملة الأجنبية والمحلية أو موجودات نقدية أخرى على شكل نقود أو مسكوكات أو سبائك، على أن الأشخاص الطبيعيين الذين يزاولون فقط أعمال استبدال العملات الأجنبية والمحلية بالتجزئة والأشخاص الذي يديرون منشآت تجارية بالتجزئة وأماكن السكن والإقامة العامة التي تقوم باستبدال العملات الأجنبية خدمة لعملائها، لا يعتبر أنهم يمارسون الأعمال المصرفية".

عليها في المواد (3–6) من هذا القانون، إذا وقعت على نظام معلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع أو التقاص أو التسويات أو بأيٍّ من الخِدْمات المصرفية المقدمة من البنوك والشركات المالية. .إلخ". والفعل الذي أحالت إليه المادة (7) إلى المادة (6)، وتطلبت أن يقع على نظام المعلومات المصرفي هو– فعلُ الحصول على المعلومات المصرفية المخزنة في النظام[1].

ولتوافر ركن المحل في جناية الحصول على المعلوماتِ المستهدفةِ في القانون الأردني يجب أن تتعلق هذه المعلومات، ببطاقات الائتمان أو بأعمال مصرفية أو مالية إلكترونية. وهذا ما عبَّرت عنه المادة (6) سالفة الذكر بقولها: "يُعاقب كل من حصل... على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية. .إلخ".

وفي سياق متصل بالمعلومات التي تتعلق ببطاقات الائتمان يمكن القول، إنَّه وعلى الرغم من أن المادة (6) ذكرت المعلومات التي تتعلق ببطاقات الائتمان دون غيرها من بطاقات الدفع المالي الأخرى، وذلك خلافًا لبعض التشريعات المقارنة[2]، إلا أن المعلومات التي تتعلق ببطاقات الدفع الأخرى مشمولة بذات الحماية المقررة لمعلومات بطاقات الائتمان في المادة (6) سالفة الذكر، وذلك لأن هذه المادة ذكرت عبارة: (... أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية...).

---

[1] عرّفت المادة (2) من قانون الجرائم الإلكترونية الأردني(المعلومات)، بأنها: "البيانات التي تمت معالجتها وأصبحت لها دلالة"، وكذا أوضحت المادة ذاتُها المقصودَ بالبيانات بقولِها: "هي الأرقام, أو الحروف, أو الرموز, أو الأشكال, أو الأصوات, أو الصور, أو الرسوماتُ التي ليس لها دلالة بذاتها"، وبشكلٍ عام، يُقصَدُ بنظام المعلومات، كما جاء في المادة (2) السالفة الذكر، بأنَّهُ:"مجموعة الأدوات والبرامج المُعدَّة لإنشاء المعلومات أو البيانات إلكترونيًّا, أو إرسالها, أو تسلمها, أو معالجتها, أو تخزينها, أو إدارتها, أو عرضها بالوسائل الإلكترونية"– وعرّفت المادة (2) من ذات القانون الشبكة المعلوماتية بأنَّها: "ارتباطٌ بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها", وكذا عرّفت المادة ذاتُها الموقعَ الإلكترونيَّ بأنه: "الحيِّزُ الذي يكون من خلال إتاحة البيانات والمعلومات على الشبكة المعلوماتية، ويكون ذلك من خلال عنوان إلكتروني مُحدَّد".

[2] نصت بعض التشريعات العربية، كالتشريع الإماراتي والكويتي، على بطاقات الدفع المالي الأخرى صراحةً، أنظر نص المادة (12) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، وأنظر كذلك نص المادة (5) من قانون مكافحة جرائم تقنية المعلومات الكويتي.

وهذه العبارة في تقدير الباحثين، تستوعب معلومات جميع بطاقات الدفع المالي، ولا سيما أن تنفيذ الكثير من المعاملات المصرفية يتطلب معرفة كل أو بعض معلومات بطاقات الدفع المالي, كأرقامها, أو تاريخ انتهاء صلاحيتها, أو أرقام حساب مالكها, أو أسمائهم, أو اسم البنك الصادرة عنه هذه البطاقات, وبناءً على ذلك فلا يجد الباحثان، ضرورةً لقيام المُشرِّع الأردني، وخلافًا لما يراه جانِبٌ من الفقه الأردني الذي نُجِلُّه[1]، بتجريم الحصول على المعلومات الخاصة ببطاقات الدفع المالي الأخرى.

ولطالما جاء النص الأردني على بطاقة الائتمان دون غيرها من بطاقات الدفع المالي الأخرى، فإننا سنوضحها – كما تم تعريفها فقهًا وقانونًا، إذ تمَّ تعريفُها بأنَّها: "أداة مصرفية للوفاء بالالتزام، وهي مقبولة الدفع على نطاق واسع محليًّا ودَوْليًّا لدى الأفراد والمؤسسات المالية، وتُعَدُّ بديلًا للنقود لدفع قيمة السلع والخِدْمات المقدمة لحامل البطاقة، على أن يقوم التاجر بتحصيل قيمة السلع، عن طريق البنك المصدر للبطاقة الذي صرح له بقبول البطاقة باعتبارها وسيلة دفع"[2].

نخلص مما تقدم أنه ومن خلال مقارنة جناية الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية في القوانين المقارنة، يتضح بأن محل جناية الحصول على المعلومات المصرفية الإلكترونية التي تتعلق بحسابات العملاء المنصوص عليها في المادة (1/3) من قانون مكافحة جرائم تقنية المعلومات الكويتي – هو الأضيق نطاقاً من محل جناية الحصول على المعلومات المصرفية والمالية الإلكترونية المنصوص عليها في القانون الإماراتي والعُماني والأردني.

وذلك لأن محل الجناية في القانون الكويتي يقتصر على (معلومات حسابات عملاء المنشأة المصرفية المُخزنة في نظام المعلومات الخاص بهذه المنشأة) بينما محل الجناية المنصوص عليها في المادتين (6 و7) من قانون الجرائم الإلكترونية الأردني، يتسع ليشمل جميع المعلومات المصرفية والمالية المُخزنة في نظام المعلومات الخاص بالبنك أو الشركة المالية التي تقدم خدمات مصرفية، ويعتبر محل الجناية المنصوص عليها في المادة (4) من قانون

---

[1] د. عبدالإله النوايسة، ود. ممدوح العدوان، الحماية الجنائية للعمليات المصرفية الإلكترونية، الهيئة العالمية للتسويق الإسلامي، مجلة الإدارة والقيادة الإسلامية، المجلة 3، العدد1، 2018، ص51، 62.

[2] د. محمد العبادي، الجرائم المستحدثة في ظل العولمة، دار جليس الزمان، الطبعة الأولى، الأردن، 2015، ص 77.

مكافحة جرائم تقنية المعلومات الإماراتي، ومحل الجناية المنصوص عليها في المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني، هما الأوسع نطاقاً، لأنهما يشملان جميع المعلومات المالية المُخزنة في نظام المعلومات الخاص بالمنشأة المالية.

ثانياً: الركن المادي المُكون لجناية الحصول غير المشروع على المعلومات المستهدفةِ

1- الركن المادي المُكون لجناية الحصول غير المشروع على المعلومات المستهدفةِ في القانون الإماراتي

يتضح من المادة(4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، بأن السلوك المادي المكون لهذه الجناية، يتمثل بالدخول غير المشروع في نظام معلومات إلكتروني خاص بمُنشأة مالية، بقصد الحصول على المعلومات المالية المُخزنة في هذا النظام، وهذا السلوك يُفترض أن يكون إيجابيًا، وذلك من خلال سعي الجاني لإحراز المعلومات المستهدفة، وقد اشترط المشرع الإماراتي صراحةً، أن يتم الدخول في النظام المعلوماتي، بقصد الحصول على المعلومات المستهدفة، بصورةٍ غير مشروعة، وهذا ما عبرت عنه المادة (4) سالفة الذكر بقولها: "يعاقب بالسجن المؤقت.... كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني.... سواءً كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية.... ألخ"

وتعتبر هذه الجريمة من جرائم السلوك المُجرد، فلا يشترط لقيامها، تحقق نتيجة معينة وهي (الحصول على المعلومات المستهدفة)، وبمعنى آخر، فإن الركن المادي، يكتمل في هذه الجريمة بمجرد الدخول غير المشروع في النظام المعلوماتي بقصد الحصول على المعلومات المستهدفة، وذلك حتى ولو لم يحصل الجاني على هذه المعلومات، ولكن يُشترط في هذه الحالة، أن يتم إثبات دخول الجاني في النظام المعلوماتي، بقصد الحصول على المعلومات المستهدفة[1].

[1] لمزيد من المعلومات عن إثبات الجرائم الإلكترونية بشكل عام، أنظر، د. عادل الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، عمّان، 2015، ص225 وما بعدها.

2– الركن المادي المُكون لجناية الحصول على المعلومات المستهدفةِ في القانونين الكويتي والعُماني

يتضح من المادة (3) من قانون مكافحة جرائم تقنية المعلومات الكويتي، بأن السلوك المادي المكون لهذه الجناية، يتمثل بالدخول غير المشروع في نظام معلومات خاص بمنشأة مصرفية للحصول على حسابات عملاء هذه المنشأة، وهذا السلوك يُفترض أن يكون إيجابيًا، وذلك من خلال سعي الجاني لإحراز المعلومات المستهدفة.

ويتضح كذلك من المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني، بأن السلوك المادي المكون لهذه الجناية، يتمثل بالدخول غير المشروع في نظام معلومات خاص بمصرف أو شركة مالية بقصد الحصول على معلومات مصرفية أو مالية، وهذا السلوك يُفترض أن يكون إيجابيًا، وذلك من خلال سعي الجاني لإحراز المعلومات المستهدفة.

وقد اشترط المشرعان الكويتي والعُماني صراحةً، أن يتم الدخول في النظام المعلوماتي، بقصد الحصول على المعلومات المستهدفة بصورةٍ غير مشروعة، ويستوي بهذا الدخول أن يكون مباشراً أو أن يتم من خلال إحدى وسائل تقنية المعلومات، وهذا ما عبرت عنه المادة (3) من قانون مكافحة جرائم تقنية المعلومات الكويتي بقولها: " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات .... كل من ارتكب دخولاً غير مشروع إلى موقع إلكتروني، أو نظام معلومات إلكتروني مباشرة أو عن طريق إحدى وسائل تقنية المعلومات، وإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها.... تكون العقوبة الحبس مدة لا تجاوز عشر سنوات .... سواءً كان الدخول، .... ويسري هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية".

وهذا ما عبرت عنه كذلك المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني بقولها: "يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات.... كل من دخل عمداً ودون وجه حق موقعاً إلكترونياً أو نظاماً معلوماتياً بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها....، وتكون العقوبة السجن مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات.... إذا ترتب على الفعل المجرّم إلغاء أو تغيير أو تعديل.... المعلومات الإلكترونية، وتعد البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات

المالية في حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة."

وينبغي التنبيه بأن هذه الجناية تعتبر من الجرائم ذات النتيجة (الجرائم المادية)، وفقاً لأحكام القانونين الكويتي والعُماني، فيجب لقيامها تحقق نتيجةٌ مُعيَّنة، (كإلغاء المعلومات المستهدفة)، وبمعنى آخر، فإن الركن المادي لا يكتمل في هذه الجناية إلا بعد الدخول في النظام بصورة غير مشروعة بقصد الحصول على المعلومات المستهدفةِ، ومن ثم تحقق نتيجة معينة كإلغاء المعلومات المصرفية على سبيل المثال.

3- الركن المادي المُكون لجناية الحصول غير المشروع على المعلومات المستهدفةِ في القانون الأردني

وفقًا لنص المادة (6) من قانون الجرائم الإلكترونية الأردني، يتمثل السلوك المادي في هذه الجناية بالحصول على المعلومات المستهدفة، وهذا السلوك يُفترض أن يكون إيجابيًا، وذلك من خلال سعي المعتدي لإحراز المعلومات المستهدفة، وخلافاً (للمشرع الإماراتي والكويتي والعُماني) – لم يشترط المُشرّع الأردني الدخول غير المشروع في النظام المعلوماتي للحصول على المعلومات المستهدفة [1]، إلا أنه وعلى الرغم من ذلك، فإن الجريمة تقع في حالة الدخول غير المشروع في النظام المعلوماتي للحصول على المعلومات المستهدفة، كما أنها تقع أيضاً في حالة الدخول المشروع في النظام المعلوماتي إذا تم الحصول على المعلومات دون موافقة من يملكها، وبذلك فإن النص يستوعب الحالتين معًا.

وينبغي التنبيه أن هذه الجريمة من الجرائم ذات النتيجة (الجرائم المادية)، إذ يجب أن ينجُمَ عن النشاط الجرمي نتيجةٌ مُعيَّنة، وهي (الحصول على المعلومات المستهدفة)، وبمعنى آخر، فإن الركن المادي يكتمل في هذه الجريمة بمجرد الحصول على المعلومات المستهدفةِ، حتى ولو لم يستفد الجاني من هذه المعلومات، ويجب أن يتم الحصول على المعلومات المستهدفة بوسيلة إلكترونية معينة. ويُقصَدٌ بذلك وجوبُ الحصول على هذه المعلومات بوساطة نظام

[1] لمزيد من التفاصيل عن الدخول غير المشروع في النظام المعلوماتي، أنظر أسامة المناعسة و جلال الزعبي، جرائم تظم المعلومات الإلكترونية، دار الثقافة للنشر، عمّان، 2017، ص277 وما بعدها.

معلوماتي يستعين به الجاني للحصول على هذه المعلومات، وهذا ما عبَّرت عنه صراحةً المادة (6) من قانون الجرائم الإلكترونية الأردني بقولها: "يُعاقب كل من حصل قصدًا دون تصريح عن طريق... أي نظام معلومات على... معلومات تتعلق ببطاقات الائتمان.. إلخ".

وعليه، فلو تمَّ الحصول على المعلومات المستهدفة بأيّ طريقةٍ أخرى فلا مجال لقيام هذه الجناية، فعلى سبيل المثال لو حصل شخص على معلومات بطاقة ائتمان لشخصٍ آخر، حين شاهدها في درج مكتبه (أي مكتب الأخير)، ففي هذه الواقعة لا تقوم جناية الحصول على معلومات بطاقة الائتمان، وهنا لا بُدَّ من تكييف هذه الواقعة في ضوء نصوص قانونية أخرى.

كما ويجب أن يتم الحصول على المعلومات المستهدفة بطريقةٍ غير مشروعة، ويُقصَدُ بذلك أن يتم الحصول على المعلومات بدون موافقة من يملكها، وهذا ما عبَّرت عنه صراحةً المادة (6) السالفِ ذِكْرُها بقولها: "يُعاقب كل من حصل قصدًا دون تصريح عن طريق.. إلخ".

ثالثًا: الركن المعنوي في جناية الحصول غير المشروع على المعلومات المستهدفةِ

من الرجوع للمادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، والمادة (3) من قانون مكافحة جرائم تقنية المعلومات الكويتي، والمادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني، يتضح بأن هذه المواد اشترطت صراحةً لقيام هذه الجناية توافر الركن المعوي (بصورة القصد)، وبشكلٍ عام اشترطت المادة الأولى، من قانون مكافحة جرائم تقنية المعلومات الكويتي توافر القصد في الدخول غير المشروع، وذلك حينما عرّفت مصطلح" الدخول غير المشروع"، ويتعيّن لقيام جناية الحصول على المعلومات المستهدفة في القانون الأردني، أن يتوافر الركن المعنوي بصورة القصد. وهذا عبّرت عنه المادة (6) من قانون الجرائم الإلكترونية صراحةً، لذلك يتعيَّنُ توافر عنصري هذا القصد، وهما العلم والإرادة، فينبغي أن يعلم الجاني بأنه يستعين بنظام معلومات، ليحصل بواسطته وبصورةٍ غير مشروعة على معلومات إلكترونية تتعلق ببطاقات الائتمان أو بإحدى المعاملات المالية أو المصرفية الإلكترونية، ويتعيّن توافُرُ العنصر الثاني، وهو الإرادة، فيجب أن تنصرف إرادة الجاني الحرة لاستخدام نظام معلومات ليحصل من خلاله على المعلومات المستهدفة التي يحتويها نظام المعلوماتي المصرفي.

▪ الفرع الثاني: العقوبة المقررة لجناية الحصول غير المشروع على المعلومات المستهدفةِ

أولاً: العقوبة المقررة لجناية الحصول غير المشروع على المعلومات المستهدفةِ في القانون الإماراتي

عاقبت المادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي على هذه الجناية " بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم، وتكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم، إذا تعرضت هذه المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

ومن الرجوع للقواعد العامة في الواردة في المادة (68) من قانون العقوبات الإماراتي رقم (3) لسنة 1987 يتضح بأن الحد الأدنى لمدة عقوبة السجن المؤقت هو ثلاث سنوات وحدها الأعلى خمسة عشر سنة.

ثانياً: العقوبة المقررة لجناية الحصول غير المشروع على المعلومات المستهدفةِ في القانون الكويتي

عاقبت المادة (1/3) من قانون مكافحة جرائم تقنية المعلومات الكويتي على جريمة الحصول على المعلومات المصرفية إذا ترتب عليها نتيجة معينة كإلغاء هذه المعلومات أو إتلافها بعقوبة جناية، وهي الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، ومن الرجوع للقواعد العامة الواردة في المادة (3) من قانون الجزاء الكويتي رقم (16) لسنة1960، يتضح بأن الحد الأدنى لمدة عقوبة الحبس الجنائي هو ثلاث سنوات[1]، ويجدر بالذكر بأنه يُعاقب على هذه الجريمة إذا لم ينجم عنها نتيجة كإلغاء المعلومات، بعقوبة جنحية، هي الحبس مدة لا تجاوز

[1] تنص المادة (3) من قانون الجزاء الكويتي على أنه: " الجنايات هي الجرائم المعاقب عليها بالاعدام أو بالحبس المؤبد أو بالحبس المؤقت مدة تزيد على ثلاث سنوات"، وقالت المادة (5) من ذات القانون أن " الجنح هي الجرائم التي يعاقب عليها بالحبس مدة لا تجاوز ثلاث سنوات والغرامة أو بإحدى هاتين العقوبتين".

ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين.

ثالثاً: العقوبة المقررة لجناية الحصول غير المشروع على المعلومات المستهدفةِ في القانون العُماني

عاقبت المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني على جريمة الحصول على المعلومات المصرفية إذا ترتب عليها نتيجة معينة كإلغاء هذه المعلومات أو إتلافها بعقوبة جناية[1]، وهي السجن مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني، وعملاً بالمادة (24) من قانون الجزاء العُماني رقم (7) لسنة2018 فإن هذه العقوبة من عقوبات الجنايات، لأن الحد الأدنى للسجن في الجنايات هو ثلاث سنوات وحده الأعلى خمس عشرة سنة[2]، ويجدر بالذكر بأنه يُعاقب على هذه الجريمة إذا لم ينجم عنها نتيجة كإلغاء المعلومات بعقوبة جنحية، هي السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين.

رابعاً: العقوبة المقررة لجناية الحصول غير المشروع على المعلومات المستهدفةِ في القانون الأردني

عاقبت المادة (7) من قانون الجرائم الإلكترونية الأردني على هذه الجناية، بعقوبة الأشغال مدةً لا تقِلُّ عن خمس سنوات, ولا تزيد عن عشرين سنة، وبغرامة لا تقِلُّ عن (5000) دينار، ولا تزيد عن (15000) دينار، ويرى الباحثان أنَّ المادة (7) من قانون الجرائم الإلكترونية

---

[1] لمزيد من التفاصيل حول جرائم الاتلاف التقني، أنظر، أسامة المناعسة و جلال الزعبي، جرائم تظم المعلومات الإلكترونية، مرجع سابق، ص118 وما بعدها، وأنظر كذلك، محمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر، عمّان، 2011، ص222، وأنظر لدى – حسن المناصير، جريمة الدخول عير المشروع إلى النظام المعلوماتي والتعدي على محتوياته, رسالة ماجستير، جامعة جرش, الأردن2016، ص56.

[2] أنظر النص الكامل للمادة (24) من قانون الجزاء العُماني رقم (7) لسنة2018.

أحالت تطبيق العقوبة الجنائية الواردة فيها على جريمة الحصول على المعلومات التي تتعلق ببطاقات ائتمان أو بمعاملات مالية أو مصرفية، بشرط أن تكون هذه المعلومات مخزنة في نظام معلومات مصرفي، وبمعنى آخر، فقد جاءت المادة (7) السالف ذِكْرُها بهدف واضح هو تشديد عقوبة الجريمة سالفة الذكر، حينما يتم الحصول على المعلومات المستهدفة من نظام معلومات مصرفي.

المطلب الثاني: الوصف الجنحي لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية

يُستفاد من نصوص المواد (12من قانون مكافحة جرائم تقنية المعلومات الإماراتي، و5 من قانون مكافحة جرائم تقنية المعلومات الكويتي، و28 من قانون مكافحة جرائم تقنية المعلومات العُماني و12 من قانون مكافحة الجرائم الإلكترونية القطري، و4 من قانون جرائم تقنية المعلومات البحريني و6 من قانون الجرائم الإلكترونية الأردني)، والتي سنكتب محتواها فيما بعد– أنه يُشترط لقيام جنحة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية وجود ثلاث أركان، وهي ركن المحل، والركنين المادي والمعنوي، وبناءً على ذلك سنوضح أركان هذه الجنحة وعقوباتها في القوانين سالفة الذكر، وسنوضح أيضاً جريمة الحصول على المعلومات المصرفية والمالية وعقوبتها في النظام السعودي في الفروع التالية، ونؤكد هنا بأننا، سنستعمل عبارة (الحصول على المعلومات المستهدفة) اختصاراً لعبارة: (الحصول على المعلومات المصرفية والمالية الإلكترونية):

▪ الفرع الأول: أركان جنحة الحصول غير المشروع على المعلوماتِ المُستهدفةِ وعقوبتها في القانون الإماراتي

نصت المادة (12) من قانون مكافحة جرائم تقنية المعلومات الإماراتي على أنه: "يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طريق استخدم الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام

أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني".

من مطالعة المادة (12) السالفة الذكر، يتبيّن بأنه يشترط لقيام جنحة الحصول على معلومات تتعلق بحسابات مصرفية أو تتعلق ببطاقة ائتمانية أو إلكترونية أو بأي وسيلة من وسائل الدفع الإلكتروني – توافُر ثلاث أركان، الركن الأول هو ركن المحل الذي يتمثل بمعلومات إلكترونية تتعلق بحسابات مصرفية أو ببطاقة ائتمانية أو إلكترونية أو بأي وسيلة من وسائل الدفع الإلكتروني، والركن الثاني هو المادي، ويتمثل بالحصول بوسيلةٍ إلكترونية، وبصورة غير مشروعة على معلومات إلكترونية تتعلق بحسابات مصرفية أو بإحدى بطاقات الدفع الإلكتروني، والركن الثالث فهو المعنوي ويتخذ صورة القصد أو الخطأ.

من المُلاحظ أن هذه الأركان تختلف إلى حدٍ ما عن الأركان المطلوبة لقيام جناية الحصول على المعلومات المالية المنصوص عليها في المادة(4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، وتظهر أوجه الاختلاف فيما يلي:

أولاً: من حيث ركن المحل

يتمثل ركن المحل المطلوب لقيام الجناية بالمعلومات المالية المُخزنة في نظام معلومات إلكتروني خاص بمُنشأة مالية، (المعلومات المستهدفة)، بينما يتمثل ركن المحل المطلوب لقيام الجنحة المنصوص عليها في المادة(12) المعلومات الإلكترونية التي تتعلق بحسابات مصرفية أو ببطاقة ائتمانية أو إلكترونية أو بأي وسيلة من وسائل الدفع الإلكتروني، (المعلومات المستهدفة).

ويُلاحظ هنا أن ركن المحل المطلوب في الجناية أوسع نطاقاً من ركن المحل المطلوب في الجنحة، لأن الأخير يقتصر على المعلومات الإلكترونية التي تتعلق بحسابات مصرفية أو ببطاقة ائتمانية أو إلكترونية أو بأي وسيلة من وسائل الدفع الإلكتروني، بينما ركن المحل في الجناية، يتسع ليشمل جميع المعلومات المالية– هذا من جهة.

ومن جهة أخرى، يُشترط لقيام الجناية، أن تكون المعلومات التي تم الحصول عليها مُخزنة في نظام معلومات إلكتروني خاص بمُنشأة مالية، بينما لا يشترط في

الجنحة، سوى أن يقع السلوك الجرمي (فعل الحصول) على المعلومات الإلكترونية المستهدفة، وبِغَضِّ النظر عن نظام المعلومات أو الموقع أو التطبيق الإلكتروني الذي يحتوي هذه المعلومات.

ثانياً: من حيث الركن المادي

يُشترط لقيام هذا الركن في الجناية سالفة الذكر، توافر شرط الدخول غير المشروع في نظام المعلومات الإلكتروني الخاص بالمُنشأة المالية، بقصد الحصول على المعلومات المالية المُخزنة في هذا النظام، بينما لا يشترط لقيام الركن المادي المكون للجنحة المنصوص عليها في المادة(12) توافر هذا الشرط، إذ يمكن توافر الركن المادي لهذه الجنحة بالحصول على المعلومات المستهدفة من أي وعاء إلكتروني، ولكن يُشترط هنا أن يتم الحصول على هذه المعلومات باستخدام الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وهذا ما أكدته محكمة النقض في أحد أحكامها[1]: "لما كانت المادة 12 من المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات تنص على أنه يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طريق استخدام الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني.... فإن تلك الجريمة تتحقق بمجرد استيلاء شخص على مال الغير بطريق استخدام الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات، والركن المادي فيها هو الوسيلة التي يلجأ إليها المتهم لتحقيق الغرض الذي يهدف إليه على أن تكون بإحدى وسائل تقنية المعلومات".

[1] حكم محكمة النقض في أبو ظبي بصفتها الجزائية، رقم1052 لسنة2019، الموقع الإلكتروني لدائرة القضاء في أبو ظبي.

ثالثاً: من حيث الركن المعنوي

يُشترط لقيام الجناية سالفة الذكر، توافر القصد[1]، لأن الجاني يقصد من الدخول غير المشروع في نظام المعلومات الإلكتروني الخاص بالمُنشأة المالية الحصول على المعلومات المالية المُخزنة في هذا النظام، بينما قد ترتكب الجنحة سالفة الذكر، بالقصد أو الخطأ، لأنه ومن الرجوع للمادة (12) من قانون مكافحة جرائم تقنية المعلومات الإماراتي نجدها لم تشترط (القصد) لقيام هذه الجنحة، وبالتالي وبحسب تقديرنا، أنه يمكن ارتكاب هذه الجنحة بالقصد أو الخطأ، وذلك لأنه يُستفاد من المادة (43) من قانون العقوبات الإماراتي رقم (3) لسنة1987، بأنه حينما يسكُت المشرع عن بيان صورة الركن المعنوي في جريمة معينة، فهذا يعني أن الجاني يسأل عن هذه الجريمة سواءً ارتكبها قصداً أم خطأ[2].

لذلك يوصي الباحثان المشرع الإماراتي التدخل بوضع نص صريح في قانون مكافحة جرائم تقنية المعلومات يُشترط بمقتضاه توافر القصد لقيام جنحة الحصول على معلومات تتعلق بحسابات مصرفية أو تتعلق ببطاقة ائتمانية أو إلكترونية أو بأي وسيلة من وسائل الدفع الإلكتروني، لأن أي شخص معرضاً للحصول على هذه المعلومات بالخطأ، ومن غير المنطق معاقبته على ذلك بسبب خطأ غير مقصود.

وفي ختام هذه الجزئية نشير للعقوبة المقررة لهذه الجنحة في القانون الإماراتي، وهي عقوبة الحبس والغرامة أو بإحدى هاتين العقوبتين، وذلك عملاً بالمادة (12) من قانون مكافحة جرائم تقنية المعلومات.

---

[1] لمزيد من التفاصيل عن القصد الجنائي في الجرائم الإلكترونية يُنظَر: د. زياد العنزي، د. عبدالله احجيله، الجوانب القانونية لمسؤولية مدير المجموعة في مواقع التواصل الاجتماعي في القانون الاتحادي الإماراتي، بحث منشور في مجلة الحقوق، جامعة البحرين، المجلد 16، العدد1، 2019، ص251 وما بعدها.

[2] لمزيد من التفاصيل عن القصد الجنائي أنظر، د. محمد السعيد عبدالفتاح، الوجيز في شرح قانون العقوبات الإتحادي الإماراتي، القسم العام، الآفاق المشرقة، عمّان، 2014، ص148 وما بعدها.

▪ الفرع الثاني: أركان جنحة الحصول غير المشروع على المعلوماتِ المُستهدفةِ وعقوبتها في القانون الكويتي

تنص المادة (5) من قانون مكافحة جرائم تقنية المعلومات الكويتي على أنه: " يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تقل عن ألف دينار ولا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول دون وجه حق الى أرقام أو بيانات بطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية".

من مطالعة المادة (5) السالفة الذكر يتبيّن بأنه يشترط لقيام جنحة الحصول على معلومات تتعلق ببطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية – توافُر ثلاث أركان، الركن الأول هوُ ركن المحل الذي ويتمثل بالمعلومات الإلكترونية التي تتعلق ببطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية، والركن الثاني هو المادي، ويتمثل بالحصول بوسيلةٍ إلكترونية، وبصورة غير مشروعة، على معلومات إلكترونية تتعلق ببطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية، أما الركن الثالث، فهو الركن المعنوي بصورة القصد.

ومن المُلاحظ أن هذه الأركان تختلف إلى حدٍ ما عن الأركان المطلوبة لقيام جناية الدخول غير المشروع في نظام معلومات خاص بمنشأة مصرفية للحصول على حسابات عملاء هذه المنشأة، المنصوص عليها في المادة (3) من قانون مكافحة جرائم تقنية المعلومات الكويتي، وتظهر أوجه الاختلاف فيما يلي:

أولاً: من حيث ركن المحل

يتمثل ركن المحل المطلوب لقيام الجناية (بمعلومات حسابات عملاء منشأة مصرفية مُخزنة في نظام المعلومات الخاص بهذه المنشأة).) بينما يتمثل ركن المحل المطلوب لقيام الجنحة المنصوص عليها في المادة(5) بالمعلومات الإلكترونية التي تتعلق ببطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية، (المعلومات المستهدفة).

ويُلاحظ هنا أن ركن المحل المطلوب في الجناية أوسع نطاقاً من ركن المحل المطلوب في الجنحة، لأن الأخير يقتصر على المعلومات الإلكترونية التي تتعلق ببطاقة ائتمانية أو ما

في حكمها من البطاقات الإلكترونية، بينما ركن المحل في الجناية، يتسع ليشمل جميع معلومات حسابات عملاء منشأة مصرفية، هذا من جهة.

ومن جهة أخرى، يُشترط لقيام الجناية أن تكون المعلومات التي تم الحصول عليها مُخزنة في نظام معلومات إلكتروني خاص بمُنشأة مصرفية، بينما لا يشترط في الجنحة، سوى أن يقع السلوك الجرمي (فعل الحصول) على المعلومات الإلكترونية المستهدفة، وبِغَضّ النظر عن نظام المعلومات أو الموقع أو التطبيق الإلكتروني الذي يحتوي هذه المعلومات.

ثانياً: من حيث الركن المادي

يُشترط لقيام هذا الركن في الجناية سالفة الذكر، توافر شرط الدخول غير المشروع في نظام المعلومات الإلكتروني الخاص بالمُنشأة المصرفية، بقصد الحصول على المعلومات المالية المُخزنة في هذا النظام، بينما لا يشترط لقيام الركن المادي المكون للجنحة المنصوص عليها في المادة(5) توافر هذا الشرط، إذ يمكن توافر الركن المادي لهذه الجنحة بالحصول على المعلومات المستهدفة من أي وعاء إلكتروني.

وفي نهاية هذه الجزئية نشير للعقوبة المقررة لهذه الجنحة في القانون الكويتي، وهي الحبس مدة لا تجاوز سنة وبغرامة لا تقل عن ألف دينار ولا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين، وذلك عملاً بالمادة (5) من قانون مكافحة جرائم تقنية المعلومات.

▪ الفرع الثالث: أركان جنحة الحصول غير المشروع على المعلوماتِ المُستهدفةِ وعقوبتها في القانون العُماني

تنص المادة(28) من قانون مكافحة جرائم تقنية المعلومات العُماني على أنه: " يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين، كل من.... استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في الوصول دون وجه حق إلى أرقام أو بيانات بطاقة مالية.... ألخ).

من مطالعة المادة (28) السالفة الذكر، يتبيّن بأنه يشترط لقيام جنحة الحصول على معلومات تتعلق ببطاقة مالية – توافُر ثلاث أركان، الركن الأول، هوُ ركن المحل ويتمثل بالمعلومات الإلكترونية التي تتعلق ببطاقة مالية، وقد عرّفت المادة (1) من قانون مكافحة جرائم تقنية المعلومات العُماني البطاقة المالية بأنها: "وسيط إلكتروني ملموس يستعمل في عمليات السحب أو الإيداع أو الدفع الإلكتروني باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات كبطاقات الائتمان والبطاقات الذكية، ولا يشمل ذلك بطاقات الاتصالات والخِدْمات الإلكترونية المدفوعة مسبقًا".

والركن الثاني هو الركن المادي، ويتمثل بالحصول بوسيلةٍ إلكترونية، وبصورة غير مشروعة على معلومات إلكترونية تتعلق ببطاقة مالية، أما الركن الثالث، فهو الركن المعنوي بصورة القصد.

ومن المُلاحظ أن هذه الأركان تختلف إلى حدٍ ما عن الأركان المطلوبة لقيام جناية الدخول غير المشروع في نظام معلومات إلكتروني خاص بمصرف أو بشركة مالية بقصد الحصول على معلومات مصرفية أو مالية المنصوص عليها في المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني، وتظهر أوجه الاختلاف فيما يلي:

أولاً: من حيث ركن المحل

يتمثل ركن المحل المطلوب لقيام الجناية بمعلومات مصرفية أو مالية مُخزنة في نظام معلومات خاص بمصرف أو بشركة مالية، بينما يتمثل ركن المحل المطلوب لقيام الجنحة المنصوص عليها في المادة(28) بالمعلومات الإلكترونية التي تتعلق ببطاقة مالية، (المعلومات المستهدفة)، ويُلاحظ هنا أن ركن المحل المطلوب في الجناية أوسع نطاقاً من ركن المحل المطلوب في الجنحة، لأن الأخير يقتصر على المعلومات الإلكترونية التي تتعلق ببطاقة مالية، بينما ركن المحل في الجناية، يتسع ليشمل جميع المعلومات المصرفية أو المالية، هذا من جهة.

ومن جهة أخرى، يُشترط لقيام الجناية، أن تكون المعلومات التي تم الحصول عليها مُخزنة في نظام معلومات إلكتروني خاص بمصرف أو بشركة مالية، بينما لا يشترط في الجنحة،

سوى أن يقع السلوك الجرمي (فعل الحصول) على المعلومات الإلكترونية المستهدفة، وبِغَضّ النظر عن نظام المعلومات أو الموقع أو التطبيق الإلكتروني الذي يحتوي هذه المعلومات.

ثانياً: من حيث الركن المادي

يُشترط لقيام هذا الركن في الجناية سالفة الذكر، توافر شرط الدخول غير المشروع في نظام المعلومات الإلكتروني الخاص بالمصرف أو بالشركة المالية، بقصد الحصول على المعلومات المصرفية أو المالية المُخزنة في هذا النظام، بينما لا يشترط لقيام الركن المادي المكون للجنحة المنصوص عليها في المادة(28) توافر هذا الشرط، إذ يمكن توافر الركن المادي لهذه الجنحة بالحصول على المعلومات المستهدفة من أي وعاء إلكتروني.

وبقي أن نقول في هذه الجزئية أن العقوبة المقررة لهذه الجنحة في القانون العُماني، هي السجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين، وذلك عملاً بالمادة (28) من قانون مكافحة جرائم تقنية المعلومات.

▪ الفرع الرابع: أركان جنحة الحصول غير المشروع على المعلوماتِ المُستهدفةِ وعقوبتها في القانون القطري

تنص المادة (1/12) من قانون مكافحة الجرائم الإلكترونية القطري رقم(14) لسنة2014 على أنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، أو بإحدى هاتين العقوبتين، كل من.... حصل أو سهل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات".

يُستفاد من هذا النص أنه يُشترط لقيام هذه الجنحة توافر ثلاث أركان، ركن المحل والركنين المادي والمعنوي، وحينما تتوافر هذه الأركان فإنه يُعاقب على هذه الجنحة بالعقوبة السالفة الذكر، سنوضح أركان هذه الجنحة وعقوبتها كما يلي:

أولاً: ركن المحل (معلومات بطاقة التعامل الإلكتروني)[1]

يتمثل ركن المحل في هذه الجنحة، بالمعلومات التي تتعلق ببطاقة التعامل الإلكتروني، وقد تم تعريف هذه البطاقة بموجب المادة (1) من القانون السالف الذكر بأنها: "البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو غيرها من وسائل تقنية المعلومات والتي تحتوي على بيانات أو معلومات إلكترونية والتي تصدرها الجهات المُرخّص لها بذلك".

ثانياً: الركن المادي

يتمثل السلوك المادي هنا، بالحصول أو تسهيل الحصول بصورة غير مشروعة على المعلومات الإلكترونية التي تتعلق ببطاقة التعامل الإلكتروني، وهذا السلوك يُفترض أن يكون إيجابيًا، وذلك من خلال سعي الجاني لإحراز معلومات البطاقة، ويجب أن يتم ذلك بوسيلةٍ إلكترونية، وهي الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وهذا ما عبرت عنه المادة (12) سالفة الذكر صراحةً بقولها: " حصل أو سهل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات".

وقد عرّفت المادة (1) من قانون مكافحة الجرائم الإلكترونية القطري، تقنية المعلومات بأنها: " أي وسيلة مادية أو غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام معلوماتي أو شبكة معلوماتية"، وعرّفت المادة ذاتها الشبكة المعلوماتية بأنها: " ارتباط بين أكثر من وسيلة لتقنية المعلومات، للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة والعامة والشبكة العالمية –الإنترنت"– وأخيراً، يتعيّن لقيام هذا الركن، تحقق نتيجة

[1] لمزيد من المعلومات حول هذه البطاقة وحمايتها جزائياً، أنظر، د. حمزة أبو عيسى، جرائم تقنية المعلومات – دراسة مقارنة في التشريعات العربية، دار الثقافة للنشر والتوزيع، عمَّان، ص89 وما بعدها، وأنظر، حسام الخولى، الحماية الجنائية والمدنية لعمليات البنوك الإلكترونية، مرجع سابق، ص285، وما بعدها.

معينة، وهي الحصول على المعلومات التي تتعلق ببطاقة التعامل الإلكتروني، وعلى ذلك فهذه الجنحة من الجرائم ذات النتيجة[1].

ثالثاً: الركن المعنوي (بصورة القصد أو الخطأ)

يتخذ الركن المعنوي في هذه الجنحة صورة القصد أو الخطأ، لأن المادة (12) من قانون مكافحة الجرائم الإلكترونية القطري، لم تشترط (القصد) لقيام هذه الجنحة، وبالتالي وبحسب تقديرنا، أنه يمكن ارتكاب هذه الجنحة بالقصد أو الخطأ، وذلك لأنه يُستفاد من الماد (32) من قانون العقوبات القطري رقم (11) لسنة2004، بأنه حينما يسكُت المشرع عن بيان صورة الركن المعنوي في جريمة معينة، فهذا يعني أن الجاني يسأل عن هذه الجريمة سواءً ارتكبها قصداً أم خطأ[2].

لذلك يوصي الباحثان المشرع القطري، التدخل بوضع نص صريح في قانون مكافحة الجرائم الإلكترونية، يُشترط بمقتضاه توافر القصد لقيام جنحة الحصول على معلومات تتعلق ببطاقات الدفع الإلكتروني، لأن أي شخص معرضاً للحصول على هذه المعلومات بالخطأ، ومن غير المنطق معاقبته على ذلك بسبب خطأ غير مقصود.

رابعاً: العقوبة المقررة لهذه الجنحة في القانون القطري

يُعاقب على هذه الجنحة، بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، أو بإحدى هاتين العقوبتين، وهاتان العقوبتان من عقوبات الجنح، وذلك عملاً بنص المادة (23) من قانون العقوبات القطري التي نصت على أنه: " الجنح هي الجرائم المعاقب عليها بالحبس لمدة لا تزيد على ثلاث سنوات وبالغرامة التي تزيد على ألف ريال".

---

[1] لمزيد من التفاصيل عن الجرائم ذات النتيجة والأخرى ذات السوك المُجرد، يُنظَر: د. أحمد أبو خطوة، شرح الأحكام العامة لقانون العقوبات الإماراتي، الجزء الأول، ط1، منشورات أكاديمية شرطة دبي، 1989، ص159 وما بعدها

[2] تنص الماد (32) من قانون العقوبات القطري على أنه: " يسأل الجاني عن الجريمة سواء ارتكبها عمداً أم خطأ، ما لم يشترط القانون توفر العمد صراحة".

واستكمالاً للفائدة في هذه الجزئية فإن الباحثين يأملان من المشرع القطري تعديل نص المادة (12) من قانون مكافحة الجرائم الإلكترونية، بحيث يضاف إليه تجريم فعل الحصول غير المشروع على المعلومات المصرفية أو المالية الإلكترونية بأي وسيلةٍ إلكترونية، والمعاقبة على هذا الفعل (بعقوبة جنائية) أذا تم الحصول على هذه المعلومات من نظام معلومات إلكتروني خاص ببنك أو شركة مالية تقدم خدمات مصرفية، مع ضرورة توافر القصد لقيام جريمة الحصول على المعلومات المصرفية أو المالية الإلكترونية في جميع الأحوال.

▪ الفرع الخامس: أركان جنحة الحصول غير المشروع على المعلوماتِ المُستهدفةِ وعقوبتها في القانون البحريني

في واقع الأمر، لم يفرد قانون جرائم تقنية المعلومات البحريني رقم (60) لسنة2014 نصاً خاصاً لتجريم واقعة الحصول على المعلومات المصرفية أو المالية الإلكترونية بصورة غير مشروعة كسائر القوانين المقارنة، ولكن يرى الباحثان بأنه يمكن تطبيق المادة (4) من القانون السالف الذكرعلى هذه الواقعة، وقد جرى نص هذه المادة كما يلي: " مع عدم الإخلال بأية عقوبة أشد في أي قانون آخر، يعاقب بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين، من تنصت أو التقط أو اعترض دون مسوغ قانوني مستخدماً وسائل فنية، إرسالاً غير موجه للعموم لبيانات وسيلة تقنية المعلومات، سواءً كانت البيانات مرسلة من نظام تقنية المعلومات أو إليه أو ضمنه، ويشمل هذا الإرسال أي انبعاثات لموجات كهرومغناطيسية من نظام تقنية المعلومات تحمل معها هذه البيانات".

وعليه، وانطلاقاً من هذه المادة يمكن تجريم واقعة الحصول على المعلومات المصرفية أوالمالية الإلكترونية بصورة غير مشروعة والمعاقبة عليها بموجب العقوبة الواردة فيها، وبتقدير الباحثان، فإن هذه المادة تتضمن بصورةٍ ضمنيةٍ الأركان المطلوبة لقيام جنحة الحصول على المعلومات المصرفية أو المالية الإلكترونية، وذلك كما يلي:

أولاً: بالنسبة لركن المحل (المعلومات المستهدفة)

أشارت المادة (4) من قانون جرائم تقنية المعلومات البحريني سالفة الذكر للمعلومات المستهدفة (بصيغة العموم) وذلك بقولها:" من تنصت أو التقط أو اعترض دون مسوغ قانوني مستخدماً وسائل فنية، إرسالاً غير موجه للعموم لبيانات وسيلة تقنية المعلومات"، فعبارة (لبيانات وسيلة تقنية المعلومات) جاءت هنا بصيغة العموم، وهي تستوعب جميع المعلومات، وبغض النظر عن نوعها أوطبيعتها، ومحل الحماية في هذه المادة هو هذه البيانات، وعلاوة على ذلك عرّفت المادة (1) من قانون جرائم تقنية المعلومات البحريني (بيانات وسيلة تقنية المعلومات) بأنها:" تمثيل لحقائق أو لوقائع أو لمعلومات أو لمفاهيم في صورة مناسبة تسمح لنظام تقنية المعلومات بمعالجتها".

ثانياً: بالنسبة للركن المادي

يرى الباحثان بأن (فعل الالتقاط الإلكتروني للبيانات بصورة غير مشروعة) الذي تم ذكره كأحد صور السلوك المادي المكون للجريمة المنصوص عليها في المادة(4) من قانون جرائم تقنية المعلومات البحريني يستوعب فعل الحصول على المعلومات المصرفية أو المالية الإلكترونية – لأنه يُقصَدُ بالالتقاط[1]، كما تمَّ تعريفُهُ في المادة (1) من قانون مكافحة جرائم تقنية المعلومات الإماراتي بأنه: "مشاهدة المعلومات أو البيانات أو الحصول عليها"، وعرَّفَهُ نظام مكافحة الجرائم المعلوماتية السعودي في المادة (10/1) بأنه: "مشاهدة البيانات أو الحصول عليها دون مسوغ نظامي صحيح"، وعليهِ, فإن التقاط بيانات وسيلة تقنية المعلومات يتحقَّقُ بالاطِّلاع عليها بالمشاهدة، أو السماع، أو الحصول عليها بأيّ طريقةٍ إلكترونية غير مشروعة.

ثالثاً: بالنسبة للركن المعنوي

على الرغم من أن القانون البحريني لم يشترط القصد صراحةً لقيام الجنح المنصوص عليها المادة(4) من قانون جرائم تقنية المعلومات، إلا أنه وبتقدير الباحثين، فإن هذه الجنح لا تقوم

[1] لمزيد من التفاصيل عن فعل الالتقاط، أنظر د. حمزة أبو عيسى، جرائم تقنية المعلومات، مرجع سابق، ص85.

إلا بتوافر القصد، وذلك لأنه يستفاد من المادة(31) من قانون العقوبات البحريني رقم (15) لسنة1976 [1]، بأنه حينما يسكت المشرع عن بيان صورة الركن المعنوي في جريمة معينة، فهذا يعني أن هذه الجريمة من الجرائم القصدية، ومن غير المتصور ارتكابها بالخطأ.

رابعاً: العقوبة المقررة لهذه الجنحة في القانون البحريني

عاقبت المادة (4) من قانون جرائم تقنية المعلومات البحريني على هذه الجنحة، بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين، وتعتبر هاتان العقوبتان من عقوبات الجنح، عملاً بنص المادة (50) من قانون العقوبات البحريني[2].

وفي نهاية هذه الجزئية، يوصي الباحثان المشرع البحريني، بوضع نصاً خاصاً في قانون جرائم تقنية المعلومات البحريني، يُجرّم صراحةً فعل الحصول غير المشروع على المعلومات المصرفية أو المالية الإلكترونية بأي وسيلةٍ إلكترونية، والمعاقبة على هذا الفعل بعقوبة جنائية إذا تم الحصول على هذه المعلومات من نظام معلومات إلكتروني خاص ببنك أو شركة مالية تقدم خدمات مصرفية، والمعاقبة على ذات الفعل بعقوبة جنحية، إذا تم الحصول على المعلومات ذاتها بوسيلةٍ إلكترونية، من أي وعاء إلكتروني، (باستثناء نظام المعلومات الإلكتروني الخاص بالبنوك أو الشركات المالية التي تقدم خدمات مصرفية).

▪ الفرع السادس: جريمة الحصول غير المشروع على المعلوماتِ المُستهدفةِ وعقوبتها في النظام السعودي

تنص المادة (2/4) من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي (م/17, رقم 79) لسنة 2007 على أنه: " يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من

---

[1] تنص المادة (31) من قانون العقوبات البحريني على أنه: " لا مسؤولية على من ارتكب الفعل المكون للجريمة من غير إدراك أو اختيار).

[2] تنص المادة(50) من قانون العقوبات البحريني على أنه: " عقوبات الجنحة هي الحبس والغرامة التي يجاوز حدها الأقصى خمسة دنانير والتجريد المدني الذي لا تزيد مدته على ثلاث سنين ولا تقل عن سنة".

الجرائم المعلوماتية.... 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".

نود الإشارة ابتداءً، بأن النظام السعودي لا يعترف بحسب علمنا، بتقسيمات الجرائم من حيث الجسامة إلى جنايات وجنح ومخالفات كما هو معروف في القوانين الوضعية المختلفة، لذلك فإننا سنتحفظ على الحديث عن تقسيمات الجرائم من حيث الجسامة إلى جنايات وجنح ومخالفات في مجال حديثنا عن جريمة الحصول على المعلومات المصرفية أوالمالية الإلكترونية وعقوبتها في النظام السعودي، وعليه سنكتفي بالإشارة لذكر أركان هذه الجريمة وعقوبتها كما يلي:

أولاً: أركان جريمة الحصول على المعلوماتِ المُستهدفةِ وعقوبتها في النظام السعودي

1- ركن المحل

يتمثل هذا الركن كما جاء في المادة (2/4) من نظام مكافحة الجرائم المعلوماتية السعودي، بالبيانات الإلكترونية البنكية أو الائتمانية أو التي تتعلق بملكية أوراق مالية.

2- الركن المادي

يتمثل بالحصول بصورةٍ غير مشروعة على البيانات الإلكترونية البنكية أو الائتمانية أو التي تتعلق بملكية أوراق مالية، ويتعيّن الحصول على هذه البيانات باستخدام الحاسب الآلي أو الشبكة المعلوماتية، ويستفاد ذلك من تعريف الجريمة المعلوماتية الوارد في المادة (1) من نظام مكافحة الجرائم المعلوماتية السعودي التي عرّفتها بأنها: "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".

3- الركن المعنوي

لم تحدد المادة (2/4) من نظام مكافحة الجرائم المعلوماتية السعودي صورة الركن المعنوي المطلوب توافرها لقيام هذه الجريمة وبتقدير الباحثان، فإن هذه الجريمة لا تقوم إلا بتوافر

القصد، ولأن الأصل العام في التشريعات المختلفة، إن سكوت المشرع عن بيان صورة الركن المعنوي في جريمة معينة، يُعني أن هذه الجريمة من الجرائم القصدية، ومن غير المتصور ارتكابها بالخطأ[1].

ثانياً: العقوبة المقررة لجريمة الحصول غير المشروع على المعلوماتِ المُستهدفةِ في النظام السعودي

عملاً بالمادة (2/4) من نظام مكافحة الجرائم المعلوماتية السعودي يعاقب على هذه الجريمة بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين.

وفي نهاية هذه الجزئية المتعلقة بالشأن السعودي، فإننا نأمل من المنظم السعودي، تعديل نص المادة(4) من نظام مكافحة الجرائم المعلوماتية، بحيث يضاف إليها تجريم فعل الحصول غير المشروع على المعلومات المصرفية أو المالية الإلكترونية بأي وسيلةٍ إلكترونية، والمعاقبة على هذا الفعل (بعقوبة السجن لمدة تزيد على ثلاث سنوات) إذا تم الحصول على هذه المعلومات من نظام معلومات إلكتروني خاص ببنك أو شركة مالية تقدم خدمات مصرفية.

▪ الفرع السابع: أركان جنحة الحصول غير المشروع على المعلوماتِ المُستهدفةِ وعقوبتها في القانون الأردني

نُذكر بنص المادة(6) من قانون الجرائم الإلكترونية الأردني الذي جاء فيه بأنه: "يُعاقب كل من حصل قصدًا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة, ولا تزيد على ثلاث سنوات، وبغرامة لا تقل عن (500) خمسمائة دينار, ولا تزيد على (2000) الفي دينار".

---

[1] لقد خرج على هذا الأصل العام المشرع الإماراتي في المادة(43) من قانون العقوبات، والمشرع القطري في المادة (32) من قانون العقوبات، وبشأن القصد المطلوب توافره في هذه الجريمة، أنظر، حسام الخولى، الحماية الجنائية والمدنية لعمليات البنوك الإلكترونية، مرجع سابق، ص285، وما بعدها.

كما أسلفنا القول، أنه ومن مطالعة المادة (6) السالفة الذكر بشكلٍ مستقل (أي دون ربطها بالمادة 7)، يتبيّن بأن جريمة الحصول على المعلومات المصرفية أوالمالية الإلكترونية ترتدي ثوب الجنحة، ويشترط لقيامها توافُر ثلاثة أركان، الركن الأول هوُ المحل ويتمثل بـ (المعلومات المصرفية أوالمالية المخزنة في أي وعاء إلكتروني)، والركن الثاني هو المادي، ويتمثل بـ (الحصول على المعلومات المصرفية أوالمالية المخزنة في أي وعاء إلكتروني بوسيلةٍ إلكترونية) أما الركن الثالث فهو المعنوي بصورة القصد، ومتى توافرت جميع هذه الأركان، يمكن القول بأننا أمام جنحة الحصول على المعلومات المصرفية أوالمالية الإلكترونية وحينئذٍ يتعين الحكم بعقوبتها الجنحية المنصوص عليها في المادة (6) من قانون الجرائم الإلكترونية.

ومن المُلاحظ أن جميع الأركان المطلوبة لقيام هذه الجنحة، هي ذاتها المطلوبة لقيام جناية الحصول على المعلومات المصرفية أو المالية الإلكترونية، باستثناء الركن الأول(ركن المحل) الذي يتمثل بالمعلومات المصرفية أوالمالية المخزنة في أي وعاء إلكتروني)، فهذا الركن يختلف عن ركن المحل في جناية الحصول على المعلومات المصرفية أوالمالية الإلكترونية الذي يتمثل بـ (المعلومات المصرفية أوالمالية المخزنة في وعاء إلكتروني مصرفي).

وبتوضيحٍ أكثر إن الفرق بين الجُنحة والجناية السالف ذِكْرُهُما، يكمُنُ في ركن المحل المطلوب توافُرُهُ فقط في جناية الحصول على المعلومات , وهو لزوم أن يقع السلوك المادي (فعل الحصول) على معلومات إلكترونية مخزنة في نظام معلوماتي خاص بشركة مالية تقدم خِدْمات مصرفية، فهذا الشرط غير مطلوب لقيام (جُنحة الحصول على المعلومات)؛ إذ لا يشترط لقيام هذه الجُنحة سوى أن يقع السلوك الجرمي على معلومات إلكترونية، وبِغَضّ النظر عن النظام المعلوماتي أو الموقع أو التطبيق الإلكتروني الذي يحتوي هذه المعلومات، فقد تكون هذه المعلومات مخزنة في البريد الإلكتروني الشخصي، وقد تكون موجودة في ملف إلكتروني موجود على سطح الكمبيوتر الشخصي، وقد تكون مخزنة على شكل مراسلات داخل أحد التطبيقات المسجلة بحساب شخصي، كتطبيق الواتس آب أو الفيس بوك.

سيما أن المادة (6) السالف ذِكْرُها، ذكرت كلمة (إلكترونية) فقط بقولها: "... تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية. .إلخ"، ولم يرد في المادة (6) ما يشير إلى ضرورة وجود نظام معلوماتي معيّن يحتوي هذه المعلومات المستهدفة، مثلما هو الحال في المادة (7) التي اشترطت صراحةً لزومَ

أن تكون المعلومات المستهدفة مخزنة في نظام معلومات خاص ببنك أو بشركة مالية تقدم خِدْمات مصرفية، كما أشرنا فيما سبق.

وبشأن عقوبة هذه الجنحة في القانون الأردني، فقد عاقبت عليها المادة (6) من قانون الجرائم الإلكترونية بالحبس مدة لا تقل عن سنة, ولا تزيد عن ثلاث سنوات، وبغرامة لا تقل عن (500) دينار, ولا تزيد عن (2000) دينار.

ومن المفيد الإشارة هنا إلى أنَّهُ إذا تم الشروع في هذه الجُنحة فلا عقاب على ذلك؛ لأنَّ المبدأ في قانون العقوبات الأردني كما أسلفنا القول، أنَّهُ لا عقاب على الشروع في الجُنَحِ إلا بنصّ خاص، ولا يوجد نصٌّ خاصٌّ يُعاقِبُ على الشروع في هذه الجُنحة[1].

وهذا ما أشارت إليه محكمة التمييز الأردنية بصورةٍ ضمنية بقولها[2]: "... وفي ذلك نجد أن المُشرِّع قد اشترط في المادة (6) من قانون الجرائم الإلكترونية للتجريم، أن يحصل المتهم دون تصريح قانوني عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات تتعلق ببطاقات الائتمان أو بالبيانات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية، وحيث إن المتهمين فشلا في الولوج إلى النظام الإلكتروني المصرفي الخاص بالبطاقات الائتمانية، فإن أفعالهما لم تتوافر فيها أركان وعناصر هذه التهمة".

ومُجمل القول، يرى الباحثان أنَّ المعلومات المخزنة في النظام المعلوماتي الخاص بالشركة المالية التي تقدم خِدْمات مصرفية، تُعَدُّ مَحَلًّا للجناية المقررة في المادة (7)، وهذه المعلومات تُعَدُّ في ذات الوقت ظرفًا مشددًا لعقوبة الجُنحة المقررة في المادة (6) السالِفِ ذِكْرُها.

ويستند الظرف المُشدد هنا –بحسب رأي الباحثين– على مبررات منطقية، تتمثل في ضرورة بسط المزيد من الحماية الجنائية للمعلومات المخزنة في أنظمة المعلومات المصرفية؛ وذلك لأهمية هذه المعلومات بالنسبة للاقتصاد الوطني، ناهيك أن أنظمة المعلومات المصرفية تتسم بأنها ذات وسائل حماية وإجراءات أمنية مشددة[3]، ولذلك فالجاني الذي يقتحم هذه الوسائل، ويستولي على المعلومات المصرفية، يُعَدُّ خَطِرًا وجديرًا بعقوبة الجناية.

---

[1] أنظر نص المادة (71) من قانون العقوبات الأردني رقم (16) لسنة1960.

[2] حكم محكمة التمييز، بصفتها الجزائية، رقم (555) لسنة2021, موقع قسطاس.

[3] بهذا المعنى أنظر، د. فاديا سليمان الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، المجلد 23، العدد1، 2015، ص8 وما بعدها.

وقبل أن نختم توضيح جُنحة الحصول على معلومات تتعلق ببطاقات ائتمان أو بمعاملات مالية أو مصرفية إلكترونية، في القانون الأردني ينبغي الإشارة إلى أنَّنا لا نتفق مع جانب من الفقه الأردني الذي نُجلُه[1]، فيما يراه من وجود تداخل وتناقض بين نَصَّي المادتين (6، 7) من قانون الجرائم الإلكترونية؛ لأنَّ المُشرِّع شدد العقوبة في المادة (7) إذا كان الدخول غير المشروع في نظام معلومات يتعلق بتقديم خِدْمات مصرفية، وبذات الوقت خفف المشرع عقوبة الحصول على معلومات تتعلق ببطاقات ائتمان أو بمعاملات مالية أو مصرفية إلكترونية في المادة (6).

ويرى الباحثان أنَّهُ وبالرغم من الصياغة المشوّشة والمُربِكةِ لِنَصَّي المادتين (6,7) من قانون الجرائم الإلكترونية، إلا أنه لا يوجد تناقض بين هاتين المادتين، والتنازع بينهما ليس إلا تنازعًا ظاهريًّا، ويمكن إزالتُهُ بالقول بأنه يُشترط لتطبيق نص المادة (7) مع الإحالة على المادة (6) من قانون الجرائم الإلكترونية– أن يتم الحصول على المعلومات الإلكترونية المستهدفة من نظام معلومات خاص ببنك أو بشركة مصرفية، وفي حال انتفاء هذا الشرط، يُصارُ إلى تطبيق نص المادة (6)، وبمفهوم المخالفة، فإنه إذا تمَّ الحصول على المعلومات المستهدفة من أي نظام معلوماتي بشكلٍ عام، فهنا تُطبَّقُ المادة (6) من القانون السالِفِ ذِكْرُه، وذلك على النحو الذي فصلناه فيما سبق.

وعلى الرغم من دقة المعيار القانوني الذي توصل إليه الباحثان، للتفرقة بين جناية الحصول على المعلومات المقررة في المادة (7) بالإحالة على المادة (6) من قانون الجرائم الإلكترونية، وبين جُنحة الحصول على هذه المعلومات المقررة في المادة (6) من ذات القانون– وهو معيارٌ يتعلق بوجود أو انتفاء نظام المعلومات المصرفي (محل الجريمة) الذي أُشير إليه فيما سبق, إلا أنَّ القضاء الأردني –وبكُلِّ أسف– حينَ تصدَّى لتكييف واقعة الحصول على المعلومات التي تتعلق ببطاقات الائتمان أو بالمعاملات المالية أو المصرفية، لم يُشِرْ للمعيار السالِفِ ذِكْرُه، ونراه يُكيِّفُ هذه الواقعة تارةً بأنها جناية وفقًا للمادة (7)، وتارة أخرى يُكيِّفُها بأنها جُنحة وفقًا للمادة (6)، دون الاستناد لأسانيد قانونية مقنعة، وذلك على نحوٍ سنشير إليه من خلال توضيح اتجاهين قضائيين؛ الأول: يُكيِّفُ هذه الواقعة بأنها جناية بحدود المادة (7) بالإحالة

[1] د. عبدالإله النوايسة، ود. ممدوح العدوان، الحماية الجنائية للعمليات المصرفية، مرجع سابق، ص59 و62.

على المادة (6)، والثاني: يُكيّفُها بأنها جُنحة بحدود المادة (6) من قانون الجرائم الإلكترونية، وسنستعرض هذين الاتجاهين والتعليق عليهما في البندين التاليين، ونؤكد هنا بأننا سنستعمل، عبارة(الحصول على المعلوماتِ المستهدفةِ) اختصاراً لعبارة (الحصول على معلومات بطاقات الائتمان أو المعاملات المالية والمصرفية الإلكترونية).

أولاً: الاتجاه القضائي الذي يُكيّفُ واقعة الحصول على المعلوماتِ المستهدفةِ بأنها جناية

جاء في أحد الأحكام الصادرة عن محكمة استئناف إربد لسنة 2018[1] ما نصُّه: "... وفي ذلك تجد محكمتنا وباستعراض الأفعال الصادرة عن المتهم المستأنف، والمتمثلة بقيامه بالاشتراك مع المتهم حسن، حيث قام المتهم حسن باستخدام كلمة الباسورد الخاص بالتحويلات المالية العائدة لشركة المشتكي للصرافة، والذي كان قد حصل عليها أثناء عمله في مكتب الصرافة العائدة لشركة المشتكي، ومن ثم القيام بتحويلات غير قانونية، بالاشتراك مع المتهم محمد، نَجَمَ عنها استيلاؤُهُما على مبالغ مالية من مكتب الصرافة العائدة للمشتكي دون وجه حق... وعليه فإن الأفعال التي قام بها المتهم المستأنف بالاشتراك مع باقي المتهمين، تشكل كافة أركان وعناصر، جناية المادة (7) من قانون الجرائم الإلكترونية".

يتضح من هذا الحكم، ومن الرجوع لحيثياته، أن الجاني حصل على معلومة تتعلق بخدمة مصرفية وهي (كلمة الباسورد الخاص بالتحويلات المالية). ويؤخذ على هذا الحكم أنه لم يوضح كيفية حصول الجاني على هذه المعلومة، وكل ما ورد فيه بهذا الشأن هو عبارة: "والذي كان قد حصل عليها أثناء عمله في مكتب الصرافة العائدة لشركة المشتكي", وكنا نتمنى لو جاء في الحكم ما يجيبُ عن التساؤل الآتي: – هل حصل الجاني على المعلومة من النظام المعلوماتي الخاص بالشركة من غيرِ تصريح؟ أم إنَّه حصل عليها بطريقة تقليدية كأن يكون قد حصل عليها من السجلات الورقية أو من أحد زملائه؟؛ لأنَّهُ –وبتقديرنا– من شروط قيام الجناية مدار البحث أن يتِمَّ الحصول على المعلومة من النظام المعلوماتي

[1] حكم محكمة استئناف إربد بصفتها الجزائية، رقم (13105) لسنة 2018، موقع قسطاس.

المصرفي، وبمفهوم المخالفة، فلا قيام لهذه الجناية حينما يتم الحصول على هذه المعلومة بأي طريقةٍ أخرى.

وقد قالت محكمة بداية عمَّان في حكمٍ لها صدر سنة 2018[1] ما نصُّه: "... تجد المحكمة أن الأفعال التي أقدم المتهمين على ارتكابها، والمتمثلة بحصولهم على معلومات تتعلق ببطاقات الصراف الآلي للبنوك، وحيازتهم على أوراق تتضمن مواقع الصرافات الآلية للبنك العربي والإسلامي الدولي، وقيامهم بتثبيت قطعة على مكان حاضنة بطاقات الصراف الآلي، وهي عبارة عن قارئ بيانات لبطاقات الصراف الآلي، وقيامهم بوضع كاميرات فوق الأزرار لغايات نسخ الأرقام السرية للبطاقات، وتمكنهم من نسخ بيانات 16 بطاقة، واستخدام هذه البطاقات والأرقام السرية بسحب نقود... ولهذا وتأسيسًا على ما تقدم تقرر المحكمة ما يأتي: ... تجريم المتهمين بجناية الحصول قصدًا ودون تصريح على معلومات تتعلق ببطاقة الائتمان بالاشتراك، وفقًا لأحكام المادة (7) من قانون الجرائم الإلكترونية، والمادة 76 من قانون العقوبات، وبدلالة المادة (6) من قانون الجرائم الإلكترونية".

وتعليقُنا على هذا الحكم بأنه لم يذكر في حيثياته، فيما إذا تم الحصول على معلومات بطاقات الصراف الآلي بوساطة النظام المعلوماتي للبنك العائد له الصراف الآلي أم لا، وبمعنى آخر، كنا نتمنَّى لو أنه جاء في حيثيات الحكم ما يجيب على التساؤل الآتي:– هل يُعَدُّ تثبيت قارئ معلومات بطاقة الصراف الآلي في مكان حاضنة هذه البطاقة، والحصول على معلوماتها بوساطة هذا القارئ دخولًا في النظام المعلوماتي للبنك العائد له الصراف الآلي؟

وبصيغةٍ أخرى: أتمَّ الحصول على معلومات بطاقة الصراف الآلي بهذه الطريقة بوساطة النظام المعلوماتي للبنك العائد له الصراف الآلي أم لا؟

لأنَّهُ – وفي تقديرنا– من شروط قيام الجناية مدار البحث وكما أسلفنا القول، أن يتمَّ الحصول على المعلومة من النظام المعلوماتي المصرفي، وبمفهوم المخالفة، فلا قيام لهذه الجناية حينَ يتم الحصول على هذه المعلومة بأي طريقةٍ أخرى، وفي واقع الأمر فإنَّ الإجابة عن مثل هذه التساؤلات تحتاج إلى خبيرٍ في تكنولوجيا المعلومات وبالعمليات المصرفية للبنوك.

[1] حكم محكمة بداية عمان بصفتها الجزائية، رقم (711) لسنة 2018، موقع قسطاس.

وثمّة حكم لمحكمة بداية عمّان صدر سنة 2019 قالت فيه[1]: "وبتطبيق القانون على الواقعة تجد المحكمة أن الأفعال التي أقدم عليها المتهمين المتمثلة، باستخدام بطاقات الفيزا بطريقة غير قانونية، لأشخاص معينين للاستيلاء على هذه المبالغ... أما فيما يتعلق بجُنحة الاحتيال وجُنحة السرقة وجُنحة التزوير واستعمال مزور في أوراق خاصة، المسندة للمتهمين جميعًا، وحيث تجد المحكمة أن هذه الجنح ما هي إلا عناصر رئيسة في الجناية المسندة للمتهمين جميعًا، وهي جناية الحصول دون تصريح على معلومات تتعلق ببطاقات ائتمانية واستخدامها على نظام معلومات أو موقع إلكتروني، وفقًا لأحكام المادة (7). ذلك إن استخدام هذه البطاقات والاستيلاء على الأموال والبضاعة، هي من صميم نتائج الجناية، ولا تشكل بحد ذاتها جُنحة الاحتيال أو جُنحة السرقة أو جُنحة التزوير...".

بالرجوع إلى حيثيات هذا الحكم لم نجد فيه ما يشير مطلقًا إلى أنَّهُ قد تمَّ الحصول على أرقام بطاقات الائتمان من خلال نظام معلومات مصرفي، وقد ورد فيه فقط، بأنه تم تزوير بطاقات الائتمان، واستخدامها للاستيلاء على أموال المالكين الحقيقين لهذه البطاقات، ومنعًا لتكرار ما قلناه فيما سبق، نكتفي بالقول هنا، بأنَّهُ يُفهم من هذا الحكم، بأنَّ المحكمة طبقت المادة (7) على الرغم من انتفاء شرط أساسي لقيام جناية الحصول على المعلومات مدار البحث، وهو شرط الحصول على معلومات بطاقات الائتمان من نظام معلومات مصرفي.

ثانياً: الاتجاه القضائي الذي يُكيّفُ واقعة الحصول على المعلوماتِ المستهدفةِ بأنها جُنحة

بما يتعارض تمامًا مع حكم محكمة بداية عمّان الصادر سنة 2018 الذي أشرنا إليه فيما سبق، كانت محكمة بداية غرب عمّان قد طبقت سنةَ 2016، نصَّ المادة (6) من قانون الجرائم الإلكترونية، واعتبرت جريمة الحصول على معلومات البطاقات الائتمانية بوساطة

[1] حكم محكمة بداية عمان بصفتها الجزائية، رقم (1584) لسنة 2019، موقع قسطاس. وهناك حكم مقارب لهذا الحكم تمَّ تطبيق المادة السابعة فيه، على الرغم من عدم توافر شروط تطبيقها، وهو حكم محكمة بداية عمّان بصفتها الجزائية، رقم (441) لسنة 2020.

النسخ من الصراف الآلي جريمة من نوع الجُنحة، فقالت[1]: "تجد المحكمة أنَّ فعل الظنينان، بالحصول على معلومات وبيانات البطاقات الائتمانية، بوساطة النسخ من الصراف الآلي، يُشكل كافة أركان وعناصر جرم الحصول على معلومات وبيانات تتعلق ببطاقات الائتمان بالاشتراك، خلافًا لأحكام المادة (6) من قانون الجرائم الإلكترونية...".

وفي واقعة مشابهة للواقعة السالِفِ ذِكْرُها، طبَّقَت ذاتُ المحكمة سنةَ 2016, أيضًا نص المادة (6) من قانون الجرائم الإلكترونية بقولها[2]: "وبتطبيق القانون على الواقعة، تجد المحكمة إن الأفعال التي أقدم عليها الظنين، من حيث قيامه باستخدام الشبكة المعلوماتية على سرقة المبالغ الموجودة في الصرافات الآلية، وقيامه بعد الدخول إلى الموقع الإلكتروني بالاستيلاء على الأموال، من خلال ناسخ وكاميرا وتصويرها، وتحويلها إلى أشخاص خارج الأردن، ... وعليه, وتأسيسًا لما تقدم تقرر المحكمة... إدانة الظنين عن جرم الحصول على معلومات تتعلق ببطاقات الائتمان، وبطاقات مستخدمة في تنفيذ المعاملات المالية وفقًا لأحكام المادة (6) من قانون الجرائم الإلكترونية".

ومن الجدير بالذكر، أنه وعلى الرغم من توافر جميع الشروط المطلوبة لقيام "جناية الحصول على معلومات تتعلق ببطاقات ائتمان أو بمعاملات مالية أو مصرفية يحتويها نظام معلومات مصرفي" إلا أن محكمة بداية عمّان طبقت المادة (6) من قانون الجرائم الإلكترونية بحكمٍ صدر عنها سنة 2017، إذ قالت فيه[3] ما نصُّه: "إن الأفعال التي قام بها الظنين والمتمثلة في قيامه بقرصنة حسابات المشتكيان، وتمكنه من تحويل مبالغ مالية من حساباتهم في بنك الإسكان لحسابه وحساب الظنين كساب دون علم الأخير، فإن أفعاله هذه تُشكل بحقه كافة أركان وعناصر جُنحة مخالفة أحكام المادة 6 من قانون الجرائم الإلكترونية...".

وفي عام 2017, وعلى الرغم من توافر شروط جناية الحصول على المعلومات مدار البحث، إلا أن محكمة بداية عمّان اعتبرت جريمة الحصول على معلومات مصرفية مخزنة في نظام معلومات مصرفي، عنصرًا من عناصر جُنحة السرقة، وفي ذلك قالت[4]: "... بالنسبة

---

[1] حكم محكمة بداية غرب عمّان بصفتها الجزائية، رقم (1263) لسنة 2016، موقع قسطاس.

[2] حكم محكمة بداية غرب عمّان بصفتها الجزائية، رقم (1526) لسنة 2016، موقع قسطاس.

[3] حكم محكمة بداية عمّان بصفتها الجزائية، رقم (1300) لسنة 2017، موقع قسطاس.

[4] حكم محكمة بداية عمّان بصفتها الجزائية، رقم (4714) لسنة 2017، موقع قسطاس.

لجُنحة الدخول قصدًا دون تصريح عن طريق الشبكة المعلوماتية على بيانات أو معلومات تتعلق ببطاقة الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية، خلافًا لأحكام المادة (6) من قانون الجرائم الإلكترونية، فإن المحكمة تجد أن فعل الظنين المتمثل بسرقة شريحة الهاتف لوالده، واستخدامها لغايات الدخول للحساب البنكي لوالدة، وتحويل مبلغ اربعة ألف دينار إلى حساب آخر وسحبه، فإن هذا الجرم ما هو إلا عنصر من عناصر جُنحة السرقة المسندة إلية، إذ لولا هذه الشريحة؛ لما تمكن من الاستيلاء على المبلغ الموجود في حساب والده، مما يتعين والحالة هذه إعلان عدم مسؤوليته عن هذا الجرم".

ومع الأسف فإن هذا الحكم يتعارض تمامًا مع حكمٍ آخرَ صَدَرَ عن ذات المحكمة سنة 2019، وقد أشرنا إليه فيما سبق، وسنُعيدُ مضمونَهُ هنا لتوضيح التعارض بين الحكمين، فقد قالت المحكمة في الحكم الصادر سنة 2019[1] ما نصُّه: "وبتطبيق القانون على الواقعة، تجد المحكمة أنَّ الأفعال التي أقدم عليها المتهمون, المتمثلة باستخدام بطاقات الفيزا بطريقة غير قانونية، لأشخاص معنيين للاستيلاء على هذه المبالغ... أما فيما يتعلق بجُنحة الاحتيال وجُنحة السرقة وجُنحة التزوير واستعمال مزور في أوراق خاصة، المسندة للمتهمين جميعًا، وحيث تجد المحكمة أن هذه الجُنَح ما هي إلا عناصرُ رئيسةٌ في جناية الحصول دون تصريح على معلومات تتعلق ببطاقات ائتمانية واستخدامها على نظام معلومات أو موقع إلكتروني، وفقًا لأحكام المادة(7)... ذلك أن استخدام هذه البطاقات والاستيلاء على الأموال والبضاعة، هي من صميم نتائج الجناية، ولا تشكل بحد ذاتها جُنحة الاحتيال أو جُنحة السرقة أو جُنحة التزوير...".

وفي تقديرنا فإنَّ التعارض بين الحكمين أصبح واضحًا، فالحكم الصادر سنة 2017 يقضي بأن جريمة الحصول على معلومات مصرفية مخزنة في نظام معلومات مصرفي، تُعَدُّ عنصرًا من عناصر جُنحة السرقة، في حينِ قضى الحكم الصادر سنة 2019 بأنَّ جنح السرقة والاحتيال والتزوير في أوراق خاصة واستعمالها، تُعَدُّ عناصر رئيسة في جناية الحصول على المعلومات المصرفية المخزنة في نظام المعلومات المصرفي.

[1] حكم محكمة بداية عمان بصفتها الجزائية، رقم (1584) لسنة 2019، موقع قسطاس.

ومُجمَلُ القول مِمَّا تقدم، يستنتج الباحثان أنَّ القضاء الأردني غيرُ مستقِرٍ في تكييف واقعة الحصول غير المشروع على معلومات تتعلق ببطاقات الائتمان أو بالمعاملات المالية والمصرفية الإلكترونية، على أنها جُنحة بحدود نَصِّ المادة (6) من قانون الجرائم الإلكترونية، أم أنَّها جنايةٌ بحدود نَصِّ المادة (7) بالإحالة على المادة (6). ويبدو أن القضاء الأردني يرى بأنَّهُ من الصعوبة أو الاستحالة التوفيقُ بين هذين النصين، ومن ثَمَّ فهو يميل إلى تطبيقِ النصِّ ذي العقوبة الأخف, وهو نص المادة (6) من القانون السالِفِ ذِكْرُه.

وفي الختام يوصي الباحثان القضاءَ الأردنيَّ بتطبيق العقوبة الجنائية المنصوص عليها في المادة (7) بالإحالة على المادة (6) من قانون الجرائم الإلكترونية، إذا تمَّ الحصول بوسيلة إلكترونية، على معلومات مصرفية أو مالية إلكترونية من نظام معلومات خاص ببنك أو شركة مالية تقدِّم خِدْمات مصرفية، وتطبيق المادة (6)، إذا تمَّ الحصول بوسيلة إلكترونية على هذه المعلومات من أي نظام معلومات (أي أن يتم الحصول عليها من أي وعاء إلكتروني يحوي هذه المعلومات).

الخاتمة

أولًا: النتائج

1. من الصعوبةِ وضع تعريفاً جامعاً ومانعاً للأعمال المصرفية أو المالية أو المعلومات المصرفية أو المالية، نظراً لتشعب الأعمال المصرفية والمالية من حيث موضوعها وطبيعتها، وتبعاً لذلك تشعب المعلومات المصرفية والمالية.
2. جاءت المواد (4 من قانون مكافحة جرائم تقنية المعلومات الإماراتي، و3 من قانون مكافحة جرائم تقنية المعلومات الكويتي، و6 من قانون مكافحة جرائم تقنية المعلومات العُماني، و7 من قانون الجرائم الإلكترونية الأردني)– بظرف يُشدد عقوبة جريمة الحصول على المعلومات المصرفية والمالية الإلكترونية، لتصبح عقوبة جناية، وذلك حين الحصول على هذه المعلومات من نظام معلومات خاص ببنك أو شركة تقدم خدمات مصرفية أو مالية

3. أعطى القانون الإماراتي والكويتي والعُماني والأردني لجريمة الحصول على المعلومات المصرفية والمالية من نظام المعلومات الخاص بشركة تقدم خدمات مصرفية أو مالية وصفاً جنائياً، وقد اشترط القانون الإماراتي والكويتي والعُماني (خلافاً للمشرع الأردني)، لقيام هذه الجناية أن يتم الدخول غير المشروع في النظام المعلوماتي الخاص بالشركة التي تقدم خدمات مصرفية أو مالية.
4. يرى الباحثان لا أهمية تُذكر للتفرقة بين المعلومات المصرفية والمالية في مجال الحديث عن جناية الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية في القانون الإماراتي والكويتي والعُماني والإردني، لأن جميع هذه المعلومات تصلح لأن تكون محلاً لهذه الجناية، متى كانت مخزنة في نظام معلومات خاص ببنك أو بشركة مالية تقدم خدمات مصرفية أو مالية.
5. أعطى القانون الإماراتي والكويتي والعُماني والأردني لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية وصفاً جنحياً، وذلك حين الحصول على هذه المعلومات بوسيلةٍ إلكترونية من أي وعاء إلكتروني (بإستثناء الوعاء الإلكتروني الذي يتعلق بنظام المعلومات الخاص بشركة تقدم خدمات مصرفية أو مالية)، وغالبية المعلومات المصرفية والمالية التي تُعتبر محلاً للجنحة المنصوص عليها في هذه القوانين تتعلق ببطاقات الدفع المالي الإلكتروني.
6. لم تشترط المادة (12) من قانون مكافحة جرائم تقنية المعلومات الإماراتي لقيام جنحة الحصول على المعلومات المستهدفة توافر القصد، لذلك فقد ترتكب هذه الجنحة بالقصد أو الخطأ، وذلك عملاً بالمادة (43) من قانون العقوبات الإماراتي، التي يستفاد منها أن سكوت المشرع عن بيان صورة الركن المعنوي في جريمة معينة يُعني أن الجاني يسأل عن هذه الجريمة سواءً ارتكبها بالقصد أو بالخطأ.
7. أعطى القانون القطري لجريمة الحصول على المعلومات المستهدفة وصفاً جنحياً فقط، والمعلومات المستهدفة وفقاً لهذا القانون، هي تلك التي تتعلق ببطاقات التعامل الإلكتروني فقط، ولم تشترط المادة (12) من قانون مكافحة الجرائم الإلكترونية القطري لقيام جنحة

الحصول على معلومات بطاقات التعامل الإلكتروني توافر القصد، لذلك فقد ترتكب هذه الجنحة بالقصد أو الخطأ، وهذا ما يُستفاد من المادة (32) من قانون العقوبات القطري.

8. لم يفرد قانون جرائم تقنية المعلومات البحريني نصاً خاصاً لتجريم واقعة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية.
9. نص النظام السعودي على جريمة الحصول غير المشروع على المعلومات المستهدفة وعاقب عليها في المادة (2/4) من نظام مكافحة الجرائم المعلوماتية بعقوبة مخففة هي السجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين.
10. يرى جانب من الفقه الأردني ثمَّةَ تداخُلًا وتناقُضًا بين نَصَّي المادتين (6، 7) من قانون الجرائم الإلكترونية الأردني؛ لأنَّ المُشرِّع شدَّدَ العقوبة في المادة (7) إذا كان الدخول غير المشروع في نظام المعلومات الذي يتعلق بالخِدْمات المصرفية وجعلها عقوبة جناية، وفي ذات الوقت خفف عقوبة جريمة الحصول على المعلومات التي تتعلق ببطاقات الإئتمان أو بالمعاملات المالية أو المصرفية الإلكترونية، وجعلها عقوبة جنحية بموجب المادة (6)، ويرى الباحثان عدم وجود تناقُضٌ بين نصي المادتين (6 و7) من قانون الجرائم الإلكترونية الأردني، وأنَّ التنازُعَ بينهما تنازعٌ ظاهريٌّ فحسب، ويمكِنُ إزالتُهُ بالقول بأنَّهُ يُشتَرَطُ لتطبيق نص المادة (7) مع الإحالة على المادة (6) – بأنَّ يتم الحصول غير المشروع بوسيلة إلكترونية على المعلومات التي تتعلق ببطاقات الإئتمان أو بالمعاملات المالية أو المصرفية الإلكترونية، من نظام معلومات خاص ببنك أو شركة مالية تقدم خِدْمات مصرفية، وفي حال انتفاء هذا الشرط يتمُّ تطبيق نص المادة (6).
11. لا يوجَدُ استقرارٌ في القضاء الأردني بشأنِ تكييفِ واقعة الحصول غير المشروع بوسيلة إلكترونية على المعلومات التي تتعلق ببطاقات الائتمان أو بالمعاملات المالية أو المصرفية الإلكترونية، فتارةً يُكيّفُها بأنُها جُنحة، بحدودِ نصّ المادة (6) من قانون الجرائم الإلكترونية، وتارةً أخرى يُكيّفُها بأنَّها جناية، بحدودِ نصّ المادة (7) بالإحالة على المادة (6).

ثانيًا: التوصيات

يوصي الباحثان بما يلي:

1. تعديل نص المادة (12) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، بأن يُشترط فيها توافر القصد لقيام جنحة الحصول غير المشروع على المعلومات المصرفية أو المالية الإلكترونية.
2. تعديل المادة (12) من قانون مكافحة الجرائم الإلكترونية القطري، بحيث يضاف إليها تجريم فعل الحصول غير المشروع على المعلومات المصرفية أو المالية الإلكترونية بأي وسيلةٍ إلكترونية، والمعاقبة على هذا الفعل (بعقوبة جنائية) أذا تم الحصول على هذه المعلومات من نظام معلومات إلكتروني خاص ببنك أو شركة مالية تقدم خدمات مصرفية، مع ضرورة توافر القصد لقيام جريمة الحصول على المعلومات المصرفية أو المالية الإلكترونية في جميع الأحوال.
3. وضع نصاً خاصاً في قانون جرائم تقنية المعلومات البحريني، يُجرّم صراحةً فعل الحصول غير المشروع على المعلومات المصرفية أو المالية الإلكترونية بأي وسيلةٍ إلكترونية، والمعاقبة على هذا الفعل بعقوبة جنائية أذا تم الحصول على هذه المعلومات من نظام معلومات إلكتروني خاص ببنك أو شركة مالية تقدم خدمات مصرفية، والمعاقبة على ذات الفعل بعقوبة جنحية، إذا تم الحصول على المعلومات ذاتها بوسيلةٍ إلكترونية، من أي وعاء إلكتروني، (باستثناء نظام المعلومات الإلكتروني الخاص بالبنوك أو الشركات المالية التي تقدم خدمات مصرفية).
4. تعديل نص المادة(4) من نظام مكافحة الجرائم المعلوماتية السعودي، بحيث يضاف إليها تجريم فعل الحصول غير المشروع على المعلومات المصرفية أو المالية الإلكترونية بأي وسيلةٍ إلكترونية، والمعاقبة على هذا الفعل (بعقوبة السجن لمدة تزيد على ثلاث سنوات) إذا تم الحصول على هذه المعلومات من نظام معلومات إلكتروني خاص ببنك أو شركة مالية تقدم خدمات مصرفية.
5. أن يُطبق القضاء الأردنيَّ العقوبة الجنائية المنصوص عليها في المادة (7) بالإحالة على المادة (6) من قانون الجرائم الإلكترونية، إذا تمَّ الحصول غير المشروع بوسيلة إلكترونية على معلومات تتعلق ببطاقات ائتمان أو بمعاملات مالية أو مصرفية إلكترونية، من

نظام معلومات خاص ببنك أو شركة مالية تقدم خِدْمات مصرفية، وبتطبيق المادة (6) إذا تمَّ الحصول غير المشروع بوسيلة إلكترونية على هذه المعلومات من أيِّ نظامِ معلوماتٍ بشكلٍ عام.

قائمة المصادر والمراجع

أولًا: الكتب

- د. اكرم ياملكي، الأوراق التجارية والعمليات المصرفية، دار الثقافة، عمّان، 2009
- أسامة المناعسة و جلال الزعبي، جرائم تظم المعلومات الإلكترونية، دار الثقافة للنشر، عمّان، 2017
- محمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر، عمّان، 2011
- د. عادل الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، عمّان، 2015
- د. احمد أبو خطوة، شرح الأحكام العامة لقانون العقوبات الإماراتي، الجزء الأول، الطبعة الأولى، منشورات أكاديمية شرطة دبي، الإمارات العربية المتحدة، 1989.
- د. حمزة أبو عيسى، جرائم تقنية المعلومات – دراسة مقارنة في التشريعات العربية، دار الثقافة للنشر والتوزيع، عمَّان، 2019.
- د. محمد العبادي، الجرائم المستحدثة في ظل العولمة، الطبعة الأولى، دار جليس الزمان، الأردن، 2015.
- د. محمد السعيد عبدالفتاح، الوجيز في شرح قانون العقوبات الاتحادي الإماراتي، القسم العام، الآفاق المشرقة، عمَّان، 2014.
- د. عبد الإله النوايسة، جرائم تكنولوجيا المعلومات، دار وائل للنشر والتوزيع، عمَّان، 2017.

ثانيًا: الرسائل الجامعية

- حسام الخولى، الحماية الجنائية والمدنية لعمليات البنوك الإلكترونية "دراسة مقارنة"، أطروحة دكتوراه، جامعة عين شمس، مصر، 2016.
- حسن المناصير، جريمة الدخول عير المشروع إلى النظام المعلوماتي والتعدي على محتوياته، رسالة ماجستير، جامعة جرش، الأردن، 2016.

ثالثًا: الأبحاث العلمية المنشورة

- د. فاديا سليمان، الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، المجلد 23، العدد1، الأردن، 2015.

- العنزي، زياد واحجيلة، عبدالله، الجوانب القانونية لمسؤولية مدير المجموعة في مواقع التواصل الاجتماعي في القانون الاتحادي الإماراتي، بحث منشور في مجلة الحقوق، جامعة البحرين، المجلد 16، العدد1، مملكة البحرين، 2019.
- د. عبدالإله النوايسة، و د. ممدوح العدوان، الحماية الجنائية للعمليات المصرفية الإلكترونية' الهيئة العالمية للتسويق الإسلامي، مجلة الإدارة والقيادة الإسلامية، المجلة 3، العدد1، 2018.

رابعًا: القوانين

- قانون العقوبات الأردني رقم (16) لسنة 1960
- قانون العقوبات الإماراتي رقم (3) لسنة1987
- قانون العقوبات القطري رقم (11) لسنة2004
- قانون العقوبات البحريني رقم (15) لسنة1976
- قانون الجزاء العُماني رقم (7) لسنة2018
- قانون الجزاء الكويتي رقم (16) لسنة1960
- قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015
- قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (5) لسنة 2012
- قانون مكافحة جرائم تقنية المعلومات العماني رقم (12) لسنة 2011
- قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014
- قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (63) لسنة 2015
- قانون جرائم تقنية المعلومات البحريني رقم(60) لسنة2014
- قانون البنوك الأردني رقم (28) لسنة2000
- قانون المصرف المركزي وتنظيم المنشآت والأنشطة المالية الإماراتي رقم (14) لسنة2018
- قانون النقد وبنك الكويت المركزي وتنظيم المهنة المصرفية الكويتي رقم (32) لسنة1968
- قانون مصرف قطر المركزي وتنظيم المؤسسات المالية رقم (13) لسنة2012
- القانون المصرفي العُماني رقم (114) لسنة2000
- نظام مراقبة البنوك السعودي رقم (م/5) لسنة 1966 (1386 هـ)
- قانون البنوك الموحد المصري رقم (88) لسنة 2003