الحماية الجنائية لنظم المعلومات المصرفية وبياناتها من خطر الجرائم ذات السلوك المُجرَّد من النتيجة

دراسة مقارنة بين القانون الأردني وقوانين دول مجلس التعاون الخليجي(*)(**)

د. عبدالله محمد احجيله
أستاذ القانون الجزائي المساعد

أ. أميرة سعيد الشماسي
باحث دكتوراه، القانون الجزائي

كلية القانون، جامعة اليرموك، إربد، المملكة الأردنية الهاشمية

الملخص

يتمحور موضوع هذه الدراسة حول الحماية الجنائية لنظم المعلومات المصرفية – وما تحتويه من معلومات – من خطر الجرائم ذات السلوك المُجرَّد من النتيجة، وفق القانون الأردني، وقوانين دول مجلس التعاون لدول الخليج العربية. وجاءت الدراسة لتعالج عدة مشكلات، أهمها: أن المادة (7) من قانون الجرائم الإلكترونية الأردني أقرّت عقوبةً جنائية واحدة لعدة جرائم تُشكل خطرًا على نظم المعلومات المصرفية، وذلك على الرغم من تفاوت درجة جسامة هذه الجرائم، وعدم النص في القانون الأردني والكويتي والبحريني والنظام السعودي على جريمة البقاء غير المصرح به في نظام المعلومات المصرفي.

وتوصلت الدراسة إلى عدة نتائج، أهمها: أن قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء القانونين القطري والبحريني) أقرَّت حمايةً جنائية نسبية للمعلومات المصرفية الإلكترونية من خطر جرائم السلوك المُجرَّد، وأن هناك عدم تناسب في العقوبات الجنحية المنصوص عليها في القوانين العُمانية والكويتية والسعودية، مع خطورة جريمة الدخول غير المشروع إلى نظام المعلومات المصرفي؛ بهدف تهديد سلامة المعلومات المصرفية.

(*) جزء من هذا البحث مُسْتَخلَص من رسالة ماجستير (للباحثة) بعنوان «جرائم الاعتداء على المعلومات المالية والمصرفية في قانون الجرائم الإلكترونية الأردني – دراسة مقارنة»، جامعة اليرموك، 2021، والدراسة المقارنة مع قوانين دول مجلس التعاون الخليجي وعدد من الجوانب الأخرى تم إضافتها وهي غير موجودة في متن الرسالة، وقد أجازته هيئة التحرير للنشر لأهمية الموضوع، وللإضافات التي أجراها الباحثان، وذلك وفقًا لقواعد النشر المعتمدة.

(**) تاريخ تقديم البحث للنشر: 22 سبتمبر 2021 تاريخ قبوله للنشر: 9 مارس 2022

وأوصت الدراسة بعدة توصيات، أهمها: تعديل العقوبة المقرَّرة في المادة (7) من قانون الجرائم الإلكترونية، بحيثُ تتدرَّجُ هذه العقوبة من حيثُ الشدة، وفقًا لجسامة الجريمة، كما أوصت بأن يتدخل المُشرِّعَ في كل من الأردن والكويت والبحرين والسعودية لوضع نصٍّ، يُجرِّم فعل البقاء غيرِ المُصرَّح بِهِ في نظام المعلومات المصرفي، وأن يشدد المشرِّع، في كل من عمان والكويت والسعودية عقوبة الجريمة التي تشكل خطرًا يهدد سلامة المعلومات المصرفية لتصبح عقوبة جنائية.

كلمات دالة: نظام معلومات، ومصرفية، وسلوك مُجرَّد، وخطر، وجرائم، وعقوبات.

المقدمة

أولًا: موضوع الدراسة

تحرصُ البنوك التجارية والشركات المالية على أن تكون هناك درجة عالية من الأمان التقني؛ وذلك حمايةً للمعلومات المصرفية وخصوصية عملائها، غير أنه، وعلى الرغم من ذلك، فإن الأعمال المصرفية الإلكترونية محفوفةٌ بالمخاطر التقنية، لذلك تنبهت بعض القوانين الحديثة لهذه المخاطر، ومن هذه القوانين، قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، فهذه القوانين تضمنت عدة نصوص تجريمية وعقابية، ويمكن الاستناد إلى هذه النصوص أو بعضها، لتوفير قدر من الحماية الجنائية لنظم المعلومات المصرفية – وما تحتويها من معلومات – من خطر بعض الأفعال التي تهدد سرية هذه النظم، أو سلامة معلوماتها المصرفية.

ثانيًا: إشكالية الدراسة

تتلخَّصُ إشكالية هذه الدراسة بأنَّ المادة (7)، من قانون الجرائم الإلكترونية الأردني، أقرت عقوبة جنائية واحدة لجريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية، وجريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية بهدف ارتكاب أفعال تشكل خطرًا يهدد سلامة المعلومات المصرفية، وجريمة استخدام برنامج إلكتروني بهدف ارتكاب أفعال تشكل خطرًا يهدد سلامة المعلومات المصرفية، هذا على الرغم من تفاوت هذه الجرائم من حيث درجة جسامتها.

وجاءت هذه الدراسة أيضًا لتعالج مشكلة ثانية في القانون الأردني؛ لأنه لم يميِّزَ بين عقوبات جرائم الدخول إلى نظم المعلومات المصرفية بهدف تشكيل خطر يهدد سلامة المعلومات المصرفية، مثل: إلغائها أو حذفها (جرائم السلوك المُجرَّد)، وعقوبات جرائم الدخول الذي يسبب نتيجة ضارَّة، مثل: إلغاء هذه المعلومات، أو حذفها (الجرائم ذات النتيجة).

كما سعت هذه الدراسة إلى معالجة مشكلة عدم النص على جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية في نظام مكافحة جرائم المعلوماتية السعودي، ومعالجة مشكلة عدم النص في القانون الأردني والكويتي والبحريني والنظام السعودي على جريمة البقاء غير المصرح به في نظام المعلومات المصرفي، وأخيرًا تطرقت الدراسة إلى مشكلة، عدم تناسب العقوبات الجنحية المنصوص عليها في القانون العُماني

والكويتي والسعودي مع خطورة جريمة الدخول غير المشروع في نظام المعلومات المصرفي؛ بهدف تهديد سلامة المعلومات المصرفية.

ثالثًا: تساؤلات الدراسة

تثيرُ إشكاليات الدراسة عدة تساؤلاتٍ جوهرية، أهمها ما يلي:

- ما مدى الحماية الجنائية التي وفّرها قانون الجرائم الإلكترونية الأردني وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية ،لنظم المعلومات المصرفية – وما تحتويها من معلومات – من خطر جرائم السلوك المُجرَّد؟
- إذا سلمنا بوجود حماية جنائية لنظم المعلومات المصرفية في القوانين المقارنة؛ فما الأركان المطلوبة لقيام الجرائم التي تشكل خطرًا على نظم المعلومات المصرفية، وعلى ما تحتويها من معلومات؟
- ما العقوباتُ المُقرَّرة للجرائم التي تشكل خطرًا على نظم المعلومات المصرفية، وعلى ما تحتويها من معلومات في القوانين المقارنة؟
- هل ثمّة مساواة بين عقوبات جرائم الدخول إلى نظم المعلومات المصرفية؛ بهدف تشكيل خطر يهدد سلامة المعلومات المصرفية، وبين عقوبات جرائم الدخول التي تنجم عنها نتيجة ضارَّة، مثل إلغاء المعلومات المصرفية في القوانين المقارنة؟
- هل تتناسب عقوبة جريمة الدخول غير المشروع إلى نظم المعلومات المصرفية بهدف تشكيل خطر يهدد سلامة المعلومات المصرفية مع خطورة هذه الجريمة في القوانين المقارنة؟

رابعًا: أهمية الدراسة

أدى تقديم الخدمات المصرفية، بالوسائل الإلكترونية، إلى اختراق بعض نظم المعلومات المصرفية، وارتكاب بعض الجرائم التي تشكل خطرًا يهدد سلامة المعلومات المصرفية المُخَزَّنة في هذه النُظم، وعليهِ تكمُنُ أهمية هذه الدراسة، لكونِها أوضحت مدى الحماية الجنائية لنظم المعلومات المصرفية – وما تحتويها هذه النظم من معلومات – من خطر جرائم السلوك المُجرَّد، وذلك في ضوء أحكام قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، وقد حددت هذه الدراسة مواطن قصور بعض القوانين المقارنة، بشأن موضوع الحماية

الجنائية لنظم المعلومات المصرفية، وما تحتويها هذه النظم من معلومات، وقدمت بعض المقترحات لمعالجة هذا القصور التشريعي.

خامسًا: أهداف الدراسة

تهدف هذه الدراسة إلى بيان مدى الحماية الجنائية التي وفّرها قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، لنظم المعلومات المصرفية – وما تحتويها من معلومات – من خطر جرائم السلوك المُجرَّد. وكذا تهدف هذه الدراسة إلى بيان أركان وعقوبات الجرائم التي تشكل خطرًا يهدد نظم المعلومات المصرفية، وعلى ما تحتويها من معلومات في القوانين المقارنة. كما تهدف هذه الدراسة إلى بيان مدى تناسب عقوبة جريمة الدخول غير المشروع في نظم المعلومات المصرفية؛ بهدف تشكيل خطر يهدد سلامة المعلومات المصرفية مع خطورة هذه الجريمة في القوانين المقارنة.

سادسًا: منهجية الدراسة

اتبع الباحثان، في هذه الدراسة، المنهجين الوصفي والتحليلي، وذلك من خلال استعراض وتحليل جميع نصوص قانون الجرائم الإلكترونية الأردني، ونصوص قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، التي تتعلق بالحماية الجنائية لنظم المعلومات المصرفية – وما تحتويها من معلومات – من خطر جرائم السلوك المُجرَّد، وذلك وفقًا للقواعد الأصولية في تفسير النصوص القانونية وتطبيقها.

وقد اتبع الباحثان أيضًا المنهج المقارن، وذلك بالمقارنة بين قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية في دول مجلس التعاون لدول الخليج العربية، وذلك لبيان مواطن القصور في هذه القوانين، وتقديم بعض المقترحات لمعالجة هذا القصور التشريعي.

سابعًا: خطة الدراسة

قُسِّمت خطة هذه الدراسة إلى مبحثين: خُصِّص الأوَّلُ منهما للحماية الجنائية لنظم المعلومات المصرفية من خطر الدخول المُجرَّد غير المشروع. وأوضح المبحث الثاني الحماية الجنائية للمعلومات المصرفية الإلكترونية من خطر جرائم السلوك المُجرَّد.

المبحث الأول
الحماية الجنائية لنظم المعلومات المصرفية
في مواجهة جريمة الدخول غير المشروع

أدى تقديم الخِدمات المصرفية والمالية بالوسائل الإلكترونية إلى ظهور أساليب احتيال جديدة؛ بهدف السطو على الأموال، وإجراء تحويلات مالية بصورةٍ غير مشروعة، وذلك من خلال نسخ معلومات البطاقات المصرفية، أو سرقة هذه البطاقات واستخدامها لإجراء عمليات السحب والتحويل الإلكتروني للأموال، أو من خلال اختراق المنظومة الأمنية المصرفية[1]، وتماشيًا مع ذلك، جرَّم القانون الأردني، وجميع قوانين دول مجلس التعاون لدول الخليج العربية، الدخول المُجرَّد غير المشروع إلى نظم المعلومات، ومن ضمنها نظام المعلومات المصرفي (باستثناء النظام السعودي، فهو لم يُجرِّم الدخول المُجرَّد غير المشروع إلى نظم المعلومات)[2]، وهذا التجريم، لم يكن أمرًا عفويًا، بل يحمل دلالات قانونية وفنية على أهمية جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات؛ فمعظم الجرائم الإلكترونية يتطلب ارتكابها المرور بهذه الجريمة، فهي بوابة مرور إجباري لارتكاب غيرها من الجرائم؛ وهي تعتبر بمنزلة الأُم لأغلب الجرائم الإلكترونية[3].

وينبغي التنبيه هنا على أنه من غير المُتَصَوَّر وجود حماية جنائية لنظم المعلومات المصرفية من خطر الدخول المُجرَّد غير المشروع من دون وجود نصوص قانونية تُجرّم هذا الدخول، وتعاقب عليه بعقوبة جزائية، ومن مطالعة المادة (7)، وبالإحالة إلى المادة

(1) فاديا سليمان الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، عمان، الأردن، المجلد 23، العدد1، سنة 2015، ص9.

(2) جرَّم قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012 الدخول المُجرد غير المشروع، في المادة (2)، وجرَّمه قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015، في المادة (2)، وجرَّمه قانون مكافحة الجرائم الإلكترونية القطري رقم 14 لسنة 2014، في المادة (3)، وجرَّمه قانون جرائم تقنية المعلومات البحريني رقم 60 لسنة 2014 في المادة (3)، كما جرَّمه قانون مكافحة جرائم تقنية المعلومات العُماني رقم 12 لسنة 2011 في المادة (3).

(3) عبدالإله النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، مج15، ع1، سنة 2016، ص15.

(3/ أ) من قانون الجرائم الإلكترونية الأردني، رقم (27) لسنة 2015، نجدها جرّمت هذا الدخول، وعاقبت عليه بعقوبة جزائية، وعلى هذه الوتيرة سارت إلى حدٍّ ما قوانين الجرائم الإلكترونية في دول مجلس التعاون لدول الخليج العربية.

لذلك سنوضح الحماية الجنائية لنظم المعلومات المصرفية من خطر الدخول المُجرَّد غير المشروع، من خلال بيان أركان جريمة الدخول المُجرَّد في نظم المعلومات المصرفية وعقوبتها. وبالعودة إلى القانون الأردني، فإننا نجده جرَّم في المادة (3/ أ)، من قانون الجرائم الإلكترونية، الدخول المُجرَّد غير المشروع إلى نظم المعلومات بشكلٍ عام، وعاقبت عليه هذه المادة بعقوبة جنحية سنفصلها فيما بعد، وبشكلٍ خاصٍّ جرّمت المادة (7) من قانون الجرائم الإلكترونية الأردني، وبالإحالة إلى المادة (3/ أ) من القانون ذاته الدخول المُجرَّد إلى نظم المعلومات المصرفية، وعاقبت عليه بعقوبة جنائية، فجاء في المادة (7) السالفة ذِكْرُها: «يُعاقَب كل من قام بأحد الأفعال المنصوص عليها في المواد من (3) إلى (6)، من هذا القانون، إذا وقعت على نظام معلومات، أو موقع إلكتروني، أو شبكة معلوماتية، تتعلق بتحويل الأموال، أو بتقديم خِدْمات الدفع، أو التقاص، أو التسويات، أو بأيٍّ من الخِدْمات المصرفية المُقدَّمة من البنوك والشركات المالية بالأشغال... إلخ».

يتضح مما تقدم أنه يتعيَّن ابتداءً لقيام جريمة الدخول غير المشروع إلى نظم المعلومات المصرفية توافر ركن مُفتَرَض هو «وجود نظام معلومات مصرفي»، بالإضافة إلى لزوم توافر الركنين المادي والمعنوي، وعليه، سنقسم هذا المبحث إلى أربعة مطالب، نُخصِّصُ الأولَ منها، للركن المُفتَرَض في هذه الجريمة، ونوضح في الثاني الركنَ الماديَّ المكون لها، وفي الثالث، سنُحدِّدُ الركنَ المعنويَّ المطلوب لقيام هذه الجريمة، وسنتناول في المطلب الرابع العقوبات التي أقرها القانون الأردني وقوانين دول مجلس التعاون لدول الخليج العربية لهذه الجريمة.

المطلب الأول

الركن المُفتَرَض في جريمة الدخول المُجرَّد غير المشروع في نظم المعلومات

لفهم الركن المُفتَرَض في جريمة الدخول المُجرَّد إلى نظم المعلومات المصرفية؛ وفقًا لأحكام القانون الأردني؛ يتعيَّن – ابتداءً – معرفة الشركات المالية التي تقدم الخِدْمات المصرفية؛ لأن نظام المعلومات المقصود بالحماية الجنائية هنا هو النظام الخاص بالشركات المالية التي تقدم خِدْمات مصرفية؛ وفقًا لأحكام المادة (7) من قانون الجرائم

الإلكترونية الأردني، بعد الإحالة إلى المادة (3/ أ) من القانون ذاته، هذا من جهة أولى، ومن جهة ثانية يتعيَّن لفهم الركن المُفتَرَض في الجريمة السالف ذكرها، وفقًا لأحكام قوانين دول مجلس التعاون لدول الخليج العربية، التعرّف على نظام المعلومات بشكل عام، وذلك لعدم وجود نصوص جنائية خاصة تحمي نظام المعلومات المصرفي في هذه القوانين، كما هي الحال في القانون الأردني، وبناءً على ذلك سنقسم هذا المطلب إلى فرعين، الفرع الأول: التعريف – بإيجاز – بالشركات المالية التي تقدم خِدْمات مصرفية في القانون الأردني، والفرع الثاني: التعريف بنظام المعلومات كمحلٍ لجريمة الدخول المُجرَّد غير المشروع (الركن المفترض)، وذلك كما يلي:

الفرع الأول

التعريف بالشركات المالية التي تختص بتقديم خدمات مصرفية

سنتناول أولًا مفهوم هذه الشركات، ثم نبيِّن ثانيًا بعض الخدمات المصرفية التي تقدمها، وذلك على النحو التالي:

أولًا: مفهوم الشركات المالية المختصة بتقديم خدمات مصرفية

هناك اتجاهٌ[4] يرى أن الخِدْمات المصرفية لا تُقدَّمُ من جميع الشركات المالية، بل تُقدَّمُ من بعضها فقط؛ لأن الشركات المالية تنقسم – بشكلٍ عام – إلى نوعين، النوع الأول: الشركات المالية المصرفية بطبيعتها، وتتمثل في البنوك التجارية (المصارف)، وقد عرَّفت المادة (2) من قانون البنوك الأردني، رقم 28 لسنة 2000، البنك بأنه: «الشركة التي يُرخَّصُ لها بممارسة الأعمال المصرفية وفق أحكام هذا القانون، بما في ذلك فرع البنك الأجنبي المُرخَّص له بالعمل في المملكة».

ويتلخص الدور الرئيس للبنوك في القيام بالأعمال المصرفية؛ مثل: فتح الحسابات الجارية، وقبول الودائع، ومنح القروض. وقد أشارت المادة السالف ذكرُها إلى الأعمال المصرفية التي تقوم بها البنوك، وهي: قبول الودائع من الجمهور، واستخدامها بصورة كلية – أو جزئية – لمنح الائتمان، أو أي أعمال أخرى يقرر البنك المركزي اعتبارها أعمالًا مصرفية.

(4) نورا عدلي رزق، المؤسسات المالية غير المصرفية، صندوق النقد العربي، الإمارات العربية المتحدة، ع6، السنة 2021، ص5.

ومن الجدير بالذكر أنَّ جميع البنوك (المصارف) الأردنية تُعَدُّ شركات مُساهِمَةً عامَّة، باستثناء البنك المركزي[5]، إذ يشترط لترخيص البنك أن يكون شركةً مساهِمة عامة، وذلك عملًا بنص المادة (6/ أ) من قانون البنوك، ويرى الباحثان أنَّ المعلومات المصرفية التي يحتويها نظام المعلومات المصرفي الخاص بالبنك المركزي الأردني مشمولًا بالحماية الجنائية للمعلومات المصرفية المقررة في المادة (7) من قانون الجرائم الإلكترونية الأردني، وذلك لأنَّ عبارة «... تتعلق بأي خدمة من الخِدْمات المصرفية التي تُقدَّمُ من البنوك والشركات المالية» جاءت مُطْلَقةً بنص المادة (7) السالف ذكرُها، ومن ثَمَّ فهذه العبارة تستوعب جميع البنوك المصرفية، بما في ذلك البنك المركزي.

وأما النوع الثاني من الشركات، فهو الشركات المالية غير المصرفية بطبيعتها، مثل: شركات التأمين، والوساطة المالية، وشركات الصرافة[6]، وهذا النوع من الشركات لا يجوز له القيام بالأعمال المصرفية التي هي حِكر على البنوك دون غيرها، ولكن قد تقوم بعض هذه الشركات، مثل شركات الصرافة (استثناءً) بتقديم بعض الخِدْمات المصرفية الإلكترونية، مثل: تحويل الأموال أو تلقيها من أي جهة أخرى، وشراء العملات النقدية وبيعها، وذلك وفقًا لنص المادة (16) من قانون أعمال الصرافة الأردني، رقم 44 لسنة 2015[7].

وقد عرَّفت المادة (2) من قانون البنوك الأردني الشركة المالية بأنها: «الشركة التي ينص عقد تأسيسها ونظامها الأساسي على أن من غاياتها ممارسة أنشطة مالية، باستثناء قبول الودائع غير مشروطة التوظيف». وعرَّفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الإماراتي، رقم 5 لسنة 2012، المُنشآت المالية أو التجارية أو الاقتصادية بأنها: «أي منشأة تكتسب وصفها المالي، أو التجاري، أو الاقتصادي، بموجب الترخيص الصادر لها من جهة الاختصاص بالدولة».

(5) تُعَدُّ جميع البنوك، باستثناء البنك المركزي الأردني، شركات خاصة، وهذا يُستفَاد من تعريف البنك الوارد في المادة الثانية من قانون البنوك الأردني. ويُستثنى من ذلك البنك المركزي، فهو يُعَدُّ مؤسسة عامة وفقًا لنص المادة (3/ أ) من قانون البنك المركزي رقم 23 لسنة 1971.

(6) في واقع الأمر لا يوجد تعريف موّحد للشركات المالية غير المصرفية بطبيعتها «حيث يختلف تعريف هذه الشركات من دولة إلى أخرى، وقد أشار إلى ملامحها مجلس الاستقرار المالي بقوله إنَّ «جميع الشركات المالية التي ليست بنوكًا مركزية، أو بنوكًا تجارية، أو شركات مالية عامة». وبالمجمل يمكن القول إنَّ الشركات المالية غير المصرفية تتكون – وفق الخدمات التي توفرها – من عدَّة شركات مالية، أهمُّها: شركات الصرافة والتأمين، وشركات التمويل غير المصرفية وشركات الوساطة المالية. بهذا المعنى يُنظَر: كارمايكل جفري ومايكل بومرليانو مايكل، تطور المؤسسات المالية غير المصرفية ومراقبتها، منشورات البنك الدولي (السلسلة المالية)، ترجمة: الأكاديمية العربية للعلوم المالية والمصرفية، عمان، الأردن، 2004، ص3 - 6.

(7) يُنظر: نص المادة (16) من قانون أعمال الصرافة الأردني رقم 44 لسنة 2015، فهذه المادة حددت الأعمال التي تمارسها شركات الصرافة.

ومن المفيد الإشارة هنا إلى ذكر المؤسسات المالية، كما جاءت في المادة (1) من قانون مصرف البحرين المركزي والمؤسسات المالية، رقم 64 لسنة 2006، وهي: «البنوك وشركات التأمين، والشركات العاملة في مجال الأوراق المالية والمحافظ والصناديق الاستثمارية، وشركات التمويل، وشركات الصرافة، وسماسرة ووسطاء المال، ووسطاء التأمين، ووسطاء سوق الأوراق المالية، وشركات الاستشارات المتخصصة في مجال صناعة الخدمات المالية، وشركات التقييم والتصنيف الائتماني، وسوق البحرين للأوراق المالية، وأسواق المعادن الثمينة، والسلع الاستراتيجية، والمؤسسات المساندة للقطاع المالي، بما في ذلك المؤسسات التي تقدم خدماتها المالية وفقا لأحكام الشريعة الإسلامية».

ثانيًا: بعض الخدمات المصرفية التي تقدمها الشركات المالية

ذكرت المادة (7) من قانون الجرائم الإلكترونية الأردني – صراحةً – بعض الخِدْمات المصرفية التي قد تُقدَّمُ من الشركات المالية بالمعنى الواسع (البنوك والشركات المالية الأخرى)، وذكرت بعض هذه الخِدْمات على سبيل المثال، ومنها تحويل الأموال، ويقصد بـ«تحويل الأموال»، كما يرى جانب من الفقه[8]: «التحويل الذي يتم بصورة إلكترونية من حساب إلى حساب آخر لذات الجهة، أو إلى مستفيد آخر، وقد يتم بين البنوك والشركات المالية». ومن هذه الخدمات المصرفية أيضًا «المقاصة»، وهذه المقاصة تعتبر تسوية إلكترونية بين البنوك، وتتم بشكل إلكتروني في غرفة المقاصة، وذلك عن طريق منح بنكٍ بنكًا آخَر القيام بحركات التحويلات المالية الدائنة والمدينة، وبشكلٍ إلكتروني من حساب مصرفي إلى حساب مصرفي آخر[9].

ويُقصد بالمقاصة، وفقًا للمادة (1) من قانون مصرف البحرين المركزي والمؤسسات المالية: «تحويل مجموعة من حقوق والتزامات أي مرخص له إلى رصيد واحد صافٍ مستحق له أو عليه»، ومن الخدمات المصرفية، على سبيل المثال أيضًا، «التسويات»، ويُقصد بها – وفقًا للمادة (1) من قانون مصرف البحرين المركزي: «تسوية مدفوعات أو التزامات الأطراف الناشئة عن المعاملات المتعلقة بالشيكات والأوراق المالية».

(8) عبدالإله النوايسة، جرائم تكنولوجيا المعلومات – شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمَّان – الأردن، 2017، ص293.

(9) المرجع السابق، ص295.

الفرع الثاني
التعريف بنظام المعلومات المُسْتَهدَف بجريمة
الدخول المُجرَّد غير المشروع

يُقصَدُ بالركن المُفتَرَض، الركنُ الذي يَفترِضُ القانونُ قيامَهُ وقتَ مباشَرَة الفاعل نشاطَه، وبغيرِه لا يُوصَفُ هذا النشاطُ بأنَّهُ جريمة. وقد يتمثل الركن المُفتَرَضُ بصفة خاصة في فاعل الجريمة، كما قد يتمثل في محل جريمة مُعيَّنة، كأن يكون المجنيُّ عليه إنسانًا حيًّا في جريمة القتل، وكذا الحالُ فإنَّ نظام المعلومات الخاص بالشركة المالية التي تقدم خِدْمات مصرفية يُعَدُّ مَحَلًا لجريمة الدخول غير المشروع في النظام الخاص بهذه الشركة. وقد 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 ليست لها دلالة بذاتها».

وبشكلٍ عام، يُقصَدُ بنظام المعلومات، كما جاء في المادة (2) من قانون الجرائم الإلكترونيةً الأردني بأنَّهُ: «مجموعة الأدوات والبرامج المُعدَّة لإنشاء المعلومات، أو البيانات إلكترونيًا، أو إرسالها، أو تسلمها، أو معالجتها، أو تخزينها، أو إدارتها، أو عرضها بالوسائل الإلكترونية». وعرَّفت المادة (2) من القانون ذاته الشبكة المعلوماتية بأنَّها: «ارتباطٌ بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها»، وكذا عرَّفت المادة ذاتُها الموقعَ الإلكتروني بأنه: «الحيِّزُ الذي يكون من خلال إتاحة البيانات والمعلومات على الشبكة المعلوماتية، ويكون ذلك من خلال عنوان إلكتروني مُحدَّد».

وقد عرَّفت المادة الأولى، من قانون مكافحة جرائم تقنية المعلومات الإماراتي نظام المعلومات الإلكتروني بأنه: «مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية، أو ما شابه ذلك».

وبهذا المعنى تم تعريف نظام المعلومات في المادة الأولى، من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015، وفي المادة الأولى من قانون مكافحة الجرائم الإلكتروني القطري رقم 14 لسنة 2014، وفي المادة الأولى من قانون جرائم تقنية المعلومات البحريني، رقم 60 لسنة 2014، وفي المادة الأولى من قانون جرائم تقنية المعلومات العُماني رقم 12 لسنة 2011، وفي المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي رقم 17م لسنة 2007، ويُستنتج من جماع التعاريف القانونية

لنظام المعلومات، كما وردت في قوانين دول مجلس التعاون لدول الخليج العربية السالفة الذكر، أنها تنطبق على أيِّ نظام معلومات، بما في ذلك نظام المعلومات المصرفي.

نخلص مما سلف، بأنه يُسْتَفَاد من المادة (7)، وبالإحالة إلى المادة (3/ أ) من قانون الجرائم الإلكترونية الأردني، أن أيَّ نظام معلومات خاص بشركة مالية تقدم خِدْمات مصرفية، يتضمن العديد من المعلومات المصرفية، وهذه المعلومات قد تتعلق بتحويل الأموال، وقد تتعلق بالمقاصة أو بالتسويات المالية، وقد تتعلق هذه المعلومات بأي خدمة من الخِدْمات المصرفية، كما أن النظام المعلوماتي الخاص بالشركات التي تُقدِّم خِدْمات مصرفية يصلُحُ لِأَنْ يكونَ مَحَلًا لجريمة الدخول المُجرَّد غير المشروع، المنصوص والمعاقَب عليها في المادة (7) بالإحالة إلى المادة (3/ أ) من قانون الجرائم الإلكترونية الأردني.

ويُسْتَفَاد من نصوص قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء النظام السعودي؛ لأنه لم ينص على جريمة الدخول المُجرَّد في نظم المعلومات) أن نظام المعلومات المصرفي يصلح لأن يكون محلًا لجريمة الدخول المُجرَّد غير المشروع في نظم المعلومات، حتى لو لم يتم النص بشكلٍ خاص على جريمة الدخول المُجرَّد غير المشروع في نظم المعلومات المصرفية في تلك القوانين؛ وذلك لأن هذه القوانين نصت على جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات بشكلٍ عام.

المطلب الثاني

الركن المادي في جريمة الدخول المُجرَّد غير المشروع في نظم المعلومات المصرفية

يقوم الركن المادي في هذه الجريمة، وفقًا لأحكام القانون الأردني، بمُجرَّد الدخول بطريقة غير مشروعة إلى نظام المعلومات المصرفي، وبمعنى آخر فإنَّ الركن المادي لهذه الجريمة يتحقق، حتى لو لم تقع أيُّ نتيجة جُرميّة، ويتحقق النشاط المادي لهذه الجريمة – كذلك – بصورته البسيطة الواردة في المادة (3/ أ) بالقيام بسلوك إجرامي يتخذ شكل الدخول إلى نظام معلومات مملوك للغير بصورةٍ غير مشروعة، ويستوي أن يكون الدخول إلى جميع قواعد المعلومات أو بعضها.

ويتحقق الركن المادي، في حال الدخول إلى النظام المعلوماتي من دون إذنٍ من مالِكه، أو في حالِ مخالفة حدود الإذنِ الممنوحة له، أو في حالِ تجاوز الحدِّ المسموح به بالدخول

إلى النظام، وهذا يُسْتَفَاد من صياغة نصِّ المادة (3/ أ) من قانون الجرائم الإلكترونية الأردني التي جاء فيها: «يُعاقَب كل من دخل قصدًا إلى الشبكة المعلوماتية، أو نظام معلومات، بأي وسيلة دون تصريح، أو بما يخالف أو يجاوز التصريح، بالحبس...». ويقوم الركن المادي في هذه الجريمة، وفقًا لأحكام قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء النظام السعودي؛ لأنه لم ينص على هذه الجريمة)، بمُجرَّد الدخول بطريقة غير مشروعة إلى نظام المعلومات المصرفي.

وبناءً على ما تقدم، سنوضح المقصود بالدخول غير المشروع، وسنبيِّن مدى قيام جريمة الدخول المُجرَّد إلى نظام المعلومات المصرفي، إذا كان هذا النظام محميًّا بوسائل حماية أمنية، وسنبيِّن كذلك، مدى تجريم البقاء غير المصرح به داخل نظام المعلومات المصرفي في ضوء أحكام القانون الأردني، وقوانين دول مجلس التعاون لدول الخليج العربية، من خلال الفروع التالية:

الفرع الأول

المقصود بالدخول كنشاط جرمي في جريمة الدخول غير المشروع إلى نظم المعلومات

لم يُعرِّف قانون الجرائم الإلكترونية الأردني الدخول غير المشروع، ولكن تطرَّقت المادة الثانية منه إلى تعريف التصريح بشكلٍ عام، وقالت بأنه: «الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو الشبكة المعلوماتية بقصد الاطلاع، أو إلغاء، أو حذف، أو إضافة، أو تغيير، أو إعادة نشر بيانات، أو معلومات، أو حجب الوصول إليها، أو إيقاف عمل الأجهزة، أو تغيير موقع إلكتروني، أو إلغائه، أو تعديل محتوياته».

وقد تم تعريف الدخول غير المشروع بموجب المادة الثانية من نظام مكافحة الجرائم المعلوماتية السعودي بقولها إنَّهُ: «دخولُ شخصٍ بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها»، وقد عرّفته المادة الأولى من قانون جرائم تقنية المعلومات الكويتي بأنه: «النفاذ المتعمد غير المشروع إلى أجهزة وأنظمة الحاسب الآلي، أو لنظام معلوماتي، أو شبكة معلوماتية، أو موقع إلكتروني، من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأيِّ غرضٍ كان، من دون تفويض في ذلك، أو بالتجاوز للتفويض الممنوح».

ويرى الباحثان أنَّ المنهج التشريعيَّ الأكثر توفيقًا هو المنهجُ الذي لم يُعرِّف الدخولَ غير المشروع إلى نظم المعلومات؛ لأنَّ تجريم الدخول غير المشروع إلى نظام معلوماتي يرتبط بأمور تقنية متغيِّرة ومتطورة، ومن ثَـمَّ فإنَّ تعريفَهُ قد يَحُدُّ من مدى التجريم لعجز التعريف عن مجاراة واستيعاب المستجدات الإلكترونية، وقد سلك هذا الاتجاه القانون الأردني والإماراتي، والقطري، والعُماني، والبحريني.

ومما يجدر ذِكْرُهُ أنَّهُ يمكن أن يتم الدخول إلى نظام المعلومات بأيِّ وسيلة، وهذا ما عبّرت عنه المادة (3/ أ) من قانون الجرائم الإلكترونية الأردني صراحةً، بقولها: «يُعاقَب كل من دخل قصدًا إلى... نظام معلومات بأي وسيلة»، ووسائل الدخول التي يمكن اللجوء إليها للدخول غير المشروع تتعدد وتتنوع؛ ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل جهاز الحاسب الآلي، أو فتح برنامج معين، أو الحصول على شفرات خاصة بالدخول، وقد يتطلب الحصول على اسم مستخدم مُعيَّنٍ ورقمٍ سِرِّيٍّ مُعيّن.

الفرع الثاني

مدى اشتراط وجود وسائل حماية أمنية لنظام المعلومات لقيام جريمة الدخول المُجرَّد

ثمّة اتجاهان بشأن هذه المسألة، يتلخص رأيُ الاتجاه الأول، بأنَّه لا يُشترط وجود «وسائل حماية أمنية أو نظام أمني» لنظام المعلومات لقيام جريمة الدخول غير المشروع في النظام المعلوماتي؛ لأنه ليس للنظام الأمني إلا دورٌ واحدٌ هو إثبات سوءِ نيَّةِ من قام بالدخول إلى النظام المعلوماتي. ويتلخَّصُ رأيُ الاتجاه الثاني بأنَّ وجودَ «النظام الأمني» يُعَدُّ شرطًا مُفتَرَضًا لقيام جريمة الدخول في النظام المعلوماتي؛ لأن العدالة تقتضي عدم حماية الحق جنائيًا، إلا إذا اتخذ صاحبُهُ الاحتياطات اللازمة لحمايته[10].

ولم يتطلب القانون الأردني، وقوانين دول مجلس التعاون لدول الخليج العربية، شرط الحماية الأمنية، باستثناء القانون الكويتي الذي اشترط في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات التي عرَّفت «الدخول غير المشروع»، بأن يتم الدخول باختراق وسائل وإجراءات الحماية.

(10) خالد الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري – دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة قطر، 2019، ص74 وما بعدها، وانظر كذلك: مروان محمد الزعبي، الحماية الجنائية للنقود الرقمية ودورها في تنشيط التجارة الإلكترونية، ط1، دار وائل للنشر والتوزيع، عمان، الأردن، 2020، ص106.

الفرع الثالث

مدى تجريم البقاء غير المصرح به داخل نظام المعلومات المصرفي

يُقصد بـ «البقاء غير المصرح به في نظام المعلومات» الدخول فيه بطريق الخطأ، أو أن يتجاوز الجاني حدود ما هو مسموح له أو مصرح له به، فالجاني هنا يستقر في نظام المعلومات، على الرغم من علمه بأنه لا يجوز له البقاء فيه، وتعتبر جريمة البقاء غير المصرح به في نظام المعلومات، حينما ينص عليها القانون، من الجرائم الشكلية مثلها، في ذلك، مثل جريمة الدخول المُجرَّد غير المشروع، حيث لا يُشترط في البقاء داخل النظام حدوث نتيجة معيَّنة، مثل: إتلاف أو تخريب أو تعديل البيانات، أو غير ذلك من الأفعال غير المشروعة[11].

ولم يتطرق المُشرِّع الأردني في قانون الجرائم الإلكترونية للبقاء غير المصرح به داخل النظام المعلوماتي بعد العلم بأنه تم الدخول في النظام بصورةٍ غير مشروعة، وكما أسلفنا القول يحدُثُ هذا الفرضُ حينما يتم الدخول إلى النظام المعلوماتي بطريق الخطأ أو بالمصادفة، ثم يكتشف من دخل إلى النظام أن دخوله تم بصورةٍ غير مشروعة، وعلى الرغم من اكتشافه ذلك فإنه لم يخرج من النظام. ومن المعروف أن جريمة الدخول قصدية، ولا تُرتَكب بالخطأ، وذلك على نحو سنوضحه بعد قليل، وبناءً على ذلك فإن فعل البقاء غير المصرح به في النظام المعلوماتي على النحو السالف ذِكْرُه، لا يُعَدُّ جريمةً وفقًا للقانون الأردني؛ وذلك لعدم وجود نصٍّ يُجَرّم هذا الفعل، وذلك بخلاف القانون الفلسطيني الذي جرَّم ذلك صراحةً في القرار بقانون رقم 10 للعام 2018 بشأن الجرائم الإلكترونية[12].

ويؤيدُ الباحثان الاتجاهَ الفقهيَّ[13] الذي يرى ضرورةَ سَدِّ هذا الفراغ في القانون الأردني، بنصٍّ صريحٍ يُجَرِّم ويُعاقِبُ على فعل البقاء غير المصرح به في النظام المعلوماتي بشكلٍ عام. وبالرجوعِ إلى قوانين دول مجلس التعاون لدول الخليج العربية، وبعض القوانين العربية، اتضح أن القانون الإماراتي نص على جريمة البقاء غير المصرح به في

(11) حسام الخولى، الحماية الجنائية والمدنية لعمليات البنوك الإلكترونية، أطروحة دكتوراه، جامعة عين شمس، القاهرة، 2016، ص119.

(12) عبدالله ذيب محمود، جريمة الدخول غير المشروع وفقًا للقرار بقانون رقم 10 لعام 2018 بشأن الجرائم الإلكترونية الفلسطيني، مجلة جامعة القدس المفتوحة للبحوث الإنسانية والاجتماعية، مج1، ع48، سنة 2019، ص5 وما بعدها.

(13) عبدالإله النوايسة، جرائم تكنولوجيا المعلومات، مرجع سابق، ص236.

النظام المعلوماتي صراحةً في المادة (1/2) من قانون مكافحة جرائم تقنية المعلومات، ونص عليها القانون القطري في المادة (3) من قانون مكافحة الجرائم الإلكترونية، ونص عليها القانون العُماني في المادة (3) من قانون مكافحة جرائم تقنية المعلومات.

وفي المقابل اتضح لنا خلو القانون الكويتي، والقانون البحريني، والنظام السعودي، والقانون السوري، من النص على جريمة البقاء غير المصرح به في النظام المعلوماتي، ولذلك نتمنى على المشرِّع الكويتي والبحريني والسعودي والسوري معالجة هذا القصور التشريعي.

المطلب الثالث

الركن المعنوي في جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية

يُشتَرط لقيام جريمة الدخول غير المشروع إلى نظم المعلومات المنصوص عليها في المادة (3/أ) من قانون الجرائم الإلكترونية الأردني، توافر القصد الجنائي، بعنصريه: العلم والإرادة، أي العلم بجميع ماديات الجريمة، وإرادة متجهة لارتكابها. ويمكن الاستدلال على القصد الجنائي، إذا كان النظام المعلوماتي محاطًا بنظام أمني وتم اختراقه، ومتى توافر القصد الجنائي العام بعنصريه: العلم والإرادة؛ قامت جريمة الدخول غير المشروع إلى النظام المعلوماتي، ولا يُعتَدُّ في الدافع على هذه الجريمة كدافع التسلية واللهو؛ لأنَّ الدافع لا يُعَدُّ عنصرًا من عناصر هذه الجريمة؛ لذلك لا يشترط في جميع القوانين المقارنة توافر قصد خاص لقيام جريمة الدخول المُجرَّد غير المشروع في نظم المعلومات المصرفية [14]. وقد أكد المُشرِّع الأردني صراحةً في المادة (3/ أ) من قانون الجرائم الإلكترونية بأنَّ هذه الجريمة من الجرائم القصدية؛ وعليهِ لا تُرتَكَبُ هذه الجريمةُ عن طريق الخطأ.

ومن الرجوع إلى قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، اتضح أن بعض هذه القوانين اشترط صراحةً لقيام جريمة الدخول المُجرَّد غير المشروع إلى النظام المعلوماتي توافر القصد، وهذه القوانين هي الكويتي والقطري والعُماني[15]، وبشكلٍ عام اشترطت المادة الأولى من نظام مكافحة جرائم المعلوماتية

(14) عادل حماد عثمان، الحماية الجنائية للمعاملات الإلكترونية في التشريع السوداني، أطروحة دكتوراه، جامعة أم درمان الإسلامية، السودان، 2015، ص48.

(15) المادة (1) من قانون مكافحة جرائم تقنية المعلومات الكويتي، والمادة (3) من قانون مكافحة الجرائم الإلكترونية القطري، والمادة (3) من قانون مكافحة جرائم تقنية المعلومات العُماني.

السعودي توافر القصد في الدخول غير المشروع، وذلك حينما عرّفت مصطلح «الدخول غير المشروع».

وعلى الرغم من أن القانون البحريني لم يشترط القصد – صراحةً – لقيام جريمة الدخول المُجرَّد غير المشروع المنصوص عليها في المادة (2) من قانون جرائم تقنية المعلومات، إلا أنه، وبتقدير الباحثَين، أن هذه الجريمة لا تقوم إلا بتوافر القصد، وذلك لأنه يُسْتَفَاد من المادة (31) من قانون العقوبات البحريني رقم 15 لسنة 1976[16]، بأنه حينما يسكت المشرِّع عن بيان صورة الركن المعنوي في جريمة معيَّنة، فهذا يعني أن هذه الجريمة من الجرائم القصدية، ومن غير المُتَصَوَّر ارتكابها بالخطأ.

وبالرجوع إلى أحكام القانون الإماراتي نجده لم يشترط (القصد) لقيام جريمة الدخول المُجرَّد غير المشروع المنصوص عليها في المادة (2) من قانون مكافحة جرائم تقنية المعلومات، وبتقدير الباحثين أنه يمكن ارتكاب هذه الجريمة بالقصد أو الخطأ، وذلك لأنه يُسْتَفَاد من المادة (43) من قانون العقوبات الإماراتي رقم 3 لسنة 1987، بأنه حينما يسكُت المشرِّع عن بيان صورة الركن المعنوي في جريمة معيَّنة، فهذا يعني أن الجاني يسأل عن هذه الجريمة سواء ارتكبها قصدًا أم خطأ[17].

ويخلص الباحثان، مما تقدم، إلى أنه يُشترَط لقيام جريمة الدخول غير المشروع إلى نظم المعلومات توافر القصد الجنائي وفقًا لأحكام القانون الأردني، وأحكام جميع قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء القانون الإماراتي) الذي يُسْتَفَاد من أحكامه أن الجاني يسأل عن هذه الجريمة، سواء ارتكبها قصدًا أو خطأ.

ويوصي الباحثان المُشرِّع الإماراتي بالتدخل بوضع نص صريح في قانون مكافحة جرائم تقنية المعلومات، يُشترط بمقتضاه توافر القصد لقيام جريمة الدخول المُجرَّد غير المشروع إلى نظام المعلومات المصرفي؛ لأن أي شخص معرّض للدخول إلى هذا النظام بالخطأ، ومن غير المنطقي معاقبته على ذلك بسبب خطأ غير مقصود.

(16) تنص المادة (31) من قانون العقوبات البحريني على أنه: «لا مسؤولية على من ارتكب الفعل المُكوِّن للجريمة من غير إدراك أو اختيار».

(17) تنص المادة (43) من قانون العقوبات الإماراتي على أنه: «يُسأَل الجاني عن الجريمة، سواء ارتكبها عمدًا أو خطأ ما لم يشترط القانون العمد صراحةً».

المطلب الرابع
عقوبة جريمة الدخول المُجرَّد غير المشروع
في نظم المعلومات المصرفية

يُعاقَب من يرتكب جريمة الدخول المُجرَّد إلى نظام معلومات مصرفي وفقًا للمادة (7) من قانون الجرائم الإلكترونية الأردني، بالأشغال المؤقتة لمدَّة لا تقلُّ عن خمس سنوات (يُعَدُّ الحَدُّ الأعلى لهذه العقوبة عشرين سنة عملًا بنص المادة (20) من قانون العقوبات الأردني)، وبغرامة لا تقلُّ عن (5000) خمسة آلاف دينار، ولا تزيد على (15000) خمسة عشر ألف دينار. وتتضاعف هذه العقوبة على مكرر هذه الجريمة؛ وذلك عملًا بنص المادة (16) من قانون الجرائم الإلكترونية الأردني، وقد خرج قانون الجرائم الإلكترونية على الأحكام العامة في الاشتراك الجرمي، وساوى بين عقوبة الاشتراك الأصلي والتبعي، فوفقًا للمادة (14) من القانون السالف ذِكْرُه، فيُعاقَب على الاشتراك، أو التدخل، أو التحريض على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحدَّدة لفاعلها.

وبشكلٍ عام جاءت عقوبات جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية في قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء النظام السعودي الذي لم يُجرِّم الدخول المُجرَّد غير المشروع إلى نظم المعلومات) من العقوبات الجنحية، وتتمثل بالحبس والغرامة أو إحداهما[18]، وذلك خلافًا لما هي عليه الحال في القانون الأردني الذي عاقب على هذه الجريمة بعقوبة جنائية هي الأشغال المؤقتة من خمس سنوات لغاية عشرين سنة، وبغرامة تتراوح بين خمسة آلاف دينار (5000 دينار) وخمسة عشر الف دينار (15000 دينار).

ويؤيد الباحثان المنهج المتشدد الذي تبناه المشرع الأردني بشأن المعاقبة على جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية؛ لأن نظم المعلومات المصرفية ذات وسائل حماية وإجراءات أمنية مشددة، والجاني الذي يقتحِمُ هذه الوسائل، ويدخل إلى نظم المعلومات المصرفية، يُعَدُّ خَطِرًا وجديرًا بعقوبة الجناية.

(18) لمعرفة مدة الحبس، ومقدار الغرامة يُنظر، المادة (2) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، والمادة (2) من قانون مكافحة جرائم تقنية المعلومات الكويتي، والمادة (3) من قانون مكافحة الجرائم الإلكترونية القطري، والمادة (3) من قانون جرائم تقنية المعلومات البحريني، والمادة (3) من قانون مكافحة جرائم تقنية المعلومات العُماني.

وخلاصة القول، في جريمتي الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية، والبقاء غير المصرح به في هذه النظم، إن كلًا منهما تعتبر جريمة قائمة بذاتها، وكلتاهما تقع بمُجرَّد إتيان الفعل المُجرَّد، وهو الدخول غير المشروع أو البقاء غير المصرح به في النظام، وكلتاهما لا تتطلب تحقق نتيجة معيَّنة، وبذلك فهما من الجرائم الشكلية (جرائم الخطر).

المبحث الثاني
الحماية الجنائية للمعلومات المصرفية الإلكترونية من خطر جرائم السلوك المُجرَّد

من المُسلَّم به أنَّ أحد تقسيمات الجرائم، من حيثُ ركنها المادي، هو تقسيمُها إلى نوعين: النوع الأول: الجرائم ذات النتيجة، وتُطلَقُ عليها تسميةُ «الجرائم المادية، أو جرائم الضرر»؛ لأنَّ السلوك الإجرامي فيها يُحقِّقُ ضررًا بالمصلحة التي يحميها القانون، ويتألَّفُ الركن المادي في هذه الجرائم من سلوكٍ إجرامي، ونتيجةٍ، وعلاقةٍ سببيَّةٍ تربِطُ بين السلوك وبين النتيجة.

أما النوع الثاني: فهي الجرائم ذات السلوك المُجرَّد من النتيجة، وتُطلَقُ على هذه الجرائم تسميةُ «الجرائم الشكلية أو جرائم الخطر»؛ لأنَّها تُعرِّضُ المصلحة المحمية للخطر من غيرِ أن تضُرَّ بها، ويتألف الركن المادي في هذه الجرائم من سلوكٍ إجراميٍّ مُجرَّد من النتيجة، وهذا السلوكُ يكفي وحدَهُ لتحقيق النتيجة في مدلولها القانوني أو الاعتداء على المصلحة التي يحميها القانون[19].

وتبرز أهمية هذا التقسيم من جهتين، الأولى: إنَّ الشروع في الجريمة غير مُتَصَوَّر إلا في الجرائم ذات النتيجة، أما جرائم السلوك المُجرَّد من النتيجة فلا محلَّ للشروع فيها؛ لأن السلوك الإجرامي فيها إما أن يقع فتقع الجريمة كاملة، وإما ألا يقع فلا يكون هناك جريمة، أما الجهة الثانية: فتتمثَّلُ في أنَّ بحث علاقه السببية لا يثور إلا في الجرائم ذات النتيجة؛ إذ تفترِضُ هذه العلاقةُ وجودَ عنصرين، هُما: السلوك الإجرامي والنتيجة، ولا مكانَ لبحث هذه العلاقة في جرائم السلوك المُجرَّد من النتيجة[20].

وبعد هذا التمهيد الموجز للجرائم ذات النتيجة، والجرائم ذات السلوك المُجرَّد من النتيجة، وبعد مطالعة الباحثين لنصوص قانون الجرائم الإلكترونية الأردني، ونصوص قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، يُلاحَظ أنَّ قانون الجرائم الإلكترونية الأردني، وأغلبية قوانين دول مجلس التعاون لدول الخليج العربية نصت على عدة جرائم تشكل خطرًا على سلامة المعلومات المصرفية الإلكترونية، وأدرجتها ضمن الجرائم ذات السلوك المُجرَّد من النتيجة.

(19) أسامة عبدالحفيظ، جرائم الاعتياد وتطبيقاتها في قانون العقوبات الجزائري، رسالة ماجستير، جامعة محمد بوضياف، المسيلة، الجزائر، 2018، ص32.

(20) أحمد أبو خطوة، شرح الأحكام العامة لقانون العقوبات الإماراتي، ج1، ط1، منشورات أكاديمية شرطة دبي، 1989، ص159.

وبناءً على ذلك سنقسم هذا المبحث إلى مطلبين، نخصص المطلب الأول للحماية الجنائية للمعلومات المصرفية الإلكترونية من جرائم تُشكل خطرًا على سلامتها، وسنوضح في المطلب الثاني، الحماية الجنائية للمعلومات المصرفية الإلكترونية من برنامج يُشكل خطرًا على سلامتها، وذلك كما هو تالٍ:

المطلب الأول

الحماية الجنائية للمعلومات المصرفية الإلكترونية من جرائم تُشكِّل خطرًا يُهدد سلامتها

بدايةً نود أن ننبه إلى أن وضع تعريف جامع مانع للأعمال المصرفية، أو المعلومات المصرفية، يُعد أمرًا بالغ الصعوبة؛ نظرًا إلى تشعب الأعمال المصرفية من حيث موضوعها وطبيعتها[21]، وتبعًا لذلك تشعب المعلومات المصرفية، وقد يكون من الصعب أيضًا تعداد حصري لتخصص الشركات المالية التي تقدم خدمات مصرفية، والدليل على ذلك أن قوانين البنوك في أغلب الدول اكتفت بوضع تعداد للأعمال المصرفية على سبيل المثال، من دون وضع تعريف منضبط ومحدَّد لها[22]، ويمكن الاستفادة من تعداد الأعمال المصرفية لمعرفة وتحديد طبيعة المعلومات كمعلومات مصرفية.

وكما أسلفنا القول، من غير المُتَصَوَّر وجود حماية جنائية لحق معيَّن، من دون وجود نصوص قانونية تُحدِّد السلوكيات التي تُشكل اعتداءً على هذا الحق، والجزاءات الجنائية التي تتناسب مع خطورة هذه السلوكيات، ومن هنا جاءت المادة (7) من قانون الجرائم الإلكترونية الأردني؛ لتقر الحماية الجنائية للمعلومات المصرفية الإلكترونية من أفعال معيَّنة تُشكل خطرًا على سلامة هذه المعلومات بقولها: «يُعاقَبُ كلُّ من قام بأحد الأفعال المنصوص عليها في المادتين (3) و(4) من هذا القانون، إذا وقعت على نظام معلومات... يتعلق بتحويل الأموال...، أو بأيٍّ من الخِدْمات المصرفية المقدَّمة من البنوك والشركات المالية بالأشغال المؤقتة... إلخ».

(21) حسام الخولي، مرجع سابق، ص43. أكرم يا ملكي، الأوراق التجارية والعمليات المصرفية، دار الثقافة، عمّان – الأردن، 2009، ص273.

(22) يُنظر: المادة (2) من قانون البنوك الأردني رقم 28 لسنة 2000، والمادة (1) من قانون المصرف المركزي وتنظيم المنشآت والأنشطة المالية الإماراتي رقم 14 لسنة 2018، والمادتان (54) و(77) من قانون النقد وبنك الكويت المركزي وتنظيم المهنة المصرفية الكويتي رقم 32 لسنة 1968، والمادة (1) من قانون مصرف قطر المركزي وتنظيم المؤسسات المالية رقم 13 لسنة 2012، والمادة (5) من القانون المصرفي العُماني رقم 114 لسنة 2000، والمادة (1) من نظام مراقبة البنوك السعودي رقم م/ 5 لسنة 1966 (1386هـ)، والمادة (31/ 2) من قانون البنوك الموحد المصري رقم 88 لسنة 2003.

وتنُصُّ المادة (3/ ب) من القانون ذاته على أنه: «إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء، أو حذف، أو إضافة، أو تدمير، أو إفشاء، أو إتلاف، أو حجب، أو تعديل، أو تغيير، أو نقل، أو نسخ بيانات، أو معلومات، أو توقيف، أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية، فيُعاقَبُ الفاعل بالحبس... إلخ».

وقد أُقرت الحماية الجنائية للمعلومات المصرفية الإلكترونية من هدف معيَّن (هو الحصول على هذه المعلومات بصورة غير مشروعة) يُشكل خطرًا على سلامة هذه المعلومات بنصوص خاصة وصريحة في جميع قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء القانون البحريني والقانون القطري).

فالقانون الإماراتي أقر الحماية الجنائية للمعلومات المصرفية الإلكترونية من محاولة تحقيق هدف معيَّن (هو الحصول على هذه المعلومات بصورة غير مشروعة) يُشكل خطرًا على سلامة هذه المعلومات صراحةً في المادة (4) من قانون مكافحة جرائم تقنية المعلومات، بقولها: «يُعاقَب بالسجن المؤقت والغرامة... كل من دخل من دون تصريح... إلى نظام معلومات إلكتروني،... سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية... إلخ».

وأكد القانون الكويتي هذه الحماية صراحةً في المادة (3/ 1) من قانون مكافحة جرائم تقنية المعلومات، بقولها: «يعاقَب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة... كل من ارتكب دخولًا غير مشروع إلى موقع أو نظام معلوماتي مباشرة... بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون... ويسري هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية».

وأقر القانون القطري هذه الحماية صراحةً في المادة (12/ 1) من قانون مكافحة الجرائم الإلكترونية، بقولها: «يعاقَب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة...، كل من استخدم أو حصل أو سهّل الحصول من دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات».

كما أقر القانون العُماني الحماية ذاتها صراحةً، في المادة (6) من قانون مكافحة جرائم تقنية المعلومات، بقولها: «يُعاقَب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة...، كل من دخل عمدًا ومن دون وجه حق موقعًا إلكترونيًا أو نظامًا معلوماتيًا، بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها... وتعد البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات المالية في حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة».

وأخيرًا، أقر نظام مكافحة جرائم المعلوماتية السعودي الحماية ذاتها صراحةً في المادة (4/ 2)، بقولها: «يُعاقَب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة... كل شخص يرتكب أيًا من الجرائم المعلوماتية: للوصول 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».

وينبغي التنبيه هنا إلى ملاحظتين، الأولى: إنه، وعلى الرغم من عدم وجود حماية جنائية للمعلومات المصرفية في قانون جرائم تقنية المعلومات البحريني، بشكل خاص وصريح، فإن هذه المعلومات تتمتع بحماية جنائية مثل سائر المعلومات الأخرى التي تمتّ حمايتها بموجب نصوص جزائية عامة، جاءت في هذا القانون، مثل نص المادة (2) الذي يُسْتَفَاد من صياغته أن جرائم الاعتداء على المعلومات الإلكترونية، بشكل عام، تندرج في القانون البحريني ضمن الجرائم ذات النتيجة، وبناءً على ذلك فالقانون البحريني يخرج عن موضوع دراستنا في هذه الجزئية.

أما المُلاحظة الثانية، فتتعلق بالمادة (12/ 1) من قانون مكافحة الجرائم الإلكترونية القطري، حيث يُسْتَفَاد من صياغة هذه المادة أن جرائم الاعتداء على المعلومات المصرفية الإلكترونية تندرج في القانون القطري ضمن الجرائم ذات النتيجة، وبناءً على ذلك فالقانون القطري يخرج عن موضوع دراستنا في هذه الجزئية.

وعليه، فالباحثان يستنتجان، مما سبق، أنَّ القانون الأردنيَّ، وجميع قوانين دول مجلس التعاون لدول الخليج العربية (باستثناء القانون البحريني والقانون القطري)، نَصّت صراحةً على العديد من الجرائم التي تُشكل اعتداء على المعلومات المصرفية، وجميع هذه الجرائم تدخل في دائرة الجرائم ذات السلوك المُجرَّد، وينبغي التنبيه هنا على أنَّنا سنذكر أسماء هذه الجرائم من خلال توضيح صور الركن المادي المكوِّن لكلٍّ منها؛ لأن كل صورة من صور الركن المادي تشكل جريمة مستقلة وقائمة بذاتها، وهذه الجريمة تُشكل خطرًا يهدد سلامة المعلومات المصرفية، وعليه سنوضح أركان هذه الجرائم وعقوباتها في الفروع التالية:

الفرع الأول

الركن المُفتَرَض في الجرائم التي تشكل خطرًا يهدد سلامة المعلومات المصرفية

يتمثَّلُ الركن المُفتَرَض في الجرائم التي تشكل خطرًا يهدد سلامة المعلومات المصرفية بـ «المعلومات المصرفية الإلكترونية المُخَزَّنة في نظام المعلومات المصرفي»، وهذا الركن

أشارت إليه المادة (7)، وبالإحالة إلى المادة (3/ ب) من قانون الجرائم الإلكترونية الأردني كما أسلفنا القول، ومن مطالعة قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، يتضح أن جميع هذه القوانين (باستثناء القانون البحريني والقانون القطري) نصت صراحةً على المعلومات المصرفية الإلكترونية بصيغ مختلفة كمحلٍّ للجرائم التي تشكل خطرًا يهدد سلامة هذه المعلومات، وهذا يُسْتَفَاد صراحة من نصوص المواد: (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، و(3) من قانون مكافحة جرائم تقنية المعلومات الكويتي، و(6) من قانون مكافحة جرائم تقنية المعلومات العُماني، و(4/ 2) من نظام مكافحة جرائم المعلوماتية السعودي، وقد سبق أن كتبنا تفاصيل هذه النصوص.

الفرع الثاني

الركن المادي في الجرائم التي تشكل خطرًا يُهدِّد سلامة المعلومات المصرفية

من مطالعة نصوص قانون الجرائم الإلكترونية الأردني، ونصوص قوانين الجرائم الإلكترونية في دول مجلس التعاون لدول الخليج العربية (باستثناء القانون البحريني والقانون القطري)، يتضح تعدد وتنوع صور الركن المادي في الجرائم ذات السلوك المُجرَّد التي تشكل خطرًا يهدد سلامة المعلومات المصرفية، وكما أسلفنا القول فإن كل صورة من صور الركن المادي تشكل جريمة مستقلة وقائمة بذاتها، وتُشكل خطرًا يهدد سلامة المعلومات المصرفية الإلكترونية، وسنوضح هذه الصور كما وردت في قانون الجرائم الإلكترونية الأردني، وقوانين الجرائم الإلكترونية في دول مجلس التعاون لدول الخليج العربية، كما يلي:

أولًا: صور الركن المادي في جرائم الخطر الذي يهدد سلامة المعلومات المصرفية في القانون الأردني

من التدقيق في المادتين (7) و(3/ ب) من قانون الجرائم الإلكترونية الأردني (اللتين كتبنا نصَّيهما فيما سبق)، يتَّضِحُ أنَّ ثمّةَ صُوَرًا كثيرةً من جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات المصرفية بهدف يُهدِّدُ سلامتها، وهذه الجرائم تتعدَّدُ وتتنوَّعُ تبعًا للسلوك الماديِّ المكوِّنِ لها، وكما أسلفنا القول، فإنَّ جميع هذه الجرائم ذات سلوك مُجرَّد، ومن هنا سنذكُر أسماء هذه الجرائم من خلال توضيح الركن المادي المكون لكلٍّ منها، كالآتي:

1- الركن المادي في جريمة الدخول إلى نظام المعلومات المصرفي بهدف يهدد سلامة المعلومات المصرفية بالإلغاء أو الحذف

يُقصَدُ بالإلغاءِ المكوِّنِ للسلوكِ الماديِّ في هذه الجريمة، الإزالةَ، سواءٌ أكانت كُليَّةً أم جزئية. وعلى الرغم من أن معنى الحذف لا يختلف عن الإلغاء، فكلاهما يعني الإزالة، غير أنَّ المُشرِّع الأردني استخدمهما بوصفِهما مُصطَلَحَيْنِ مختلفين، ويبدو أنَّ الحذفَ يُعَدُّ مُصطلحًا فنيًا أكثرَ من الإلغاء[23].

يُسْتَفَاد من صياغة المادة (3/ ب) من قانون الجرائم الإلكترونية، بعد الإحالة إليها بموجب المادة (7) من القانون ذاته، أن الركن المادي المُكوِّن لهذه الجريمة يقوم بمُجرَّد الدخول غير المشروع إلى النظام المعلوماتي المصرفي، بهدف إلغاء المعلومات التي يحتويها هذا النظام أو حذفها، وبعبارةٍ أخرى، فإن هذا الركن يُعد متوافرًا بمُجرَّد دخول الجاني إلى النظام، حتى لو لم يتم إلغاء المعلومات أو حذفها، ولكن يشترط لتحقق هذا الركن إثبات هدف الجاني، وهو إلغاء المعلومات أو حذفها؛ وذلك لأن هذه الجريمة – كما أسلفنا القول – من جرائم السلوك المُجرَّد (جرائم الخطر أو الجرائم الشكلية)، ومن ثَمَّ فإنَّ هذه الجريمة تُعَدُّ تامةً بمُجرَّد الدخول بهدف الإلغاء أو الحذف، ويُعاقَب مُرتكبها بعقوبة الجريمة التامة، وهو بذلك يتساوى في استحقاق العقوبة مع من ارتكب جريمة الدخول قصدًا، وألغى بعد ذلك المعلومات أو حذفها، كنتيجةٍ تحققت بعد دخوله إلى النظام.

2- الركن المادي في جريمة الدخول إلى نظام المعلومات المصرفي بهدف يهدد سلامة المعلومات المصرفية بالتغيير أو الإتلاف أو التدمير

جاء في المادة (3/ ب) من قانون الجرائم الإلكترونية الأردني ثلاث كلمات، هي: «إضافة»، و«تعديل»، و«تغيير»، وقد ذُكِرَت هذه الكلمات بوصفِها أهدافًا يسعى الجاني إلى تحقيقها بعد دخوله إلى النظام المعلوماتي، ويُقصَدُ بالإضافة الزيادةُ، أيًّا كان نوعُها أو شكلُها، ويُقصَدُ بتعديل المعلومات تغييرُها، ونحن نرى أنَّ كَلِمَتَيْ الإضافة والتعديل، كُتِبَتا من قبيلِ التكرار والتزيد؛ لأنَّهُ يُمكِنُ الاستعاضة عنهما بكلمة واحدةٍ هي كلمة «تغيير»؛ لأنَّ هذه الكلمةَ تستوعِبُهُما.

ويُقصَدُ بـ «الإتلاف» إنهاءُ صلاحية الشيء لِمَا أُعدَّ له، وجعلُهُ غيرَ قابل للإصلاح، وبناءً على ذلك يعني إتلاف المعلومات الإلكترونيةَ جعلَها غيرَ صالحَةٍ وفُقدانَها لمنفعتِها، في حينِ يُقصَدُ بتدمير المعلومات: تَضَرُّرُها وخرابُها بشكلٍ شامل[24].

(23) عبدالإله النوايسة، جرائم تكنولوجيا المعلومات، مرجع سابق، ص255.

(24) https://www.almaany.com/ar/dict/ar.

وتجنبًا للتكرار، فإنَّ ما قلنا فيما سبق بشأن الركن المادي في جريمة الدخول إلى النظام المعلوماتي، بهدف إلغاء المعلومات أو حذفها، ينطبقُ تمامًا على الركن المادي في جريمة الدخول إلى النظام المعلوماتي؛ بهدف تغيير المعلومات أو إتلافها أو تدميرها.

ومن المفيد التنبيهُ هنا إلى أنَّ الدخول غير المشروع إلى النظام المعلوماتي، وتغيير ما يحتويه من معلومات على نحو يخالف الحقيقة، لا يُشكل جريمة تزوير وفقًا لنصوص قانون العقوبات الأردني، وإنما يُشكل جُنحة الدخول غير المشروع، وتعديل معلومات إلكترونية، المنصوص والمعاقَب عليها في المادة (3/ ب) من قانون الجرائم الإلكترونية الأردني، وهذا ما أكدته محكمة التمييز الأردنية في أحد أحكامها[25].

3- الركن المادي في جريمة الدخول إلى نظام المعلومات المصرفي بهدف يهدد سلامة المعلومات المصرفية بالنسخ أو النقل أو الإفشاء

يمكن أن يكون نسخُ المعلومات – جزئيًا أو كُليًا – من غيرِ تصريح من مالكه، ويشمل ذلك القيام بتخزين ما يحتويه النظام على أداة معيَّنة من دون تركً أثر، فلا يحذف أو يضيف، ولكن يتم أخذ نسخة أو أكثر من المعلومات التي يحتويها النظام المعلوماتي[26]. وبمعنى آخر، يكون النسخ، في حال الحصول على المعلومات ونقلها من غيرِ أن يؤدي ذلك إلى فقدان الأصل المنسوخ منه[27]. ويُقصَدُ بنقل المعلومات الحصول على أصل المعلومات المُخَزَّنة على النظام المعلوماتي، ونقلها من نظام إلى آخر، أو من وسيلة حفظ معلومات إلى أخرى.

وقد يترتب على نقل المعلومات إتلاف النظام المعلوماتي، أو انتهاك للخصوصية بشكلٍ عام، ويتخذ الإفشاء صوة اختراق النظام، والحصول على المعلومات من خارج المختصين بمعالجتها، وقد يتخذ الإفشاء صورة نقل المعلومات من قبل المسيطر عليها بمناسبة معالجتها أو حفظها أو نقلها إلى شخص آخر، أو إلى جهة غير مختصة بتلقي هذه المعلومات[28]، وتجنبًا للتكرار والحشو، فإنَّ ما قِيل – فيما سبق – بشأن الركن المادي في جريمة الدخول إلى النظام المعلوماتي بهدف إلغاء المعلومات أو حذفها، ينطبِقُ تمامًا على الركن المادي في جريمة الدخول إلى نظام المعلومات المصرفي؛ بهدَفِ نسخِ المعلومات أو نقلِها أو إفشائِها.

(25) حكم محكمة التمييز الأردنية بصفتها الجزائية، رقم (192) لسنة2021، موقع قرارك.

(26) حسن المناصير، جريمة الدخول عير المشروع إلى النظام المعلوماتي والتعدي على محتوياته، رسالة ماجستير، جامعة جرش، الأردن، 2016، ص56.

(27) عبدالإله النوايسة، جرائم تكنولوجيا المعلومات، مرجع سابق، ص256.

(28) حسن المناصير، مرجع سابق، ص52.

4- الركن المادي في جريمة الدخول إلى نظام المعلومات المصرفي بهدف تعطيله أو توقيفه عن العمل أو حجب خدمته

يقوم هذا الركن بمنع الجاني المستخدمين من الدخول إلى النظام المعلوماتي الخاص بالشركات التي تقدم خِدْمات مصرفية، وذلك من خلال العبث بمعلوماته، أو تشويهها، أو بالعبث ببرامج النظام، بحيث يُصبِحُ عملُهُ غيرَ ممكن، ويكون التعطيل أو التوقيف كليًا عند مَحْوِ كل المعلومات، أو البرامج، أو الجزء المسؤول عن دخول الأشخاص المُصرَّح لهم بالدخول إلى النظام[29]، ويمكن القولُ – بعبارةٍ أدقَّ – بأنه يُقصَدُ بالتوقيف الإعاقةُ المؤقتة عن العمل، ويُقصَدُ بالتعطيل التخريبُ أيًا كان شكلُهُ ونوعُه[30].

وبشأن حجب الخدمة التي يقدمها النظام المعلوماتي، فإنَّ الأصل هو استمرار توافر الخِدْمات أو المعلومات بعناصرها الثلاثة: المعلومات، ونظم الحوسبة المستخدمة لتجهيز هذه المعلومات، والضوابط الأمنية المُستَخدَمة لحماية هذه المعلومات؛ إذ إنَّ غياب أيٍّ من هذه العوامل الثلاثة يعني أنَّ هناك حجبًا للخدمة، ومنعًا من الاستفادة منها، فعبارة إنَّ الوصول إلى هذا النظام أو الموقع الإلكتروني غير ممكن، قد تعني أنَّ النظام أو الموقع الإلكتروني الذي تحاول أن تزوره قد تعرَّض لهجمات حجب الخدمة، وقد يؤدِّي ذلك إلى تشوُّهِ بعض المعلومات التي يحتويها النظام المعلوماتي[31].

وتجنبًا للتكرار والحشو، فإنَّ ما قِيل فيما سبق، بشأن الركن المادي في جريمة الدخول إلى نظام المعلومات المصرفي بهدف إلغاء المعلومات أو حذفها، ينطبق تمامًا على الركن المادي في جريمة الدخول إلى نظام المعلومات المصرفي؛ بهَدَفِ تعطيلِهِ أو توقيفِهِ عن العمل أو حجبِ خدمتِه.

ثانيًا: الركن المادي في جرائم الخطر الذي يهدد سلامة المعلومات المصرفية الإلكترونية في قوانين دول مجلس التعاون لدول الخليج العربية

كما أسلفنا القول، لقد أُقرت جميع قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، بنصوصٍ صريحة، الحماية الجنائية للمعلومات المصرفية من خطر محاولة الحصول عليها بصورة غير مشروعة (باستثناء القانون البحريني والقانون القطري؛ لأن القانون الأخير صنَّف جريمة الحصول على المعلومات المصرفية بصورة غير مشروعة من الجرائم ذات النتيجة).

(29) حسن المناصير، مرجع السابق، ص57.
(30) عبدالإله النوايسة، جرائم تكنولوجيا المعلومات، مرجع سابق، ص256.
(31) حسن المناصير، مرجع سابق، ص76.

نصت المادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي على أنه: «يُعاقَب... كل من دخل بدون تصريح إلى... نظام معلومات إلكتروني... سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية... إلخ». كما نصت المادة (3/ 1) من قانون مكافحة جرائم تقنية المعلومات الكويتي على أنه: «يُعاقَب... كل من ارتكب دخولًا غير مشروع إلى موقع أو نظام معلوماتي... بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون... ويسري هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية».

ونصت المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني على أنه: «يُعاقَب... كل من دخل عمدًا... نظامًا معلوماتيًا بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية... وتُعدُّ البيانات والمعلومات الإلكترونية السرية الخاصة بالمصارف والمؤسسات المالية في حكم البيانات والمعلومات الإلكترونية الحكومية السرية في نطاق تطبيق حكم هذه المادة».

وأخيرًا، نصت المادة (4/ 2) من نظام مكافحة جرائم المعلوماتية السعودي على أنه: «يُعاقَب... كل شخص يرتكب أيًّا من الجرائم المعلوماتية: للوصول 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».

يُسْتَفَاد من صيغ نصوص مواد قوانين دول مجلس التعاون لدول الخليج العربية السالفة الذكر (القانون الإماراتي والكويتي والعُماني والسعودي) أن الركن المادي المُكوِّن للجريمة التي تشكل خطرًا يُهدد سلامة المعلومات المصرفية الإلكترونية، يقوم بمُجرَّد الدخول غير المشروع إلى نظام المعلومات المصرفي، بهدف الحصول على المعلومات المصرفية المُخَزَّنة في هذا النظام. وبعبارةٍ أخرى، فإن هذا الركن يُعد متوافرًا بمُجرَّد دخول الجاني إلى النظام، حتى لو لم يتمّ الحصول على المعلومات المصرفية، ولكن يُشترط لتحقق هذا الركن إثبات هدف الجاني، وهو الحصول على المعلومات المصرفية؛ وذلك لأن هذه الجريمة من جرائم السلوك المُجرَّد، ومن ثَمَّ فإنَّ هذه الجريمة تُعَدُّ تامةً، بمُجرَّد الدخول بهدف الحصول على المعلومات المصرفية.

وينبغي التنبيه هنا إلى أنه إذا نجم عن الدخول إلى نظام المعلومات المصرفي، بقصد الحصول على المعلومات المصرفية، نتيجةٌ معيَّنة كإلغاء المعلومات المصرفية، أو إتلافها، أو تدميرها، أو نشرها، أو تعديلها، فإن ذلك يعتبر من قبيل الظروف المشددة للعقوبة في القانون الإماراتي والكويتي والعُماني.

ويخلص الباحثان، مما تقدم، إلى أن القانون الإماراتي والكويتي والعُماني ميَّز في العقاب بين مُجرَّد الدخول إلى نظام المعلومات بقصد الحصول على المعلومات المصرفية، وبين الدخول الذي تنجم عنه نتيجة معيَّنة، مثل: إلغاء المعلومات أو حذفها، فهذه القوانين شددت العقوبة في الحال الأخيرة؛ وذلك لأن الجريمة فيها تكون أكثر جَسَامةً؛ بسبب تحقق نتيجتها، وذلك بخلاف القانون الأردني الذي لم يميِّزْ في العقاب بين الدخول الذي يهدف إلى إلغاء المعلومات المصرفية أو حذفها، وبين الدخول الذي تنجم عنه نتيجة معيَّنة، مثل: إلغاء المعلومات المصرفية أو حذفها.

الفرع الثالث

الركن المعنوي في جرائم الخطر

الذي يهدد سلامة المعلومات المصرفية

جرَّمت المادة (7) من قانون الجرائم الإلكترونية الأردني، وبالإحالة إلى المادة (3/ ب) من القانون ذاته، الدخولَ غير المشروع إلى نظام المعلومات المصرفي؛ بهدَف يُهدِّدُ سلامة المعلومات التي يحتويها هذا النظام، وقد جاءت الفقرة (ب) من المادة (3) السالف ذِكْرُها، معطوفةً على الفقرة (أ) من المادة ذاته، وقد تطلبت الفقرة (أ) القصد الجُرميَّ صراحةً لقيام جريمة الدخول إلى النظام المعلوماتي، فقالت: «يُعاقَبُ كلُّ من دخل قصدًا إلى... نظام معلومات»، وقد جاءت الفقرة (ب) التي تليها بهذه الصيغة: «إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو... إلخ».

يتضح من ذلك أنَّ المُشرِّع الأردني جعل جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات المصرفية؛ بهدَف يُهدِّدُ سلامتها من الجرائم القصدية، وبناءً على ذلك يُشترط لقيام هذه الجرائم توافُرُ القصد الجنائي، بعُنصُرَيهِ العِلمِ والإرادة، وهو ما سنوضحه فيما يأتي:

أولًا: عنصر العلم

من المُسلَّم به أنَّ العلم بالقانون أمرٌ مُفتَرَض، وليس لأيِّ شخص الادعاء بالجهل في القانون، سواءٌ من حيث وجود النص، أو من عدمه، أو من حيث تفسير وفهم أحكام نصوص القانون، وهذا يُسْتَفَاد من نص المادة (85) من قانون العقوبات الأردني. ولا شك في أن قاعدة «لا يُعتَبَرُ الجهل بأحكام القانون عذرًا»، جاءت حَلًّا للتنازع بين الضرورات المنطقية والضرورات العملية، فلو قُبِلَ من شخص الجهلُ بالقانون، واعتُدَّ بهذا الجهل؛

لأصبحَ تطبيقُ القواعد القانونية متعذِّرًا، ولأصبحَ قانونُ العقوبات عديمَ الفائدة[32]. ولكي يتوافر عنصر العلم؛ يتعيَّنُ أن يكونَ الجاني محيطًا بحقيقة الواقعة الإجرامية، وهي العلم بالدخول إلى النظام المعلوماتي (محل الجريمة)، وأنَّ هذا الدخول تم بصورةٍ غير مشروعة؛ لأنه من دون العلم لا يمكن أن تقوم الإرادة، فالإرادة الجُرمية تقوم على أساس العلم بالواقعة الإجرامية والعلم بالقانون.

والسؤال الذي يُطرَحُ هُنا، ماذا لو دخل شخصٌ قصدًا، وبصورة غير مشروعة، إلى نظام معلومات مصرفي خاص بإحدى الشركات التي تقدم خِدْمات مصرفية، وكان يعتقِدُ بأنه دخل إلى نظام معلوماتي لا يتبع لهذه الشركة، فهل سينتفي لديه القصد الجنائي عن جناية الاعتداء على المعلومات التي تحتويها نظم المعلومات الخاصة بالشركات التي تقدم خِدْمات مصرفية؟

في هذه الحال، وفي تقديرِ الباحثين، فإنَّهُ لا قيامَ لجناية الاعتداء على المعلومات التي تحتويها نظم المعلومات الخاصة بالشركات التي تقدم خِدْمات مصرفية، المنصوص والمعاقَب عليها في المادة (7) من قانون الجرائم الإلكترونية الأردني، وبالإحالة إلى المادة (3/ ب) من القانون ذاته؛ وذلك لانتفاء عنصر العلم بأحد الأركان الخاصة لقيام هذه الجناية، وهو ركن المحل (الركن المُفتَرَض الذي يتمثل بنظام المعلومات الخاص بإحدى الشركات التي تقدم خِدْمات مصرفية)، وسندُنا في ذلك نص المادة (86/ 1) من قانونِ العقوبات الأردني التي اشترطت لمعاقبة من يرتكب فعلًا في جريمة قصدية علمَهُ بكلِّ أركانها وعناصرِها، وذلك بقولها: «لا يُعاقَبُ كفاعلٍ أو محرِّضٍ أو متدخِّلٍ كلُّ من أقدم على الفعلِ في جريمةٍ مقصودة بعامل غلطٍ ماديٍّ واقعٍ على أحد العناصر المكوِّنة للجريمة».

ولكنَّ هذا لا يعني انتفاءَ المسؤولية الجنائية للجاني بشكلٍ مطلق في هذه الحال، فهو يُسأَلُ عن جُنحة الاعتداء على المعلومات التي يحتويها أي نظام معلوماتي بشكلٍ عام، عملًا بنص المادة (3/ ب) من قانون الجرائم الإلكترونية الأردني.

ثانيًا: عنصر الإرادة

تنصَبُّ الإرادة في القصد الجنائي على السلوك الإجرامي والنتيجة المعاقَب عليها على حدٍّ سواء؛ ففي جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات الخاصة بالشركات التي تقدم خِدْمات مصرفية، يجب أن يَثبت أن الجاني أراد الدخول غير

(32) بهذا المعنى يُنظَر: زياد العنزي وعبدالله احجيله، الجوانب القانونية لمسؤولية مدير المجموعة في مواقع التواصل الاجتماعي في القانون الاتحادي الإماراتي، مجلة الحقوق، جامعة البحرين، مج16، العدد1، سنة 2019، ص251.

المشروع إلى نظام المعلومات الخاص بالشركات السالف ذكْرُها؛ بهدَف يُهدِّدُ سلامة المعلومات التي يحتويها هذا النظام، كما يجب أن تثبت الإرادة الحرة لدى الجاني، فإذا كان الدخول في النظام ثمرةَ إكراه ماديٍّ تعرَّضَ له مثلًا من دخل إلى النظام المعلوماتي، وعلى نحو مَحا إرادته وجعل منه أداةً لارتكاب الجريمة، ففي هذه الحال ينتفي القصد الجنائي بالنسبة إلى من وقع عليه الإكراه، ويُسألُ عن الجريمة مَن أكرهَهُ على ارتكابها[33]، وننبه هنا إلى أن مثل هذا الإكراه يُعدم النشاط الجرمي ابتداءً، ومن ثم فهو يمحو الإرادة.

والسؤال الذي يُطرَحُ، في هذا السياق، ماذا لو أراد الجاني الدخول بصورة غير مشروعة إلى نظام معلومات خاص بإحدى الشركات التي تقدم خِدْمات مصرفية بهدف يُهدِّدُ سلامة المعلومات التي يحتويها هذا النظام، ولكنه دخل بالخطأ إلى نظام معلوماتي آخر ليست له علاقة بالشركات السالفة الذكر، كنظام المعلومات الخاص بإحدى الجامعات مثلًا.

فهل يُسألُ الجاني، في هذه الحال، عن جناية الدخول بصورة غير مشروعة إلى نظام المعلومات الخاص بإحدى الشركات التي تقدم خِدْمات مصرفية المنصوص والمعاقَب عليها في المادة (7) من قانون الجرائم الإلكترونية الأردني، ومع الإحالة إلى المادة (3/ ب) من القانون ذاته؟ أم يُسألُ الجاني هنا عن جُنحة الدخول بصورة غير مشروعة إلى أيِّ نظام معلوماتي المنصوص والمعاقَب عليها في المادة (3/ ب) السالفِ ذِكْرُها؟

في هذه الفرضية يُعَدُّ غلطُ الجاني من قبيل «الغلط في موضوع النتيجة، وهو ذات الغلط في الهدف أو الحيدة عنه»؛ لأنَّ سلوك الجاني هنا انحرف إلى نتيجة لا يريدها (وهي الدخول إلى نظام معلوماتي ليس هو الهدف المقصود)، وفي تقدير الباحثين أنه ما دامت النتيجة التي تحققت على أرض الواقع بسبب انحراف سلوك الجاني مساوية في قيمتها القانونية للنتيجة التي أرادها (وهي الدخول إلى نظام المعلومات المصرفي)، فإنَّ عنصر الإرادة يُعَدُّ متوافرًا لقيام جناية الدخول إلى نظام المعلومات الخاص بالشركات التي تقدم خِدْمات مصرفية، بهدَفٍ يُهدِّدُ سلامة المعلومات التي يحتويها هذا النظام.

والوضع في هذه الفرضيّة أقربُ ما يكون إلى الوضع في جريمة السرقة التقليدية، وذلك حينما يريد الجاني سرقة موبايل مُحدَّد بذاته، ومملوك لشخص مُحدَّد، وبعد أن نفّذ الجاني سرقته، اتَّضَحَ له أنّ الموبايل المسروق ليس هو المُرادُ سرقتهَ، واتَّضَحَ له أيضًا أنَّ الموبايل الذي سرقه ليس مملوكًا للشخص الذي أراد سرقته منه.

(33) بهذا المعنى يُنظَر: نظام المجالي، شرح قانون العقوبات، القسم العام، ط1، دار الثقافة، عمَّان، الأردن، 2009، ص342. محمد السعيد عبدالفتاح، الوجيز في شرح قانون العقوبات الاتحادي الإماراتي، القسم العام، الآفاق المشرقة، عمَّان، الأردن، 2014هـ، ص148.

ففرضية هذه السرقة، تُعَدُّ من قبيل الغلط في الهدف، وهو لا ينفي القصد الجنائي المطلوب لقيام جريمة السرقة، لاسيَّما أن القيمة القانونية للنتيجة التي تحققت على أرض الواقع بسبب انحراف سلوك الجاني مساوية في قيمتها القانونية للنتيجة التي أرادها الجاني ولم تتحقق.

وبعد أن أوضحنا القصد الجنائي العام المطلوب لقيام جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات الخاصة بالشركات التي تقدم خِدْمات مصرفية، آن الأوانُ لبيان مدى لزوم توافر القصد الجنائي الخاص لقيام هذه الجرائم، وبيان الأثر القانوني الذي يترتب على وجود هذا القصد أو انتفائه.

ومن خلالِ مطالعة نص المادة (3/ ب) من قانون الجرائم الإلكترونية الأردني، وبعد الإحالة إليها بموجب المادة (7) من القانون ذاته، يتضح أنه يشترط لتوافر القصد الجنائي في جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات الخاصة بالشركات التي تقدم خِدْمات مصرفية وجود قصد جنائي خاص، يتمثل بالهدف الذي يسعى الجاني لتحقيقه بعد الدخول غير المشروع إلى نظام المعلومات المصرفي، وهذا الهدف يتعدد ويتنوع، وقد تطلبه المُشرِّع الأردني صراحةً في المادة (3/ ب) من قانون الجرائم الإلكترونية، وقد يكون هذا الهدف – على سبيل المثال – هو حذف المعلومات، أو نقلها، أو نسخها، أو إتلافها... إلخ. ووفقًا لاختلاف هذا الهدف، يختلف السلوك المادي المكوِّن لكل جريمة من جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات المصرفية.

وعليه، فإنه يُشترط توافر القصد الخاص بجانب القصد العام لقيام جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات المصرفية، وفي حال انتفاء القصد الخاص، أو تعذر إثباته بكل طرائق الإثبات، فإن هذه الجرائم تنتفي وفقًا لذلك، ولكنَّ هذا لا يعني أن الجاني في هذه الحال لا يُسألُ جنائيًا، وإنما يُسألُ عن جناية الدخول (المُجرَّد من الهدف) إلى نظام المعلومات المصرفي، إذا توافرت جميع أركانها، مثلما تطلبتها المادة (7) من قانون الجرائم الإلكترونية، مع الإحالة إلى المادة (3/ أ) من القانون ذاته.

وبالرجوع إلى قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية، يتضح أن بعض هذه القوانين اشترط صراحةً – لقيام جريمة الدخول غير المشروع إلى النظام المعلوماتي المصرفي بقصد الحصول على المعلومات المصرفية – توافر القصد، وهذه القوانين هي: القانون الكويتي والعُماني والسعودي[34].

(34) ينظر: المادتان (1) و(3) من قانون مكافحة جرائم تقنية المعلومات الكويتي، والمادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني، وتُنظر: الفقرة (7) من المادة الأولى، والفقرة (2) من المادة الرابعة من نظام مكافحة جرائم المعلوماتية السعودي.

وبالرجوع إلى أحكام القانون الإماراتي نجده لم يشترط «القصد» لقيام جريمة الدخول غير المشروع إلى النظام المعلوماتي المصرفي، بقصد الحصول على المعلومات المصرفية، وبالتالي وكما أسلفنا القول، من المُتَصَوَّر ارتكاب هذه الجريمة بالقصد أو الخطأ، وذلك لأنه يُسْتَفَاد من المادة (43) من قانون العقوبات الإماراتي بأنه حينما يسكُت المشرِّع عن بيان صورة الركن المعنوي في جريمة معيَّنة، فهذا يعني أن الجاني يسأل عن هذه الجريمة، سواء ارتكبها قصدًا أم خطأ.

ويخلص الباحثان، مما تقدم، إلى أنه يُشترط لقيام جريمة الدخول غير المشروع إلى النظام المعلوماتي المصرفي بقصد الحصول على المعلومات المصرفية توافر القصد، وفقًا لأحكام القانون الأردني، والقانون الكويتي، والعُماني، والسعودي، ويُسْتَفَاد من أحكام القانون الإماراتي أن الجاني يُسأَل عن هذه الجريمة، سواء ارتكبها قصدًا أم خطأ.

الفرع الرابع

عقوبة جرائم الخطر الذي يهدد سلامة المعلومات المصرفية الإلكترونية

نعرض لذلك في قانون الجرائم الإلكترونية الأردني أولًا، ثم القانون الإماراتي والكويتي والعُماني والسعودي ثانيًا، وذلك على النحو التالي:

أولًا: العقوبة في قانون الجرائم الإلكترونية الأردني

يُعاقَب من يرتكب أيًا من جرائم الاعتداء على المعلومات التي يحتويها نظام المعلومات المصرفي بهدف يُهدد سلامة هذه المعلومات بحذفها أو تغييرها... إلخ، فهو يُعاقَب بالعقوبة الجنائية المنصوص عليها في المادة (7) من قانون الجرائم الإلكترونية الأردني، وهي الأشغال مُدَّةً لا تقلُّ عن خمس سنوات، ولا تزيد على عشرين سنة، وبغرامة لا تقِلُّ عن (5000) خمسة آلاف دينار، ولا تزيد على (15000) خمسة عشر الف دينار، ومن المُلاحظ أن هذه العقوبة الجنائية المقررة لجنايات الاعتداء على المعلومات التي يحتويها نظام المعلومات المصرفي هي ذاتها العقوبة التي أُقرت لجناية الدخول المُجرَّد غير المشروع، بموجب المادة (7) من قانون الجرائم الإلكترونية، مع الإحالة إلى المادة (3/ أ) من القانون ذاته.

ثانيًا: العقوبة في القانون الإماراتي والكويتي والعُماني والسعودي

1- العقوبة في قانون مكافحة جرائم تقنية المعلومات الإماراتي

عاقبت المادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي على جريمة الدخول غير المشروع إلى نظام المعلومات المصرفي، بقصد الحصول على المعلومات المصرفية الإلكترونية، بالسجن المؤقت، والغرامة التي لا تقل عن مائتين وخمسين ألف درهم، ولا تتجاوز مليونا وخمسمائة ألف درهم، وتكون العقوبة هي السجنَ مدة لا تقل عن خمس 5 سنوات، والغرامة التي لا تقل عن خمسمائة ألف درهم، ولا تجاوز مليونين درهم، إذا تعرضت المعلومات المصرفية للإلغاء، أو الحذف، أو الإتلاف، أو التدمير، أو الإفشاء، أو التغيير، أو النسخ، أو النشر، أو إعادة النشر.

وبناءً على ذلك فالعقوبة السالبة للحرية المقررة لهذه الجريمة في القانون الإماراتي هي عقوبة جنائية، وتتمثل في السجن المؤقت الذي تتراوح مدته بين ثلاث سنوات وخمس عشرة سنة، وذلك عملاً بالمادة (68) من قانون العقوبات الإماراتي التي حددت الحد الأدنى لمدة السجن المؤقت بثلاث سنوات، وحدها الأعلى خمس عشرة سنة.

2- العقوبة في قانون مكافحة جرائم تقنية المعلومات الكويتي

عاقبت المادة (1/3) من قانون مكافحة جرائم تقنية المعلومات الكويتي على هذه الجريمة بالحبس مدة لا تجاوز ثلاث سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار، ولا تجاوز عشرة آلاف دينار، أو بإحدى هاتين العقوبتين، وإذا ترتب على هذه الجريمة إلغاء المعلومات المصرفية، 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.

وبناءً على ذلك فالعقوبة السالبة للحرية المقررة لهذه الجريمة في القانون الكويتي هي عقوبة جنحية، وتتمثل في الحبس مدة لا تجاوز ثلاث سنوات، وذلك عملاً بالمادة (5) من قانون الجزاء الكويتي رقم 16 لسنة 1960 التي يُسْتَفَاد منها أن عقوبة الجنح هي الحبس الذي تتراوح مدته بين (24 ساعة) ولغاية ثلاث سنوات.

3- العقوبة في قانون مكافحة جرائم تقنية المعلومات العُماني

عاقبت المادة (6) من قانون مكافحة جرائم تقنية المعلومات العُماني على هذه الجريمة 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، وتكون

العقوبة السجنَ مدةً 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 المُجرَّم إلغاءٌ، أو تغييرٌ، أو تعديلٌ، أو تشويهٌ، أو إتلافٌ، أو نسخٌ، أو تدميرٌ، أو نشرُ البيانات، أو المعلوماتُ المصرفية الإلكترونية.

وبناءً على ذلك، فالعقوبة السالبة للحرية المقرَّرة لهذه الجريمة في القانون العُماني هي عقوبة جنحية، وتتمثل في السجن الذي لا تقل مدته عن سنة، ولا تزيد على ثلاث سنوات، وذلك عملًا بالمادة (39) من قانون الجزاء العُماني رقم 7 لسنة 1974 التي حددت عقوبة الجنح بالسجن الذي مدته من عشرة أيام إلى ثلاث سنوات.

4- العقوبة في نظام مكافحة جرائم المعلوماتية السعودي

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

يخلص الباحثان، من مقارنة العقوبات المقررة للجرائم ذات السلوك المُجرَّد، والتي تشكل خطرًا يهدد سلامة المعلومات المصرفية الإلكترونية في ضوء أحكام القانون الأردني والإماراتي والكويتي والعُماني والسعودي، إلى أن أشد هذه العقوبات هي العقوبة الجنائية المنصوص عليها في المادة (7) من قانون الجرائم الإلكترونية الأردني، وهي الأشغال المؤقتة من خمس إلى عشرين سنة. ثم تليها – من حيث الشدة – العقوبة الجنائية المنصوص عليها في المادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، وهي عقوبة السجن المؤقت الذي تتراوح مدته بين ثلاث وخمس عشرة سنة. ثم تليها العقوبة المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات العُماني، وهي عقوبة السجن الذي تتراوح مدته بين سنة وثلاث سنوات. ثم تليها العقوبتان المنصوص عليهما في القانون الكويتي والنظام السعودي، وهما عقوبتا الحبس الذي تتراوح مدته بين أربع وعشرين ساعة وثلاث سنوات.

وينبغي التنبيه هنا إلى أنه إذا نجم عن الدخول إلى نظام المعلومات المصرفي، بقصد الحصول على المعلومات المصرفية، نتيجةٌ معيَّنةٌ، مثل: إلغاء المعلومات المصرفية، أو إتلافها، أو تدميرها، أو نشرها، أو تعديلها، فإن ذلك يعتبر من قبيل الظرف المشدد للعقوبة في كلٍّ من القانون الإماراتي، والكويتي، والعُماني.

ويرى الباحثان أن العقوبات الجنحية المقررة لجريمة الدخول غير المشروع إلى نظام المعلومات المصرفي، بقصد الحصول على المعلومات المصرفية الإلكترونية، والمنصوص

عليها في كلٍّ من القانون العُماني، والكويتي، والسعودي، لا تتناسب مع خطورة هذه الجريمة، وبالتالي يتمنى الباحثان من كل من المشرِّع العُماني، والكويتي، والسعودي تشديد عقوبة هذه الجريمة لتصبح عقوبة جنائية، وذلك لبسط مزيد من الحماية الجنائية للمعلومات المصرفية المُخَزَّنة في نظم المعلومات المصرفية؛ وذلك لأهمية هذه المعلومات من الناحية الاقتصادية، فضلًا على أنَّ نظم المعلومات المصرفية تتمتع بوسائل حماية وإجراءات أمنية مشددة، والجاني الذي يقتحِمُ هذه الوسائل، ويستولي على المعلومات المصرفية، يُعَدُّ خَطِرًا وجديرًا بعقوبة الجناية.

المطلب الثاني

الحماية الجنائية للمعلومات المصرفية الإلكترونية من برنامج يُشكل خطرًا يهدد سلامتها

ينبغي التنبيه، ابتداءً، على أن قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية خلت من نصوص تُجرّم وتعاقب على أفعال الاعتداء على المعلومات المصرفية الإلكترونية، من خلال برنامج إلكتروني يُشكل خطرًا يهدد سلامة المعلومات المصرفية الإلكترونية، وبمعنى آخر، فلا توجد في قوانين دول مجلس التعاون لدول الخليج العربية حماية جنائية للمعلومات المصرفية الإلكترونية من خطر برنامج إلكتروني يهدد سلامة هذه المعلومات، وبناءً على ذلك ستقتصر دراستنا في هذا المطلب على أحكام القانون الأردني فقط.

من مطالعة المادة (7) من قانون الجرائم الإلكترونية الأردني، نجدها جرّمت أفعالًا تشكل خطرًا على المعلومات المصرفية الإلكترونية باستخدام برنامج، وعاقبت على هذه الأفعال بعقوبةٍ جنائية، وتنحصر هذه الأفعال في المادة (4) من قانون الجرائم الإلكترونية، وذلك بعد الإحالة إليها بموجب المادة (7) السالف ذِكْرُها، وقد جاء نصُّ المادة (4) على هذا النحو: «يُعاقَب كل من أدخل، أو نشر، أو استخدم قصدًا برنامجًا عن طريق الشبكة المعلوماتية، أو باستخدام نظام معلومات لإلغاء، أو حذف، أو إضافة، أو تدمير، أو إفشاء، أو إتلاف، أو حجب، أو تعديل، أو تغيير، أو نقل، أو نسخ، أو التقاط، أو تمكين الآخرين من الاطلاع على بيانات أو معلومات، أو إعاقة، أو تشويش، أو إيقاف، أو تعطيل عمل نظام معلومات، أو الوصول إليه... إلخ».

لذلك، فإنَّ الجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج، وعقوباتها تنحصر في المادتين (4) و(7) من قانون الجرائم الإلكترونية الأردني، ويُلاحظ على هذه الجرائم أنها من جرائم السلوك المُجرَّد، وعليه سنوضح هذه الجرائم وأركانها وعقوباتها في الفروع الآتية، مع التنبيه إلى أننا سنذكُر أسماء هذه الجرائم، من خلال توضيح الركن المادي المكوِّن لكل منها؛ وذلك كما يلي:

الفرع الأول

الركن المُفتَرَض في الجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج

يتمثل الركن المُفتَرَض في هذه الجرائم في «المعلومات التي تحتويها نظم المعلومات الخاصة بالشركات التي تقدم خِدْمات مصرفية»، وإذا كان النظام المعلوماتي المعتدى على معلوماته باستخدام البرنامج ليست له صلة بالشركات التي تقدم خِدْمات مصرفية، فلا تطبيق للمادة (7) السالف ذِكْرُها، وفي هذه الحال يُصارُ إلى تطبيق عقوبة الحبس المنصوص عليها في المادة (4) من قانون الجرائم الإلكترونية، وهي العقوبة المقرَّرة أصلًا للجرائم التي ترتكب باستخدام برنامج للاعتداء على المعلومات التي يحتويها أي نظام معلوماتي بشكلٍ عام.

الفرع الثاني

الركن المادي في جرائم الخطر التي تهدد سلامة المعلومات المصرفية باستخدام برنامج

تختلف الوسائل التي يمكن اللجوء إليها للاعتداء على المعلومات التي يحتويها أي نظام معلوماتي، إذ تتطلَّبُ جميعُها قدرًا من المعرفة بالتكنولوجيا الحديثة[35]، فلا يكفي مُجرَّد الدخول غير المشروع بالنسبة إلى المعتدي، بل قد يستخدم، أو يُدخل أو ينشر برنامجًا مُعيَّنًا عن طريق نظام معلومات مُعيّن للاعتداء على المعلومات التي يحتويها نظام معلوماتي آخر، وبناءً على ذلك سنوضح الركن المادي المُكوِّن للجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج كما يلي:

(35) أسامه العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي، مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، الرياض، ع14، السنة 2012، ص11.

أولًا: تعريف البرنامج الذي يُشكل خطرًا على المعلومات المصرفية

عرَّفت المادة الثانية من قانون الجرائم الإلكترونية الأردني البرنامج بأنه: «مجموعة من الأوامر والتعليمات الفنية المعدّة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات».

وثمّة تعريفٌ أوضحُ للبرمجيات الخبيثة صاغته المادة (2) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم 17 لسنة 2012، بقولها: «البرمجيات الخبيثة: هي برمجيات حاسوبية مصممة لإلحاق الضرر بالأجهزة الحاسوبية، أو المنظومة المعلوماتية، أو المواقع الإلكترونية، أو الشبكة أو التعطيل عليها أو تبطئتها، أو تخريب محتوياتها أو مواردها، أو جمع معلومات عنها، أو عن مالكيها أو مستخدميها، أو عن بياناتهم دون إذنهم، أو إتاحة الدخول إليها أو استخدامها أو استخدام مواردها بطريقة غير مشروعة».

ومن المُلاحظ أن أغلب محاولات الاختراق تتم من خلال برامج متوافرة على شبكة الإنترنت، ويستطيع أيُّ شخص لديه خبرة تقنية أن يستخدمها[36]، ويُسْتَفَاد من المادة (4) من قانون الجرائم الإلكترونية بأنَّهُ يتعيَّنُ استخدام البرنامج أو نشره أو إدخاله بوساطة نظام معلوماتي؛ للاعتداء على معلومات يحتويها نظام معلوماتي آخر؛ وذلك لتحقيق هدف أو أكثر من الأهداف المذكورة في المادة (4) من قانون الجرائم الإلكترونية. وسوف نوضح هذه الأهداف بالتفصيل لدى شرحنا، بعد قليل، لِصُوَرِ الركن المادي في الجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج.

ثانيًا: مدى لزوم وجود برنامج كوسيلة لارتكاب جرائم الخطر الذي يهدد سلامة المعلومات المصرفية

وفقًا للقواعد العامة لا تُعَدُّ وسيلة ارتكاب الجريمة عنصرًا مطلوبًا لتوافر الركن المادي المكوِّن لها، ولكن قد يشترط القانون استثناءً لقيام جريمة معيَّنة، وجودَ عنصر لا تقوم الجريمة إلا بتوافره، وبمعنى آخر فإنَّ الركن المادي للجريمة لا يتحقق إلا بوجود هذا العنصر، وهذا ما فعلَهُ المُشرِّع الأردني، حينَ اشترط في المادة (4) من قانون الجرائم الإلكترونية، لقيام الركن المادي في جرائم الاعتداء على المعلومات التي يحتويها النظام المعلوماتي، ضرورةَ وجود برنامج يستخدِمُهُ الجاني، أو ينشره، أو يدخله بوساطة نظام معلومات للاعتداء على معلومات يحتويها نظام معلوماتي آخر؛ وذلك بهدف حذف هذه المعلومات، أو تغييرها، أو نسخها، أو تحقيق أيِّ هدف من الأهداف الأخرى المذكورة في المادة (4) من قانون الجرائم الإلكترونية على سبيل الحصر، والتي سنوضحها بعد قليل.

(36) عادل حماد عثمان، مرجع سابق، ص138.

ثالثًا: صُوَرُ الركن المادي في الجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج

من أهمِّ هذه الصور ما يأتي:

1- استخدام برنامج بوساطة نظام معلومات؛ بهدف إلغاء أو حذف معلومات يحتويها نظام معلومات مصرفي: إنَّ من أفعال الاعتداء، باستخدام برنامج على المعلومات التي يحتويها النظام المعلوماتي الخاص بالشركات التي تقدم خِدْمات مصرفية التي وردت في المادة (4) من قانون الجرائم الإلكترونية فِعْلَي الإلغاء والحذف، وأيٌّ منهما يؤلِّفُ الركنَ الماديَّ لجريمة الاعتداء على المعلومات التي يحتويها نظام المعلوماتي المصرفي باستخدام برنامج، وفي الوقت ذاته يُعَدُّ الإلغاء أو الحذف هدفًا يسعى الجاني إلى تحقيقه. ومنعًا للتكرار؛ نُحيلُ الحديث بشأن هذين الفعلين على ما قِيلَ عنهما في المطلب السابق.

ومن الجدير بالذكر أنَّ جرائم الاعتداء على المعلومات المصرفية باستخدام برنامج، المنصوص عليها في المادة (4) من قانون الجرائم الإلكترونية الأردني، تختلف عن جرائم الدخول غير المشروع المنصوص عليها في المادة (3) من القانون ذاته؛ لأنَّ الأخيرة تشترط الدخول غير المشروع إلى النظام المعلوماتي لقيام جريمة الدخول كما أسلفنا القول، في حين لم تشترط المادة (4) هذا الدخول، بل يكفي استخدام برنامج من بُعْد، فقد يقوم الجاني بتحميل الفيروس وإرساله عن طريق قرص مَرِنٍ أو صلْب.

يُسْتَفَاد من صياغة المادة (4) من قانون الجرائم الإلكترونية، بعد الإحالة إليها بموجب المادة (7) من القانون ذاته، أنَّ الركن المادي المُكوِّن لهذه الجريمة يقوم بمُجرَّد استخدام أو نشر أو إدخال البرنامج بوساطة نظام معلوماتي للاعتداء على المعلومات التي يحتويها نظام المعلوماتي المصرفي، بهدف إلغائها أو حذفها، حتى ولو لم يتمّ إلغاءُ المعلومات أو حذفُها كنتيجةٍ للسلوك الجرمي، ولكن يشترط لقيام هذا الركن إثبات هدف الجاني، وهو إلغاء المعلومات أو حذفها؛ وذلك لأن هذه الجريمة من الجرائم ذات السلوك المُجرَّد[37]، وبناءً على ذلك يُعاقَب مُرتكِب هذه الجريمة بعقوبة الجريمة التامة، وهو بذلك يتساوى في استحقاق العقوبة مع من يرتكب جريمة إلغاء المعلومات أو حذفها باستخدام برنامج، كوسيلة اعتداء على المعلومات التي يحتويها نظام المعلومات المصرفي.

(37) بهذا المعنى يُنظَر: مروان الزعبي، مرجع سابق، ص117.

وكُنا نتمنى من المُشرِّع الأردني لو أنَّهُ ميَّزَ في العقاب بين جريمة استخدام البرنامج، بهدف إلغاء المعلومات التي يحتويها نظام المعلومات المصرفي أو حذفها، وبين جريمة إلغاء المعلومات أو حذفها باستخدام البرنامج، وتشديد العقوبة في الجريمة الأخيرة؛ لأنها هي الأكثرُ جَسَامَةً وخطورةً؛ بسبب تحقق نتيجتها.

2- استخدام برنامج بوساطة نظام معلومات؛ بهدف تغيير أو إتلاف أو تدمير معلومات يحتويها نظام معلومات مصرفي: من أفعال الاعتداء على المعلومات باستخدام البرامج المنصوص عليها في المادة (4) من قانون الجرائم الإلكترونية تغييرُ المعلومات أو إتلافها أو تدميرها، وأيٌّ من هذه الأفعال يؤلِّفُ الركنَ الماديَّ لجريمة الاعتداء على المعلومات التي يحتويها نظام المعلومات المصرفي، وفي الوقت ذاته فإنَّ أيًّا من هذه الأفعال يُعَدُّ هدفًا يسعى الجاني إلى تحقيقه. ومنعًا للتكرار؛ نُحيل الحديثَ بشأن المقصود بهذه الأفعال على ما قِيلَ عنها في المطلب السابق.

ويقوم الركن المادي المُكوِّن لهذه الجريمة، بمُجرَّد استخدام البرنامج أو نشره أو إدخاله بوساطة نظام معلوماتي للاعتداء على المعلومات التي يحتويها نظام المعلومات المصرفي؛ بهدف تغيير هذه المعلومات، أو إتلافها، أو تدميرها، حتى لو لم يتحقق التغيير أو الإتلاف أو التدمير كنتيجة للسلوك الجرمي؛ وذلك لأن هذه الجريمة من الجرائم ذات السلوك المُجرَّد.

3- استخدام برنامج بوساطة نظام معلومات بهدف نسخ، أو نقل، أو إفشاء، أو التقاط معلومات يحتويها نظام معلومات مصرفي: وفقًا للمادة (4) من قانون الجرائم الإلكترونية، تندرِجُ أفعال نسخ، أو نقل، أو إفشاء، أو التقاط المعلومات التي يحتويها نظام المعلومات المصرفي ضمن أفعال الاعتداء على المعلومات المصرفية باستخدام برنامج؛ لذا فإنَّ أيًّا من هذه الأفعال يؤلِّفُ الركنَ الماديَّ لجريمة الاعتداء على المعلومات باستخدام برنامج، وفي الوقت ذاته فإنَّ أيًّا من هذه الأفعال يُعَدُّ هدفًا يسعى الجاني إلى تحقيقه. ويُقصدُ بالالتقاط، مثلما تمَّ تعريفه في المادة (1) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، بأنه: «مشاهدة المعلومات أو البيانات أو الحصول عليها». ومنعًا للتكرار؛ نُحيل الحديث بشأن المقصود بأفعال النسخ والنقل والإفشاء على ما سبق أن قِيلَ عنها في المطلب السابق. ومن المفيد أن نشير هنا إلى معنى إفشاء المعلومات ونسخها، كما قضت إحدى المحاكم الأردنية بقولها[38]: «... أن يكون هدف الدخول غير المصرح به إلى النظام المعلوماتي للحاسب الآلي هو إفشاء معلومات أو بيانات إلكترونية،

(38) قرار محكمة صلح غرب عمان بصفتها الجزائية، رقم (4029) لسنة 2019، موقع قرارك.

أي نشرها، وإتاحتها للغير، وبما يمثل انتهاكًا للخصوصية والسرية لمالك تلك البيانات أو المعلومات، وحيث إنَّ الغاية من التجريم، في هذه الحالة، هي حماية حق مالكي تلك البيانات أو المعلومات والحفاظ على الخصوصية السرية، وترتكز الخصوصية على فكرة حق الشخص في أن يقرر متى وكيف يمكن للآخرين مشاركته في بياناته أو معلوماته المهنية أو الخاصة أو الشخصية. أمَّا فكرة السرية فترتكز على فكرة حق الشخص بأن يخفي بياناته ومعلوماته المهنية أو الخاصة أو الشخصية عن الغير».

وبشأن توضيح معنى نسخ المعلومات ونقلها قالت المحكمة ذاتها[39]: «... يُقصدُ بالنسخ، أن يكون الدخول غير المصرح به إلى النظام المعلوماتي للحاسب الآلي، أو الشبكة المعلوماتية، بغرض نسخ بيانات أو معلومات إلكترونية، أي أن الفاعل يتعدى بغرضه مُجرَّد الاطلاع إلى النسخ، وهو الاحتفاظ بنسخة من تلك المعلومات أو البيانات ويشمل ذلك طباعتها، ولكن من دون حذفها أو شطبها من موقعها الأصلي... ويُقصد بنقل المعلومات إرسالها، أي أن يكون الدخول غير المصرح به إلى النظام المعلوماتي للحاسب الآلي، أو الشبكة المعلوماتية، يكون بغرض إرسال المعلومات والبيانات المُخَزَّنة في نظام المعلومات، سواء أكان ذلك داخل ذات النظام المعلوماتي، أي من موقع إلى آخر داخل النظام ذاته، أو إلى نظام آخر، أو إلى أداة تخزين معلومات أخرى، ومن دون إبقاء تلك البيانات والمعلومات في مكانها الأصلي، أي شطبها من مكانها الأصلي».

ومن الجدير بالذكر أنَّ الركن المادي المُكوِّن لهذه الجريمة، يقوم بمُجرَّد استخدام البرنامج أو نشره أو إدخاله في النظام المعلوماتي على النحو السالف ذِكْرُه؛ وذلك بهدف نسخ المعلومات، أو نقلها، أو إفشائها، أو التقاطها، حتى لو لم يتحقق نسخ المعلومات، أو نقلها، أو إفشائها، أو التقاطها كنتيجةٍ للسلوك الجرمي؛ وذلك لأن هذه الجريمة من الجرائم ذات السلوك المُجرَّد.

4- استخدام برنامج بوساطة نظام معلومات بهدف تعطيل أو إيقاف أو تشويش أو إعاقة أو حجب خدمة نظام معلومات مصرفي: تقوم هذه الصورة من الركن المادي باستخدام الجاني برنامجًا عن طريق نظام معلومات بهدف تعطيل أو إيقاف عمل نظام معلومات مصرفي، بحيث يُصبح عملُهُ غيرَ ممكن، ويكونُ التعطيل أو التوقيف كُليًا عند مَحْوِ كلِّ المعلومات أو البرامج أو الجزء المسؤول

(39) قرار محكمة صلح غرب عمان بصفتها الجزائية، رقم (4029)، لسنة 2019، موقع قرارك.

عن دخول الأشخاص المصرح لهم بالدخول في النظام[40]، وكما أسلفنا القول، يقصد بالتوقيف الإعاقة المؤقتة عن العمل، ويقصد بالتعطيل التخريب، أيًا كان شكله ونوعه[41].

وكذا تقوم هذه الصورة للركن المادي باستخدام البرنامج على النحو السالف ذِكْرُه؛ بهدف تشويش، أو إعاقة، أو حجب خدمة نظام المعلومات المصرفي. ويرى الباحثان أنَّهُ يُقصَدُ بالتشويش اضطرابُ النظام المعلوماتي، بحيثُ تختلط المعلومات التي يحتويها بعضها مع بعض، وتصبح غير واضحة، على نحوٍ يتعذَّرُ مَعَهُ فهمُها، ويُقصَدُ بالإعاقة هنا عدمُ قدرة النظام المعلوماتي على إرسال المعلومات واستقبالها بسَبَبِ البرنامج الذي استُخدَمَ لتحقيق هذا الهدف، ويُقصَدُ بحجب خدمة النظام، مثلما أسلفنا القول، إخفاؤُها ومنعُ الاستفادة منها.

ويتحقق الركن المادي المُكوِّن لهذه الجريمة، بمُجرَّد استخدام البرنامج في النظام المعلوماتي على النحو السالف ذِكْرُه؛ بهدف تعطيل، أو إيقاف، أو تشويش، أو إعاقة، أو حجب خدمة نظام المعلومات المصرفي، حتى لو لم يتحقق تعطيل هذا النظام، أو إيقافه، أو تشويشه، أو إعاقته عن العمل كنتيجة للسلوك الجرمي؛ وذلك لأن هذه الجريمة من الجرائم ذات السلوك المُجرَّد.

5- استخدام برنامج بوساطة نظام معلومات بهدف اطلاع الآخرين على معلومات يحتويها نظام المعلوماتي المصرفي: يُقصَدُ بذلك تمكينُ الآخرين من الاطلاع على المعلومات، ويُفترض في هذه الحال أن تكون هذه المعلومات محجوبة عن العامة، كأن تكون مشفَّرةً؛ فيقوم الجاني باستخدام برنامج يفُكُّ التشفير ويجعلُها مُتاحةً للعموم[42]، وهذا السلوك المادي كغيره من السلوكيات التي ذكرناها فيما سبق، فهو يحقق الركن المادي المُكوِّن لهذه الجريمة بمُجرَّد استخدام البرنامج؛ بهدف تمكين الآخرين من الاطلاع على المعلومات التي يحتويها نظام المعلومات المصرفي، حتى لو لم يتمكن الآخرون من الاطلاع على المعلومات التي يحتويها النظام المصرفي؛ وذلك لأن هذه الجريمة من الجرائم ذات السلوك المُجرَّد.

(40) حسن المناصير، مرجع سابق، ص57.
(41) عبدالإله النوايسة، جرائم تكنولوجيا المعلومات، مرجع سابق، ص256.
(42) عبدالإله النوايسة، جرائم تكنولوجيا المعلومات، مرجع سابق، ص265.

الفرع الثالث

الركن المعنوي في جرائم الخطر الذي يهدد سلامة المعلومات المصرفية باستخدام برنامج

تُعَدُّ الجرائم التي تشكل خطرًا على المعلومات المصرفية، باستخدام البرامج المنصوص عليها في المادة (4) من قانون الجرائم الإلكترونية من الجرائم القصدية؛ لأن هذه المادة اشترطت وجود القصد صراحةً؛ لذلك يتعيّن توافر عنصري هذا القصد، وهما العلم والإرادة، فينبغي أن يعلم الجاني أن لديه برنامجًا، ويعلَمَ أنه يستخدم هذا البرنامج أو ينشره أو يدخله بوساطة نظام معلوماتي للاعتداء على معلومات يحتويها نظام المعلومات المصرفي؛ وذلك لتحقيق هدف أو أكثر من الأهداف المذكورة في المادة (4) من قانون الجرائم الإلكترونية. ولكي يكتمل القصد الجنائي هنا؛ يتعيَّنُ توافر العنصر الثاني، وهو عنصر الإرادة، فيجب أن تنصرف إرادة الجاني الحرة إلى استخدام برنامج بوساطة نظام معلومات للاعتداء على معلومات يحتويها نظام معلومات مصرفي؛ لتحقيق هدف أو أكثر من الأهداف المذكورة في المادة (4) السالِفِ ذِكْرُها.

ومن خلالِ مطالعة المادة (4) من قانون الجرائم الإلكترونية الأردني، وبعد الإحالة عليها بموجب المادة (7) من القانون ذاته، يتَّضِحُ أنه يشترط وجودُ قصدٍ خاصٍّ في جرائم الاعتداء على المعلومات باستخدام برنامج، ويتمثل القصدُ الخاصُّ هنا بالهدف الذي يسعى الجاني إلى تحقيقه، وهذا الهدف يتعدَّدُ ويتنوع، وقد تطلَّبَهُ المُشرِّعُ صراحةً في المادة (4) من قانون الجرائم الإلكترونية، وقد يكونُ هذا الهدفُ على سبيل المثال حذفَ المعلومات، أو نقلَها، أو نسخَها، أو إتلافَها... إلخ.

وعليه، يُشترط توافر القصد الخاص بجانب القصد العام لقيام جرائم الاعتداء على المعلومات التي تحتويها نظم المعلومات المصرفية باستخدام برنامج. وفي حال انتفاء القصد الخاص أو تعذر إثباتهُ بكل طرائِقَ الإثبات؛ فإنَّ هذه الجرائم تنتفي وفقًا لذلك.

الفرع الرابع

عقوبة جرائم الخطر الذي يهدد سلامة المعلومات المصرفية باستخدام برنامج

يُعاقَب من يرتكب أيًّا من الجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج بالعقوبة الجنائية المنصوص عليها في المادة (7) من قانون الجرائم الإلكترونية

الأردني، وهي الأشغالُ مُدَّةً لا تقِلُّ عن خمس سنوات، ولا تزيد على عشرين سنة، وبغرامةٍ لا تقِلُّ عن (5000) خمسة آلاف دينار، ولا تزيد على (15000) خمسة عشر دينار.

ومن المُلاحَظ أنَّ هذه العقوبة هي العقوبةُ ذاتها التي أُقِرَّت لجناية الدخول المُجرَّد إلى نظم المعلومات المصرفية (المنصوص والمعاقَب عليها في المادتين (7) و(3/ أ) من القانون ذاته)، وهي أيضًا العقوبة ذاتُها التي أُقِرَّت للجرائم التي تشكل خطرًا يهدد سلامة المعلومات المصرفية (المنصوص والمعاقَب عليها في المادتين (7) و(3/ ب) من القانون ذاته).

الخاتمة

في ضوء ما ناقشته هذه الدراسة، فقد انتهى الباحثان إلى نتائج وتوصيات نعرضها على النحو التالي:

أولًا: النتائج

1- من حيث المبدأ، وفّر قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء النظام السعودي) حمايةً جنائية نسبية لنظم المعلومات المصرفية من خطر الدخول المُجرَّد غير المشروع إلى هذه النظم.

2- من حيث المبدأ، وفّر قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء القانونين القطري والبحريني) حمايةً جنائية نسبية للمعلومات المصرفية الإلكترونية من خطر جرائم السلوك المُجرَّد التي تهدد سلامة المعلومات المصرفية الإلكترونية.

3- أقرَّ قانون الجرائم الإلكترونية الأردني عِدَّةَ جرائم تُشكل خطرًا على نظم المعلومات بشكلٍ عام، وعلى ما تحتويه هذه النظم من معلومات، وجاءت المادة (7) من القانون السالف الذكر، بظرف مشدد لعقوبات هذه الجرائم؛ لتصبح عقوبات هذه الجرائم عقوبات جنائية، ويتوافر هذا الظرف حينما يكون محل هذه الجرائم هو «نظام المعلومات المصرفي، أو ما يحتويه هذا النظام من معلومات مصرفية»، ولعل السبب في ذلك هو بسط مزيد من الحماية الجنائية لنظم المعلومات المصرفية، وما تحتويه هذه النظم من معلومات مصرفية؛ وذلك لأهمية هذا الأمر بالنسبة إلى الاقتصاد الوطني.

4- يتعيَّنُ ابتداءً؛ لقيام جميع الجرائم التي تُشكل خطرًا على نظم المعلومات المصرفية، وعلى ما تحتويه هذه النظم من معلومات، توافُرُ ركنٍ مُفتَرَض (نظام المعلومات المصرفي) وركن مادي، بالإضافة إلى لزوم توافر الركن المعنوي (بصورة القصد)، وفقًا لأحكام قانون الجرائم الإلكترونية الأردني، وأحكام جميع قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء القانون الإماراتي، فهو لم يشترط توافر القصد لقيام هذه الجرائم).

5- يقومُ الركن المادي في «جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية»، وفقًا لأحكام قانون الجرائم الإلكترونية الأردني، وأحكام جميع

قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء النظام السعودي، فهو لم يجرِّم الدخول المُجرَّد إلى نظم المعلومات المصرفية)، بمُجرَّد الدخول بطريقة غير مشروعة إلى هذه النظم، حتى لو لم تنجم عن ذلك أي نتيجة.

6- يقومُ الركن المادي في «الجرائم التي تشكل خطرًا يهدد سلامة المعلومات المصرفية»، وفقًا لأحكام قانون الجرائم الإلكترونية الأردني، وقوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء القانونين القطري والبحريني) بمُجرَّد الدخول غير المشروع إلى نظام المعلومات المصرفي؛ لتحقيق هَدَفٍ يُهدِّدُ سلامة هذه المعلومات، مثل: إلغائها، أو حذفها، أو الحصول عليها... إلخ، وذلك حتى لو لم يتحقق الهدف الذي يسعى إليه الجاني، وذلك لأن هذه الجرائم تنتمي إلى جرائم السلوك المُجرَّد (جرائم الخطر، أو الجرائم الشكلية).

7- ميّز القانون الإماراتي والكويتي والعُماني في العقوبة بين مُجرَّد الدخول إلى نظام المعلومات المصرفي، بقصد الحصول على المعلومات المصرفية، وبين الدخول الذي يكون سببًا في إلغاء هذه المعلومات، أو حذفها، فهذه القوانين اعتبرت تحقق هذه النتيجة ظرفًا مشددًا للعقوبة، وذلك بخلاف القانون الأردني الذي لم يميَّزَ في العقوبة بين الدخول الذي يهدف إلى إلغاء المعلومات المصرفية أو حذفها، والدخول الذي ينتج عنه إلغاء المعلومات المصرفية أو حذفها.

8- لم ينص القانون الأردني والكويتي والبحريني والنظام السعودي على جريمة البقاء غير المصرح به في نظام المعلومات المصرفي، وذلك خلافًا للقانون الإماراتي والقطري والعُماني التي نصت صراحةً على هذه الجريمة.

9- أقرت قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية (باستثناء النظام السعودي الذي لم يُجرِّم الدخول المُجرَّد غير المشروع في نظم المعلومات) لجريمة الدخول المُجرَّد غير المشروع في نظم المعلومات المصرفية عقوبات جنحية، وذلك خلافًا للقانون الأردني الذي عاقب على هذه الجريمة بعقوبات جنائية.

10- يؤيد الباحثان المنهج المتشدد الذي تبناه المشرع الأردني بشأن المعاقبة على جناية الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية؛ لأن هذه النظم

تتمتع بوسائل حماية وإجراءات أمنية تقنية مشددة، والجاني الذي يقتحِمُ هذه الوسائل، ويدخل إلى هذه النظم، يُعَدُّ خَطِرًا وجديرًا بعقوبة الجناية.

11 - أقرت المادة (7) من قانون الجرائم الإلكترونية الأردني، لجريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية، ولجريمة الدخول المُجرَّد غير المشروع في نظم المعلومات المصرفية بهدف ارتكاب أفعالٍ تشكل خطرًا يهدد سلامة المعلومات المصرفية الإلكترونية، ولجريمة استخدام برنامج إلكتروني بهدف ارتكاب أفعالٍ تشكل خطرًا يهدد سلامة المعلومات المصرفية الإلكترونية بعقوبةٍ جنائية واحدةٍ (وهي الأشغال المؤقتة من خمس سنوات حتى عشرين سنة، والغرامة من خمسة آلاف دينار إلى خمسة عشر ألف دينار)، هذا على الرغم من تفاوت هذه الجرائم من حيث درجة خطورتها وجسامتها.

12 - يخلص الباحثان، من مقارنة العقوبات المقررة لجرائم السلوك المُجرَّد التي تشكل خطرًا يهدد سلامة المعلومات المصرفية في ضوء أحكام (القانون الأردني والإماراتي والكويتي والعُماني والسعودي) على أن أشد هذه العقوبات هي العقوبة الجنائية المنصوص عليها في المادة (7) من قانون الجرائم الإلكترونية الأردني. وتليها، من حيث الشدة، العقوبة الجنائية المنصوص عليها في المادة (4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي. وتليها العقوبة الجنحية المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات العُماني. وتليها العقوبات الجنحية المنصوص عليها في القانون الكويتي والنظام السعودي.

13- يرى الباحثان أن العقوبات الجنحية المقررة لجريمة الدخول غير المشروع إلى نظام المعلومات المصرفي، بقصد الحصول على المعلومات المصرفية، المنصوص عليها في القانون العُماني والكويتي والسعودي، لا تتناسب مع خطورة هذه الجريمة.

14- خلت قوانين مكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية من نصوص تُجرِّم وتعاقِب على استخدام برنامج إلكتروني يُشكل خطرًا يهدد سلامة المعلومات المصرفية الإلكترونية، وذلك خلافًا للقانون الأردني الذي نص في (المادة 7، وبالإحالة للمادة 4) من قانون الجرائم الإلكترونية، على عدة جرائم تشكل خطرًا يهدد سلامة المعلومات المصرفية باستخدام برنامج إلكتروني.

ثانيًا: التوصيات

يوصي الباحثان بما يلي:

1- تدخل المنظم السعودي بوضع نص صريح في نظام مكافحة جرائم المعلوماتية، يُجرِّم ويُعاقِب على الدخول المُجرَّد غير المشروع إلى النظام المعلوماتي بشكلٍ عام، وإلى نظام المعلومات المصرفي بشكلٍ خاص.

2- تدخل المشرع الإماراتي بوضع نص في قانون مكافحة جرائم تقنية المعلومات يُشترط بمقتضاه توافر القصد لقيام جريمة الدخول المُجرَّد غير المشروع إلى نظام المعلومات المصرفي.

3- تدخل المُشرِّعَ الأردنيَّ والكويتي والبحريني والسعودي بوضع نصٍّ صريح، يُجرِّم ويعاقِب على فعل البقاء غيرِ المُصرَّح بِهِ في النظام المعلوماتي بشكلٍ عامٍ، وفي نظام المعلومات المصرفي بشكلٍ خاص.

4- تعديل العقوبة المقرَّرة في المادة (7) من قانون الجرائم الإلكترونية، بحيثُ تتدرَّجُ هذه العقوبة من حيثُ الشدة، وفقًا لجسامة الجناية، فجناية الاعتداء على المعلومات التي تحتويها نظم المعلومات المصرفية باستخدام برنامج هي الأخطر، وتستمد خطورتها من وسيلتها. وتليها – من حيثُ الخطورة – جناية الدخول إلى نظم المعلومات المصرفية، بهدف مُعيّن يشكل خطرًا يُهدِّدُ سلامة هذه المعلومات؛ لأنها من جرائم السلوك المُجرَّد. ثم تأتي في أسفل الهرم من حيث الخطورة، جنايةُ الدخول المُجرَّد إلى نظم المعلومات المصرفية.

5- أن يميّز المُشرِّع الأردني بشكلٍ عامّ بين عقوبات الجرائم التي تشكل خطرًا على المعلومات المصرفية التي لم تَنجُمْ عنها نتيجة (جرائم السلوك المُجرَّد)، وبين عقوبات هذه الجرائم إذا نَجَمَت عنها نتيجة، وذلك بتشديد عقوبات الجرائم الأخيرة؛ وذلك أُسوةً بالقانون الإماراتي والكويتي والعُماني.

6- أن يشدد المشرِّع العُماني والكويتي والسعودي عقوبة الجريمة التي تشكل خطرًا على المعلومات المصرفية لتصبح عقوبة جنائية، وذلك لبسط مزيد من الحماية الجنائية للمعلومات المصرفية الإلكترونية؛ وذلك لأهمية هذه المعلومات من الناحية الاقتصادية، فضلًا على أنَّ نظم المعلومات المصرفية، تتضمن وسائل حماية وإجراءات تقنية أمنية مشددة، والجاني الذي يقتحِمُ هذه الوسائل، ويعتدي على المعلومات المصرفية، أو يهدد سلامتها، يُعَدُّ خَطِرًا وجديرًا بعقوبة الجناية.

قائمة المراجع

أولًا: الكتب

- أحمد أبو خطوة، شرح الأحكام العامة لقانون العقوبات الإماراتي، ج1، ط1، منشورات أكاديمية شرطة دبي، 1989.
- أكرم يا ملكي، الأوراق التجارية والعمليات المصرفية، دار الثقافة، عمَّان، الأردن، 2009.
- محمد السعيد عبدالفتاح، الوجيز في شرح قانون العقوبات الاتحادي الإماراتي، القسم العام، الآفاق المشرقة، عمَّان، الأردن، 2014.
- مروان الزعبي، الحماية الجنائية للنقود الرقمية ودورها في تنشيط التجارة الإلكترونية، ط1، دار وائل للنشر والتوزيع، عمَّان، الأردن، 2020.
- نظام المجالي، شرح قانون العقوبات، القسم العام، ط1، دار الثقافة، عمَّان، الأردن، 2005.
- عبد الإله النوايسة، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمَّان، الأردن، 2017.

ثانيًا: الرسائل الجامعية

- أسامة عبدالحفيظ، جرائم الاعتياد وتطبيقاتها في قانون العقوبات الجزائري، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، 2018.
- حسام الخولى، الحماية الجنائية والمدنية لعمليات البنوك الإلكترونية: دراسة مقارنة، أطروحة دكتوراه، جامعة عين شمس، مصر، 2016.
- حسن المناصير، جريمة الدخول غير المشروع إلى النظام المعلوماتي والتعدي على محتوياته، رسالة ماجستير، جامعة جرش، الأردن، 2016.
- عادل حماد عثمان، الحماية الجنائية للمعاملات الإلكترونية في التشريع السوداني، أطروحة دكتوراه، جامعة أم درمان الإسلامية، السودان، 2015.
- خالد الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، رسالة ماجستير كلية القانون، جامعة قطر، 2019.

ثالثًا: الأبحاث العلمية

- أسامة العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي، مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، السعودية، العدد 14، سنة 2012.
- زياد العنزي وعبدالله احجيله، الجوانب القانونية لمسؤولية مدير المجموعة في مواقع التواصل الاجتماعي في القانون الاتحادي الإماراتي، مجلة الحقوق، جامعة البحرين، مج16، ع1، سنة 2019.
- كارمايكل جفري ومايكل بومرليانو مايكل، تطور المؤسسات المالية غير المصرفية ومراقبتها، منشورات البنك الدولي (السلسلة المالية)، ترجمة: الأكاديمية العربية للعلوم المالية والمصرفية، عمَّان، الأردن، 2004.
- نورا عدلي رزق، المؤسسات المالية غير المصرفية، صندوق النقد العربي، الإمارات العربية المتحدة، ع6، سنة 2021.
- فاديا سليمان، الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، عمَّان، الأردن، مج23، ع1، سنة 2015.
- عبدالإله النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، مج15، ع1، 2016.
- عبدالله ذيب محمود، جريمة الدخول غير المشروع وفقًا للقرار بقانون رقم 10 لعام 2018 بشأن الجرائم الإلكترونية الفلسطيني، مجلة جامعة القدس المفتوحة للبحوث الإنسانية والاجتماعية، مج1، ع48، سنة 2019.

المحتوى

الموضوع	الصفحة
الملخص	459
المقدمة	461
المبحث الأول: الحماية الجنائية لنظم المعلومات المصرفية في مواجهة جريمة الدخول غير المشروع	464
المطلب الأول: الركن المُفتَرَض في جريمة الدخول المُجرَّد غير المشروع في نظم المعلومات	465
الفرع الأول: التعريف بالشركات المالية التي تختص بتقديم خدمات مصرفية	466
أولًا: مفهوم الشركات المالية المختصة بتقديم خدمات مصرفية	466
ثانيًا: بعض الخدمات المصرفية التي تقدمها الشركات المالية	468
الفرع الثاني: التعريف بنظام المعلومات المُسْتَهدَف بجريمة الدخول المُجرَّد غير المشروع	469
المطلب الثاني: الركن المادي في جريمة الدخول المُجرَّد غير المشروع في نظم المعلومات المصرفية	470
الفرع الأول: المقصود بالدخول كنشاط جرمي في جريمة الدخول غير المشروع إلى نظم المعلومات	471
الفرع الثاني: مدى اشتراط وجود وسائل حماية أمنية لنظام المعلومات لقيام جريمة الدخول المُجرَّد	472
الفرع الثالث: مدى تجريم البقاء غير المصرح به داخل نظام المعلومات المصرفي	473
المطلب الثالث: الركن المعنوي في جريمة الدخول المُجرَّد غير المشروع إلى نظم المعلومات المصرفية	474

الموضوع	الصفحة
المطلب الرابع: عقوبة جريمة الدخول المُجرَّد غير المشروع في نظم المعلومات المصرفية	476
المبحث الثاني: الحماية الجنائية للمعلومات المصرفية الإلكترونية من خطر جرائم السلوك المُجرَّد	478
المطلب الأول: الحماية الجنائية للمعلومات المصرفية الإلكترونية من جرائم تُشكِّل خطرًا يُهدد سلامتها	479
الفرع الأول: الركن المُفتَرَض في الجرائم التي تشكل خطرًا يهدد سلامة المعلومات المصرفية	481
الفرع الثاني: الركن المادي في الجرائم التي تشكل خطرًا يُهدِّد سلامة المعلومات المصرفية	482
أولًا: صور الركن المادي في جرائم الخطر الذي يهدد سلامة المعلومات المصرفية في القانون الأردني	482
ثانيًا: الركن المادي في جرائم الخطر الذي يهدد سلامة المعلومات المصرفية الإلكترونية في قوانين دول مجلس التعاون لدول الخليج العربية	485
الفرع الثالث: الركن المعنوي في جرائم الخطر الذي يهدد سلامة المعلومات المصرفية	487
أولًا: عنصر العلم	487
ثانيًا: عنصر الإرادة	488
الفرع الرابع: عقوبة جرائم الخطر الذي يهدد سلامة المعلومات المصرفية الإلكترونية	491
أولًا: العقوبة في قانون الجرائم الإلكترونية الأردني	491
ثانيًا: العقوبة في القانون الإماراتي والكويتي والعُماني والسعودي	492

الموضوع	الصفحة
المطلب الثاني: الحماية الجنائية للمعلومات المصرفية الإلكترونية من برنامج يُشكل خطرًا يهدد سلامتها	494
الفرع الأول: الركن المُفتَرَض في الجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج	495
الفرع الثاني: الركن المادي في جرائم الخطر التي تهدد سلامة المعلومات المصرفية باستخدام برنامج	495
أولًا: تعريف البرنامج الذي يُشكل خطرًا على المعلومات المصرفية	496
ثانيًا: مدى لزوم وجود برنامج كوسيلة لارتكاب جرائم الخطر الذي يهدد سلامة المعلومات المصرفية	496
ثالثًا: صُوَرُ الركن المادي في الجرائم التي تشكل خطرًا على المعلومات المصرفية باستخدام برنامج	497
الفرع الثالث: الركن المعنوي في جرائم الخطر الذي يهدد سلامة المعلومات المصرفية باستخدام برنامج	501
الفرع الرابع: عقوبة جرائم الخطر الذي يهدد سلامة المعلومات المصرفية باستخدام برنامج	501
الخاتمة	503
قائمة المراجع	507