الحماية الجنائية من جرائم التعدي على (أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية) دراسة مقارنة

Criminal protection from infringement crimes

(systems, programs, information networks, and websites) a comparative study

الباحثة : علياء علي القحطاني

الدرجة العلمية: ماجستير في القانون العام

أخصائي قانوني - قطر

الملخص

تجدر الإشارة إلى أن الجريمة الإلكترونية أصبحت تشكل عبئاً ثقيلاً على مختلف دول العالم، لأنها تعتبر من الجرائم العابرة للحدود، وتتميز بالانتشار المستمر في جميع الدول نتيجة لتزايد الاعتماد على تكنولوجيا المعلومات في مختلف المجالات العلمية والعملية، كما تكمن خطورتها في أنها قد تقع على أنظمة وبرامج مرتبطة بالأمن القومي والاقتصادي، فينجم عنها خسائر وأضرار جسيمة على الدولة والمؤسسات وحتى الأفراد. حيث استحدثت الثورة التكنولوجية المعلوماتية في عصرنا الحاضر مجموعة من الجرائم الجديدة تسمى بالجرائم الإلكترونية، ويكون محل الجريمة فيها على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية.

تهدف هذه الدراسة إلى بيان مدى قدرة هذه النصوص في توفير الحماية الجنائية اللازمة للتصدي لجريمة التعدي الإلكتروني في القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري، والمرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، للتعرف على أفضل سبل الحماية الجنائية الفعالة للحد من جريمة التعدي الإلكتروني.

Abstract

It should be noted that cybercrime has become a heavy burden on various countries of the world, because it is considered a cross-border crime, and it is characterized by its continuous spread in all countries as a result of the increasing dependence on information technology in various scientific and practical fields, in fact it may fall on systems and programs that linked to national and economic security, resulting in massive losses and damages to the state, institutions, and even individuals. Where the information technology revolution in our time has introduced a group of new crimes called cybercrime, and the crime in it is on information systems, programs, networks and websites.

This study aims to demonstrate the extent of the ability of these texts to provide the necessary criminal protection to address the crime of cyber-aggression in the Qatari regulation of Cybercrime Combating No. (14) of 2014 and Federal Decree-Law No. (5) of 2012 on Combating Information Technology Crimes in UAE, to identify the best effective criminal protection methods to reduce the crime of electronic infringement.

المقدمة:

تجدر الإشارة إلى أن جرائم التعدي الإلكتروني على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية أصبحت تشكل عبئاً ثقيلاً على مختلف دول العالم، لأنها تعتبر من الجرائم الخطيرة دولياً، وتكمن خطورتها في أنها قد تقع على أنظمة وبرامج مرتبطة بالأمن القومي والاقتصادي، فينجم عنها خسائر وأضرار جسيمة على الدولة والمؤسسات وحتى الأفراد، إذ تزداد أهمية استعمال البرامج الإلكترونية والنظم المعلوماتية في عصرنا الحالي، لذلك تستوجب هذه الأنظمة حماية خاصة من جرائم الاعتداء الإلكتروني للحد منها، فبالرغم من تكاتف الدول إلى عقد مؤتمرات واتفاقيات دولية لمكافحة هذه الجريمة، بالإضافة إلى سن تشريعات خاصة لمكافحة الجريمة الإلكترونية كما فعل المشرع القطري، ألا أن جرائم التعدي الإلكتروني في انتشار مستمر في جميع دول العالم، نتيجة لتزايد الاعتماد على تكنولوجيا المعلومات في مختلف المجالات العلمية والعملية على المستوى الدولي.

أولاً: مشكلة البحث:

الإشكالية التي يتناولها البحث تتجلى في أن جريمة التعدي الإلكتروني في تزايد مستمر، رغم الجهود المبذولة في محاربة هذه الجريمة على الصعيدين المحلي والدولي، فلقد أصدرت دولة قطر تشريعاً خاصاً لمكافحة الجرائم الإلكترونية وهو القانون رقم (14) لسنة 2014، لكن جرائم التعدي الإلكتروني مازالت في تزايد مطرد، وبذلك تتحدد مشكلة هذا البحث في التساؤل التالي: هل القانون القطري وفر الحماية الجنائية الموضوعية الكاملة للنظام المعلوماتي من جرائم التعدي الإلكتروني؟ وهل العقوبات المقررة في القانون القطري كافية للحد من انتشار جريمة التعدي الإلكتروني، أم يحتاج إلى تعديل؟ لذلك سوف نحاول في هذا البحث طرح هذه المشكلة، مركزين على ناحية مدى كفاية القانون رقم (14) لسنة 2014 بشأن مكافحة الجرائم الإلكترونية في التصدي لجرائم التعدي الإلكتروني وتوفير الحماية الجنائية من جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية.

ثانياً: أهمية البحث:

تكمن أهمية هذا البحث فيما يلي:

- ندرة الدراسات القانونية التي تناولت الحماية الجنائية من جرائم التعدي الإلكتروني في القانون القطري نظراً لحداثته، مما اقتضى التعمق في النصوص القانونية التي لم يتطرق لها الباحثون من قبل.
- ضرورة معالجة النصوص التشريعية المنصوص عليها في القانون القطري، والمقررة لمكافحة جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، لبيان مواطن النقص التي تعتري هذه النصوص ليتم تلافيها ومعالجتها.
- أهمية تعديل العقوبات المقررة على مرتكبي جرائم التعدي الإلكتروني، لتوفير الحماية الجنائية الفعالة لأنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية.

ثالثاً: فرضيات البحث:

تحاول هذه الدراسة الإجابة على الفرضيات التالية:

1- ما المقصود بجرائم التعدي الإلكتروني؟
2- ما هي صور جرائم التعدي الإلكتروني؟

3- هل النصوص القانونية النافذة كافية لتوفير الحماية الجنائية لأنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية من جرائم التعدي الإلكتروني؟

4- هل العقوبات المنصوص عليها في القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، كافية للحد من الجريمة محل البحث؟

5- هل تحتاج نصوص العقوبات الخاصة بالجريمة محل البحث في القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، إلى تعديل؟

رابعاً: أهداف البحث:

يهدف هذا البحث إلى بيان مفهوم جريمة التعدي الإلكتروني وصورها، وتحديد محل الحماية الجنائية لهذه الجريمة، كما يهدف بشكل رئيسي إلى إبراز الواقع الحالي للنصوص القانونية الواردة في القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية المتعلقة بمحل البحث وتحديد مدى قدرة هذه النصوص، في توفير الحماية الجنائية اللازمة للتصدي للجريمة محل البحث.

خامساً: منهج البحث:

- المنهج الوصفي: من خلال توصيف جريمة التعدي الإلكتروني لإيضاح مفهومها وصورها، وتحديد محل الحماية الجنائية لجريمة التعدي، وصولاً إلى تحديد العقوبات المترتبة على مرتكبيها.
- المنهج التحليلي: عن طريق تحليل المحتوى لوصف صور جرائم التعدي الإلكتروني.
- المنهج المقارن: الذي يقوم على دارسة المواجهة التشريعية لجريمة التعدي الإلكتروني في دولة قطر ودولة الإمارات العربية المتحدة، وقد تم اختيار المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات لأنه يتميز بتعريفات دقيقة وعقوبات محددة بشكل واضح، لذلك ارتأينا أن يكون محلاً للمقارنة مع القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري، بغية التعرف على أفضل سبل الحماية الجنائية الفعالة للحد من جريمة التعدي الإلكتروني.

سادساً: الدراسات السابقة:

تناولت الدراسات السابقة جريمة الدخول غير المشروع في التشريعات الأخرى، والتي تعتبر أحد صور جرائم التعدي الإلكتروني، ولعل من أهم الدراسات السابقة التي تم الاستعانة بها هي:

1. حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، ط1، دار الفكر والقانون، مصر، 2015.
2. محمد كمال الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، مصر، 2015
3. عبد الإله محمد النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، وزارة العدل، قطر، العدد1، 2016.

سابعاً: خطة البحث:

تم تقسيم هذا البحث إلى مبحثين، تناول المبحث الأول: التعريف بجريمة التعدي الإلكتروني، وبيان صورها، ونطاق الحماية فيها، أما المبحث الثاني: يناقش الجزاءات المقررة على مرتكبي جريمة التعدي الإلكتروني، مختتمين البحث بأهم النتائج والتوصيات التي خلصنا إليها من خلال بحثنا هذا.

المبحث الأول: ماهية جرائم التعدي الإلكتروني

جرائم التعدي الإلكتروني على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية تُعد أحد صور الجرائم الإلكترونية وإحدى تطبيقاتها، لمعرفة ماهية جرائم التعدي الإلكتروني ينبغي علينا توضيح مفهوم جرائم التعدي الإلكتروني وصورها، وعناصر الحماية فيها.

لذلك سنخصص المطلب الأول لتوضيح مفهوم جرائم التعدي الإلكتروني وصورها، بينما نخصص المطلب الثاني لبيان العناصر محل الحماية الجنائية فيها.

المطلب الأول: مفهوم جرائم التعدي الإلكتروني

لقد تعددت التعريفات الفقهية والتشريعية والدولية لمصطلح "الجريمة الإلكترونية" نظراً لتجدد هذه الظاهرة وتطور أساليبها وبراعة الجناة في ارتكابها، وعلى الرغم من هذا الاهتمام التشريعي بهذه الظاهرة إلا أنه لا يوجد حتى الآن تعريف دقيق لها، وإن كان بعض الفقه يسميها الجريمة المعلوماتية، والبعض الآخر يسميها جرائم الكمبيوتر، وآخرون يسمونها جرائم تكنولوجيا المعلومات.

لقد أورد المشرع القطري تعريفاً للجريمة الإلكترونية في القانون رقم (14) لسنة 2014 بشأن مكافحة الجرائم الإلكترونية، حيث نصت المادة الأولى من القانون على أنها "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون"[1470]، أما المشرع الإماراتي فلم يورد تعريفاً خاصاً للجريمة الإلكترونية في المرسوم بقانون اتحادي رقم (15) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

وفي ضوء ما تقدم نتناول في الفرع الأول مفهوم جرائم التعدي الإلكتروني، أما الفرع الثاني سنبين فيه صور جرائم التعدي الإلكتروني في القانون رقم (14) لسنة 2014 بشأن مكافحة الجرائم الإلكترونية القطري، والمرسوم بقانون اتحادي رقم (15) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

الفرع الأول: مفهوم جرائم التعدي الإلكتروني

يمكن تعريف جرائم التعدي الإلكتروني بأنها كافة صور السلوك غير المشروع، والذي يمثل اعتداء بالضرر أو التهديد به، على أمن وحماية الشبكات المعلوماتية، وشبكة الاتصالات، ونظام التحكم الإلكتروني ونظم المعلومات وعمليات جمع المعلومات، أو ما شابها، والذي يقرر لها المشرع جزاء جنائي أو تدبير احترازي[1471]. ويتميز المجرم الذي يستعين بالكمبيوتر في ارتكاب جريمته بالذكاء العالي الذي يُمكنه من التغلب على الكثير من العقبات التي تواجهه في ارتكاب تلك الجريمة.[1472]

لقد حدد المشرع القطري في قانون مكافحة الجرائم الإلكترونية محل الدراسة -في الفصل الأول من الباب الثاني- جرائم التعدي الإلكتروني، ويظهر اختلاف هذه الجرائم عن غيرها من الجرائم الاخرى في أنها ترتكب عن طريق استخدام الشبكة المعلوماتية أو أحد وسائل تقنية المعلومات، كأداة أو وسيلة لارتكاب الجريمة، كجرائم المحتوى[1473]، وقد حدد القانون القطري الجرائم

1470المادة (10/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1471حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، ط1، دار الفكر والقانون، مصر، 2015، ص12-13.

1472 غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، مصر، 2013، ص15.

1473المواد (5-9) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

الإلكترونية ومنها: جريمة انشاء موقع لجماعة ارهابية[1474]، أو نشر كيفية تصنيع الأجهزة الحارقة[1475]، أو نشر أخبار غير صحيحة بقصد تعريض سلامة الدولة للخطر[1476]، وكذلك تختلف عن جرائم التزوير والاحتيال الالكتروني[1477]، وجرائم بطاقة التعامل الالكتروني[1478]، وجرائم التعدي على حقوق الملكية الفكرية[1479].

الفرع الثاني: صور جرائم التعدي الإلكتروني

هناك عدة صور لجريمة التعدي الإلكتروني، إذ نص عليها المشرع القطري في المواد (2-4) من القانون محل الدراسة، وسوف نتناولها على النحو التالي: أولاً: جريمة الدخول العمدي غير المصرح به، ثانياً: جريمة تجاوز الدخول المصرح به أو البقاء غير المصرح به، ثالثاً: جريمة الاعتراض غير القانوني، وسوف نقارنها بالمرسوم بقانون الإماراتي في المواد (2و4و5) بشأن مكافحة جرائم تقنية المعلومات، وهي على النحو التالي:

أولاً: جريمة الدخول العمدي غير المصرح به

تعتبر جريمة الدخول غير المصرح به من أبرز جرائم التعدي الإلكتروني، حيث تُعد بمثابة الشرارة الأولى لارتكاب غيرها من الجرائم الإلكترونية، ويقصد بالدخول غير المصرح به أو غير القانوني بأنه الولوج غير المشروع إلى نظام معالجة آلية البيانات، ويتحقق الدخول بالوصول إلى المعلومات والبيانات المخزنة في النظام المعلوماتي دون رضا من المسؤول عنه[1480]. ويعُيب هذا التعريف أنه قصر الدخول بقصد الوصول إلى المعلومات أو البيانات، ولم يشمل حالات الدخول المجرد لغرض الاطلاع فقط، لذا نجد تعريفاً أخر يرى أنها قيام شخص غير مرخص له بإساءة استخدام الحاسب الآلي، للوصول إلى المعلومات والبيانات فيه، أو لإشباع الشعور بالنجاح في اختراق نظام الحماية أو لأي سبب أخر[1481].

وتطبيقاً لذلك، فنص المشرع القطري على أن "يعاقب ... كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها."**1482** وبالمقارنة نص المشرع الإماراتي على أن "يعاقب .. كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية.**1483**

ثانياً: جريمة تجاوز الدخول المصرح به أو البقاء غير المصرح به

يمكن تعريف المقصود بالبقاء غير المصرح به بأنه تواجد الشخص داخل النظام المعلوماتي، دون تصريح من صاحب الإذن في التواجد في النظام في الحالات التي يكون فيها الدخول مشروع، أو لكون الدخول غير مُجرم، ويتصور ذلك في حالتين، الحالة الأولى:

1474المادة (5) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1475المادة (6) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1476المادة (7) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1477المواد (10 و11) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1478المادة (12) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1479المادة (13) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1480محمد كمال الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية: دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، مصر، 2015، ص59.

1481نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية،2005، ص216.

1482 المادة 2 من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1483 لمادة 4 من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

أن يكون الدخول مشروط بالبقاء بفترة زمنية محددة، والحالة الثانية: أن يدخل الشخص إلى النظام المعلوماتي بطريق الخطأ، ويستمر في التواجد في النظام على الرغم من اكتشافه لذلك[1484].

تتحقق هذه الحالة، إذا كان للشخص صلاحيات معينة للدخول إلى النظام المعلوماتي، وقام بتجاوز هذه الصلاحيات الممنوحة له، ودخل إلى مناطق لا يملك الحق في الدخول إليها، لذا فإن توافر هذه الجريمة يتطلب أمرين: الأول: أن يكون الشخص له صلاحية الدخول إلى النظام المعلوماتي بموجب القانون. والثاني: أن يكون هناك تحديد للصلاحيات التي يملكها الشخص في النظام، فإذا تخطى هذه الحدود يشكل فعله جريمة تجاوز الدخول المصرح به[1485].

إذ أن هذه الجريمة لها طبيعة مختلفة عن جريمة الدخول غير المصرح به، فجريمة الدخول جريمة وقتية تتحقق بمجرد الدخول إلى النظام المعلوماتي، أما جريمة البقاء فهي جريمة مستمرة، ولهذا الاختلاف برزت أهمية تجريم فعل البقاء في النظام كجريمة مستقلة.

تكريساً لذلك، نص المشرع القطري على أن: "يعاقب ... كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك.**1486** كما نص المشرع الإماراتي على أن : "يعاقب.. كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة".

وعليه، فإن الركن المادي لجريمة التجاوز المصرح يتمثل في فعل تجاوز التصريح الممنوح من صاحب الحق في الموقع الإلكتروني، والدخول إلى ما لا يشمله التصريح من معلومات، وتتضح هذه الصورة في حالة الموظفين الممنوح لهم صلاحيات محددة على سبيل الحصر، فبقيامهم بالاطلاع على أي بيانات أو معلومات تتجاوز حدود التصريح الممنوح لهم فإن ذلك يعني ارتكابهم لجريمة تجاوز الدخول المصرح به.

ثالثا: جريمة الاعتراض غير القانوني

يقصد بجريمة الاعتراض غير القانوني، "بأنه أي نشاط غير مشروع يهدف إلى الاطلاع على محتوى اتصال من بيانات ومعلومات تتم داخل نظام حاسب آلي واحد، أو أكثر تربطها شبكة اتصالات باستخدام الوسائل الفنية التي تمكنه من ذلك."**1487**

يهدف تجريم الاعتراض غير القانوني إلى حماية الحق في احترام نقل البيانات[1488]، وقد شبه بعض الفقهاء جريمة الاعتراض بالتنصت على محادثة تليفونية، فهو يعني معرفة محتوى اتصال قد يتم داخل نظام حاسب آلي واحد، أو بين عدة أنظمة ترتبط ببعضها بشبكة اتصالات[1489]، ويتم الاعتراض باستعمال وسائل فنية يتم عن طريقها التقاط الانبعاثات الكهرومغناطيسية الناتجة عن نظام معلوماتي أو غيره وهذه الانبعاثات لا تعد بيانات، ولكن يمكن إعادة بناءها بصورة بيانات[1490]، ويرى البعض أن جريمة الاعتراض غير القانوني للمعلومات أو التقاط المعلومات ينشط استخدامها بشكل كبير في المجال السياسي والعسكري والتجاري باعتبارها من قبيل أعمال التجسس على المعلومات[1491].

1484 عبد الإله النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، وزارة العدل، قطر، العدد1، 2016، ص46-47.

1485 محمد الدسوقي، مرجع سابق، ص70.

1486 المادة 3 من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1487 محمد كمال الدسوقي، مرجع سابق، ص 95.

1488 عبد الإله النوايسة، مرجع سابق، ص48.

1489 نائلة قورة، مرجع سابق، ص350.

1490 عبد الإله النوايسة، مرجع سابق، ص48-49.

1491 محمد الدسوقي، مرجع سابق، ص87.

تطبيقاً لذلك، نص المشرع القطري على أن "يعاقب ... كل من التقط أو اعترض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور."**1492** وفي المقابل نص المشرع الإماراتي على أن: " يعاقب ... كل من التقط أو اعترض عمداً وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية"[1493].

ويشترك الركن المعنوي في صور جرائم التعدي الإلكتروني الثلاث السابقة، في صورة القصد الجنائي العام، باعتبارها من الجرائم العمدية، فمن اللازم أن يتوافر لدى الجاني العلم والإرادة، فيجب أن يعلم أن فعله ينصب على نظام معلوماتي وأن يعلم أن ليس له الحق في الدخول[1494]. أما الباعث فإنه لا يعتد فيه، فلا ينفي القصد الجنائي أن يكون قصد المتهم من الدخول إلى النظام هو الإثبات للمسؤولين عن النظام أن هناك ثغرات في أنظمتهم[1495]، فإذا كان الشخص قد وقع في الخطأ أو في الجهل بوجود حظر لدخول النظام الإلكتروني فإنه ذلك يؤدي إلى عدم توافر الركن المعنوي[1496]، كما يكفي توافر القصد الجنائي العام لكي تقع الجريمة، فلا يلزم أن يتوافر لدى الجاني قصد من نوع خاص[1497].

المطلب الثاني: العناصر محل الحماية الجنائية في جرائم التعدي الإلكتروني

تعتبر الحماية الجنائية الموضوعية من أهم أنواع الحماية القانونية التي نص عليها المشرع في النصوص التشريعية، والتي تُجرم وتُعاقب كل من قام بالمساس بالمصالح ذات الأهمية، إذ يشمل نطاق الحماية الجنائية من جرائم التعدي الإلكتروني العناصر التالية:

الفرع الأول: حماية الموقع الإلكتروني

بالرجوع إلى المادة (2) من قانون مكافحة الجرائم الإلكترونية القطري، نجد أن المشرع القطري جرم الدخول بغير وجه حق، عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، إلى (الموقع الإلكتروني) لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها. كما أنه في المادة (3) من القانون سالف الذكر فقد جرم المشرع القطري الدخول العمدي دون وجه حق، بأي وسيلة، (موقعاً الكترونياً)، أو تجاوز الدخول المصرح به، أو استمر في التواجد به بعد علمه بذلك[1498]. وعند الرجوع إلى ذات القانون نجد أن المادة (1) منه عرفت الموقع الإلكتروني بأنه: "مكان إتاحة أو معالجة البيانات أو المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد"[1499].

وبالرجوع إلى التشريع الإماراتي محل المقارنة نجد أنه أيضاً أسبغ الحماية الجنائية على الموقع الإلكتروني، وذلك في كل من المواد (2و4و5) من المرسوم بقانون-محل المقارنة-بشأن مكافحة جرائم تقنية المعلومات. فنص المشرع الإماراتي في المادة (2) من المرسوم بقانون على معاقبة كل من دخل (موقع إلكتروني)، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. وجرم في المادة (4) الدخول بدون تصريح إلى (الموقع الإلكتروني)، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة

1492 المادة 4 من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1493 المادة (15) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1494 عبد الإله محمد النوايسة، مرجع سابق، ص36.

1495 شيماء عبدالغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية دراسة مقارنة بين النظامين اللاتيني والأنجلو أمريكي، رسالة دكتوراه، جامعة المنصورة، مصر، 2005، ص142.

1496 أحمد الكواري، مرجع سابق، ص13.

1497 شيماء عطا الله، مرجع سابق، ص 143.

1498 عبد الإله النوايسة، مرجع سابق، ص13. القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1499 المادة (9/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

بمنشأة مالية، أو تجارية، أو اقتصادية. وجرم في المادة (5) دخول (الموقع الإلكتروني) بقصد تغيير تصاميمه، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه.

وقد أورد المشرع الإماراتي تعريف الموقع الإلكتروني في المادة (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012، "الموقع الإلكتروني: مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية، ومنها مواقع التواصل الاجتماعي، والصفحات الشخصية والمدونات"[1500].

الفرع الثاني: حماية الأنظمة المعلوماتية

نصت المادتان (2و3) من قانون مكافحة الجرائم الإلكترونية القطري، ذات الحماية المقررة للمواقع الإلكترونية لتشمل الأنظمة المعلوماتية، ونجد أن المشرع القطري جرم في المادة (2) الدخول بغير وجه حق إلى (النظام المعلوماتي) لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، وفي المادة (3) يعاقب المشرع كل من دخل عمداً، دون وجه حق، بأي وسيلة، (نظاماً معلوماتياً)، أو تجاوز الدخول المصرح به، أو استمر في التواجد به بعد علمه بذلك. كما حدد المشرع القطري المقصود بالنظام المعلوماتي وأشار إلى أنه "مجموعة برامج وأجهزة، تستخدم لإنشاء أو استخراج المعلومات، أو إرسالها، أو استلامها، أو عرضها، أو معالجتها، أو تخزينها[1501].

ونص المشرع الإماراتي في المادتين (2و4) من المرسوم بقانون -محل المقارنة- على الحماية الجنائية لنظام المعلومات الإلكتروني، فنصت المادة (2) على معاقبة كل من دخل (نظاماً معلوماتياً)، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. أما المادة (4) تعاقب على الدخول بدون تصريح إلى (النظام المعلوماتي)، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية. وعرف المشرع الإماراتي النظام المعلوماتي بأنه "مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك"[1502].

الفرع الثالث: حماية الشبكة المعلوماتية ووسائل تقنية المعلومات

عرف المشرع القطري الشبكة المعلوماتية بأنها "ارتباط بين أكثر من وسيلة لتقنية المعلومات، للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة والعامة والشبكة العالمية "الإنترنت"[1503]، وعرفها المشرع الإماراتي بأنها "ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات"[1504].

أما تقنية المعلومات فقد أشار المشرع القطري إلى أنه يقصد بها " أي وسيلة مادية أو غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام معلوماتي أو شبكة معلوماتية"[1505]، أما المشرع الإماراتي فقد جاء فيه بأن "وسيلة تقنية المعلومات: أي أداة الكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو ايصالها للآخرين"[1506].

1500 المادة (9/1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1501 المادة (4/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1502 المادة (6/1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1503 المادة (3/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1504 المادة (7/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1505 المادة (1/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1506 المادة (10/1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الإماراتي.

كما نصت المادة (3) من قانون مكافحة الجرائم الإلكترونية القطري، ذات الحماية المقررة للمواقع الإلكترونية والأنظمة المعلوماتية لتشمل (الشبكات المعلوماتية ووسيلة تقنية المعلومات)، أما المادة (2) التي جاء في نصها "كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات" نجد أن المشرع لم يعتبر الشبكة المعلوماتية محلاً للجريمة، وإنما اعتبر الشبكة المعلوماتية ووسيلة تقنية المعلومات أداة أو وسيلة لارتكاب الجريمة.[1507]

ونص المشرع الإماراتي في المادتين (2و4) من المرسوم بقانون -محل الدراسة- الحماية الجنائية للشبكة المعلوماتية ووسيلة تقنية المعلومات، حيث جاء في نص المادة (2) يعاقب كل من دخل (شبكة معلومات أو وسيلة تقنية معلومات)، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة، أما المادة (4) فجاء فيها يعاقب كل من دخل بدون تصريح إلى (شبكة معلوماتية أو وسيلة تقنية معلومات)، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية.

الفرع الرابع: حماية البيانات الإلكترونية وبيانات المرور

عاقب المشرع القطري في المادة الرابعة من ذات القانون، كل من التقط أو اعترض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور.[1508]

إذ عرف المشرع القطري البيانات والمعلومات الإلكترونية بأنها "كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام وسيلة تقنية المعلومات، وبوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات وغيرها"[1509]. وعرف بيانات المرور بأنها " أية بيانات أو معلومات إلكترونية تنشأ عن طريق إحدى وسائل تقنية المعلومات توضح مصدر الاتصال والوجهة المرسلة إليها والطريق الذي تسلكه، ووقت وتاريخ وحجم ومدة ونوع الخدمة"[1510].

كما أن المشرع الإماراتي قد أسبغ الحماية الجنائية من الالتقاط أو الاعتراض بالنص على أن "يعاقب...كل من التقط أو اعترض عمداً وبدون تصريح أي اتصال عن طريق شبكة المعلومات"[1511]، وعرف فعل الالتقاط: بأنه "مشاهدة البيانات أو المعلومات أو الحصول عليها"[1512].

ونخلص مما تقدم، إلى أن كل من المشرع القطري والمشرع الإماراتي، كانوا واضحين في حرصهم على التوسع في محل الجريمة، لتشمل كافة ما يمكن أن يتصور أن يكون محلاً لجريمة التعدي الإلكتروني، وإن كانت بعض المصطلحات التي استخدمها المشرع الإماراتي مختلفة عن المصطلحات التي استخدمها المشرع القطري، إلا أنهم متقاربين من حيث المفهوم، كما أنهما قد أحسنا في تحديد المقصود بالعبارات محل الحماية في جرائم التعدي الإلكتروني، ولم يتركا تحديد المقصود بتلك العبارات لاجتهادات القضاء والفقه.

إلا أننا نرى أنه كان من الأجدر أن يُضيف المشرع القطري عبارة (أو بأي وسيلة أخرى) بعد عبارة (كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات) في المادتين (2و4) من القانون محل البحث، إذ تم ذكر عبارة (بأي وسيلة) في المادة (3) ولم يتم ذكرها في المادتين السابقتين، وذلك نظراً للتقدم التكنولوجي الذي نشهده في عصرنا الحالي، إذ أنه من الممكن أن تكتشف طريقة أو وسيلة أخرى يتم عن طريقها التعدي على النظام الإلكتروني غير وسيلة الإنترنت أو الوسائل التقنية.

1507 المادة (2) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1508 المادة (4) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1509 المادة (2/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1510 المادة (7/1) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1511 المادة (15) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1512 المادة (17/1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

وعليه، فقد بينا في هذا المبحث، مفهوم جرائم التعدي الإلكتروني وصورها، ونطاق الحماية فيها، وسوف نتناول في المبحث الثاني الجزاءات المقررة على مرتكبي جريمة التعدي الإلكتروني من خلال تقرير الحماية الموضوعية في القانون القطري، ونقارنها بالجزاءات المقررة في القانون الإماراتي.

المبحث الثاني: الجزاءات الجنائية المقررة لجرائم التعدي الإلكتروني

الجزاء هو أثر حتمي لكل جريمة[1513]، ويهدف الجزاء إلى تحقيق الردع العام والخاص، والعدالة في المجتمع. "ولهذا يعرف الفقه الجنائي العقوبة بأنها المظهر القانوني لرد الفعل الاجتماعي إزاء الجناة"[1514] ولقد تضمن التشريع الداخلي لدولة قطر قانونا خاصاً لمكافحة الجرائم الإلكترونية، إذ تم فرض العقوبات على مرتكبي جريمة التعدي الإلكتروني على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، كما قد تشدد العقوبة على الجاني في حالات معينة، وأيضا يجوز للمحكمة أن تعفي مرتكب الجريمة من العقوبة في بعض الحالات.

وعلى هذا سنوضح في هذا المطلب عقوبة جريمة التعدي الإلكتروني في القانون القطري والقانون الإماراتي، وذلك على النحو التالي:

المطلب الأول: العقوبات الأصلية لجريمة التعدي الإلكتروني

المطلب الثاني: الظروف المشددة لجريمة التعدي الإلكتروني

المطلب الثالث: العقوبات التكميلية لجريمة التعدي الإلكتروني

المطلب الرابع: حالات تخفيف العقوبة أو الإعفاء منها

المطلب الأول: العقوبات الأصلية لجريمة التعدي الإلكتروني

العقوبات الأصلية هي العقوبات التي تنص عليها التشريعات الجنائية باعتبارها الجزء الرئيس للجريمة ويجب على القاضي الحكم بها بعد ثبوت إدانة المتهم، ويمكن تطبيقها بشكل منفرد من دون أن يعلق على الحكم بعقوبة اخرى[1515]. ولقد نص كل من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري، والمرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي، على عقوبات تطبق على مرتكبي جريمة التعدي الإلكتروني، إذ تتنوع هذه العقوبات بحسب جسامة وخطورة الجريمة المرتكبة، فمنها عقوبات سالبة للحرية، وعقوبات مالية، وعقوبات تكميلية. وعليه سنوضح ذلك على الوجه التالي:

الفرع الأول: عقوبة جريمة الدخول العمدي غير المصرح به

نص المشرع القطري على عقوبة الحبس والغرامة المالية لمرتكبي جريمة التعدي الإلكتروني وحدد عقوبة الحبس لمدة لا تجاوز ثلاث سنوات، والغرامة التي لا تزيد على خمسمائة ألف ريال، كعقاب على كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها[1516].

نلاحظ أن المشرع القطري أقر عقوبتي الحبس والغرامة معاً، كجزاء جنائي لصور التعدي على النظام الإلكتروني والمتمثلة في مجرد الدخول الغير مشروع إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة الحكومية، ويعد هذا التشدد في تطبيق كل

1513 محمد عيد الغريب، شرح قانون العقوبات القسم العام، النظرية العامة للعقوبة والتدابير الاحترازية، بدون دار نشر، القاهرة، 2000، ص 961.

1514 أحمد عوض بلال، محاضرات في الجزاء الجنائي، دار النهضة العربية، القاهرة، 2001، ص6.

1515 أوزدن حسين دزه يي، جريمة غسل الأموال، ط1، المكتب الجامعي الحديث، الإسكندرية، مصر، 2012، ص 182.

1516 الفقرة الأولى من المادة (2) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

من عقوبتي الحبس والغرامة من قبيل الحماية المشددة للأمن الإلكتروني للدولة وأجهزتها، والتي تستوجب طبيعة هذه الأنظمة التشدد في العقوبة.

وبالمقارنة مع المشرع الإماراتي، فلقد قرر أيضاً عقوبة السجن المؤقت والغرامة معاً كجزاء جنائي لبعض صور الاعتداء الشديد على الأمن الإلكتروني، على سبيل المثال، تقرير عقوبة السجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم، ولا تجاوز مليون وخمسمائة ألف درهم[1517]، لكل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية[1518].

وعليه، نرى أن المشرع الإماراتي قد وفق في تحديد الحد الأدنى والأقصى للغرامة، كما لم يشمل النص محل الحماية البيانات الحكومية فقط، بل شملت الحماية البيانات السرية الخاصة بالمنشأة المالية، والتجارية، والاقتصادية، فلقد أشار المشرع الإماراتي إلى ضرورة تقرير الحماية لهذه المنشآت ومساواتها مع الجهات الحكومية، نظراً إلى الطبيعة المالية والاقتصادية لهذه المنشآت والتي تستوجب حماية خاصة.

إلا أن أوجه القصور في القانون القطري تكمن في عدم تحديد الحد الأدنى لعقوبة الحبس والغرامة، إذ حدد المشرع الحد الأقصى لعقوبة الحبس التي لا تتجاوز الثلاث سنوات، كما منح المشرع للقاضي تحديد مقدار الغرامة بشرط ألا تتجاوز مبلغ (500,000) ريال قطري، وكان من الأفضل أن يتخذ المشرع القطري ما أتخذه المشرع الإماراتي، وبالتالي تكون عقوبة الحبس والغرامة كالتالي: "الحبس لمدة لا تقل عن سنة ولا تتجاوز الثلاث سنوات، والغرامة التي لا تقل عن (250,000) ريال قطري، ولا تتجاوز مبلغ (500,000) ريال قطري، وذلك لحماية الأجهزة الحكومية من جرائم التعدي، ولتقييد سلطة القاضي في تقرير عقوبة الغرامة حتى لا ينزل عن الحد الأدنى للغرامة.

بالإضافة إلى أن القانون القطري أقر الحماية الإلكترونية للدولة وأجهزتها الحكومية، ولم يشمل النص المؤسسات الخاصة ذات الميزانية المستقلة، كالبنوك الخاصة، والمنشآت المالية والتجارية، إذا تستوجب هذه القطاعات حماية خاصة مشددة من التعدي الإلكتروني شأنها شأن الجهات الحكومية، وذلك نظراً للأضرار والخسائر المالية التي قد تتعرض لها تلك المنشآت عند تعرضها للجريمة الإلكترونية، وبالتالي تؤثر الأضرار بشكل تبعي على الدولة، وعليه، نرى تعديل النص ليشمل الحماية لهذه المنشآت، كما فعل المشرع الإماراتي.

الفرع الثاني: عقوبة جريمة تجاوز الدخول المصرح به

جرم القانون القطري الدخول العمدي للموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية أو وسيلة تقنية المعلومات أو جزء منها أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك بأية وسيلة، وجعل عقوبة أي من تلك الأفعال الحبس لمدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين[1519].

ولقد انتهج المشرع الإماراتي مبدأ التنوع في مدة الحبس والغرامة أيضاً، على سبيل المثال، ما تنص عليه المادة (2) من القانون الإماراتي: "يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة".

من الملاحظ، أن المواد السابقة -في القانون القطري والمقارن- تتعلق بالحماية القانونية من جرائم التعدي على المواقع الإلكترونية أو النظام المعلوماتي، بشكل عام، إذا تتمثل هذه الحماية للأفراد أيضاً، وتتمثل صور التعدي في مجرد الدخول، أو تجاوز الدخول

1517 حازم الجمل، مرجع سابق، ص 48.

1518 المادة (4) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1519 المادة (3) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

المصرح به، أو الاستمرار في التواجد فيه بعد علمه بذلك، لكن يؤخذ على المشرع القطري، في أنه لم يحدد الحد الأدنى لعقوبة الحبس والغرامة كما حددها المشرع الإماراتي، إذا اتجه المشرع الإماراتي في الفقرة الثانية من المادة (2) إلى تقييد الحد الأدنى لعقوبة الحبس، بحيث لا تقل المدة عن ستة اشهر والغرامة التي تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين في الظروف المشددة للجريمة كما سنوضحها لاحقاً، وعليه نرى تعديل النص محل النقد، واتخاذ منهج المشرع الإماراتي في هذا الشأن.

الفرع الثالث: عقوبة جريمة الاعتراض غير القانوني

عاقب المشرع القطري على فعل الالتقاط أو الاعتراض أو التنصت العمدي، ودون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور، بتقرير عقوبة الحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (100,000) ريال قطري، أو بإحدى هاتين العقوبتين [1520]. كما سار المشرع الإماراتي على نفس اتجاه المشرع القطري، إذ يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط أو اعترض عمداً وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية[1521].

وعليه، نرى أن كل من المشرع القطري والإماراتي، قد نصوا على عقوبة جريمة الاعتراض القانوني، بالحبس والغرامة، أو إحدى هاتين العقوبتين، إذ أضافت هذه المادة حماية خاصة لبعض وسائل انتهاك الحق في الخصوصية، بالاطلاع على بيانات الغير من خلال الشبكة المعلوماتية، دون وجه حق، وتتمثل صور الاعتداء الإلكتروني في الاعتراض أو الالتقاط أو التنصت العمدي عبر الشبكة المعلوماتية.

المطلب الثاني: الظروف المشددة لجريمة التعدي الإلكتروني

نص المشرع القطري والإماراتي على الظروف المشددة لجريمة التعدي على الأنظمة المعلوماتية في حالات معينة بذاتها، ويقصد بالظروف المشددة تلك التي إذا ما اقترنت بالجريمة أو بالجاني شددت عقوبتها إلى أكثر من الحد الأعلى المقرر لها في القانون[1522].

الفرع لأول: الظروف المشددة لجريمة الدخول العمدي غير المصرح به

نلاحظ أن القانون القطري ضاعف عقوبة الدخول غير المشروع إلى النظام المعلوماتي للدولة وأجهزتها المنصوص عليها في القانون القطري، من الجنحة إلى الجناية لمدة لا تتجاوز ست سنوات، وضاعف الغرامة إلى مبلغ لا يتجاوز مليون ريال، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة[1523].

وقد قضت محكمة التمييز القطرية بحبس المتهم خمس سنوات، وفقاً لحكم المادة (2) من قانون مكافحة الجرائم الإلكترونية، والتي نصت على أن تضاعف العقوبة في حالة إذا ترتب على الدخول الغير مشروع الحصول على بيانات سرية بذاتها، وهذا ما قام به المطعون حيث إنه قام بنسخ البيانات الخاصة بالقصور الأميرية ومصروفاتها على فلاش ممورى لاستخدامها لغرضه الشخصي[1524].

1520 المادة (4) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1521 المادة (15) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1522 سيد حسن البغال، الظروف المشددة والمخففة في قانون العقوبات فقهاً وقضاءً، دار الفكر العربي، القاهرة، بدون سنة، ص 10.

1523 الفقرة الثانية من المادة (2) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1524 محكمة التمييز القطرية، الطعن رقم 203 لسنة 2017، الصادر بتاريخ 2017/12/04.

وبالمقارنة، رفع المشرع الإماراتي الحد الأدنى لعقوبة الدخول غير المشروع للنظام المعلوماتي الحكومي أو للمنشأة المالية أو التجارية أو الاقتصادية، بحيث لا تقل عقوبة السجن عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر[1525].

الفرع الثاني: الظروف المشددة لجريمة تجاوز الدخول المصرح به

نص القانون القطري على أن تُضاعف عقوبة الحبس التي لا تجاوز ثلاث سنوات، والغرامة التي لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية ماله أو القائم على إدارته[1526].

نرى أن المشرع القطري ضاعف العقوبة في حالة الدخول العمدي ودون وجه حق، بأي وسيلة إلى موقع إلكتروني أو نظام معلوماتي أو تجاوز الدخول المصرح به، أو استمر في التواجد في الموقع بعد علمه بأنه غير مصرح له بالدخول، بأن ضاعف العقوبة من جنحة الحبس التي لا تتجاوز الثلاث سنوات إلى جناية الحبس لمدة لا تتجاوز الست سنوات، ومضاعفة الغرامة من مبلغ الذي لا يزيد على خمسمائة ألف ريال، إلى مبلغ الغرامة الذي لا يجاوز مليون ريال قطري، أو بإحدى هاتين العقوبتين.

ولقد قيد القانون الإماراتي الحد الأدنى لعقوبة الحبس بمدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات [1527].

نخلص إلى أن المشرع القطري وجب عليه تحديد الحد الأدنى لعقوبة الحبس والغرامة في الظروف المشددة لجريمة التعدي الإلكتروني، سواء كان ذلك التعدي على الجهات الحكومية وغير الحكومية، أو الافراد، كما حددها المشرع الإماراتي، وعدم ترك السلطة التقديرية للحد الأدنى في يد القاضي، وذلك نظراً لجسامة فعل التعدي الإلكتروني والاثار المترتبة عليه، ولتحقيق الردع الخاص في نفس الجاني، وتحقيق أفضل حماية للنظام المعلوماتي من عمليات التعدي الإلكتروني.

المطلب الثالث: العقوبات التكميلية لجريمة التعدي الإلكتروني

العقوبات التكميلية هي العقوبات التي تتبع العقوبات الأصلية، غير أنها لا تلحق المحكوم عليه بقوة القانون بل يجب أن ينص عليها القاضي صراحة في حكمة [1528] وفيما يخص جريمة التعدي الإلكتروني على الأنظمة المعلوماتية، فأن العقوبة التكميلية تتمثل في:

الفرع الأول: المصادرة

1525 الفقرة الثانية من المادة (4) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1526 الفقرة الثانية من المادة (3) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1527 المادة (10) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1528 علي حسين خلف وسلطان عبدالقادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت،1982، ص797.

المصادرة هي "إجراء الهدف منه تمليك الدولة أشياء مضبوطة ذات صلة بالجريمة، قهراً على صاحبها، وبغير مقابل، ولا يجوز الحكم بها إلا على شخص ثبتت إدانته، وحكم عليه بعقوبة أصلية"[1529].

وعليه، نصت المادة (53) من القانون القطري محل الدراسة على أن: "مع عدم الإخلال بحقوق الغير حسن النية، يحكم في جميع الأحوال، فضلاً عن العقوبات المنصوص عليها في هذا القانون، بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها.

يتضح أن المشرع القطري عاقب على جريمة التعدي الإلكتروني بالمصادرة الوجوبية كعقوبة تكميلية، إذ نص القانون على ضرورة وجوبها، إذا وردت عبارة "تقضي المحكمة" ولم يترك المشرع أمر المصادرة متروك لتقدير القاضي، كما أن المحكمة ملزمة بأن تصدر حكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة الإلكترونية، وكذلك الأموال المتحصلة من جريمة التعدي الإلكتروني في النص المشار إليه أعلاه.

وبالنسبة للمشرع الإماراتي، فلقد نص على عقوبة المصادرة كتدبير عيني وقائي على الأشياء والأدوات التي استعملت في ارتكاب الجريمة، أو كانت محلاً للجريمة، أو الأشياء المضبوطة[1530]. إذ نص القانون على: "مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها"[1531].

الفرع الثاني: غلق المنشأة أو الموقع الإلكتروني

غلق المنشأة هو جزاء عيني، ينص عليه المشرع غالباً كعقوبة تكميلية، إلى جانب ما يقضى به من عقوبات أصلية أخرى[1532]. حيث نص المشرع القطري في المادة (53) على أن يحكم بإغلاق المحل أو حجب الوقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم، بحسب الأحوال، أما المشرع الإماراتي، فقد نصت المادة (41) من القانون محل الدراسة على أن يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة.

نرى أن كل من المشرعين القطري والإماراتي، اتجها إلى أن الحكم بأغلاق المنشأة أو حجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته الجريمة الإلكترونية، كعقوبة تكميلية لجريمة التعدي الإلكتروني، لكن المشرع الإماراتي تميز عن المشرع القطري في تحديد المدة الزمنية لحجب الموقع الإلكتروني، فقد يكون حجب كلياً أو مؤقتاً وذلك حسب الأحوال التي تقدرها المحكمة، وعليه نرى أن على المشرع القطري أن يحذو حذو المشرع الإماراتي بإضافة تعيين مدة حجب الموقع الإلكتروني كما نص عليها القانون الإماراتي.

الفرع الثالث: إبعاد الأجنبي

نص المشرع القطري على عقوبة الإبعاد للأجنبي كعقوبة تكميلية لجريمة التعدي الإلكتروني، إذ يجوز للمحكمة، في حالة الإدانة بإحدى الجرائم المنصوص عليها في هذا القانون، أن تحكم، بالإضافة إلى العقوبة المقررة، بإبعاد مرتكب الجريمة غير القطري من

1529 علي عبدالقادر القهوجي، الجرائم المتعلقة باستخدام البطاقات الممغنطة، مجلة الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، كلية الحقوق، بيروت، العدد 1، 2002، ص 97.

1530 حازم الجمل، مرجع سابق، ص 52.

1531 المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1532 محمود عبدالعزيز الشريف، مدى ملائمة الجزاءات الجنائية الاقتصادية في ظل السياسة الجنائية المعاصرة، النظرية العامة للجزاء الجنائي الاقتصادي، دار النهضة العربية، القاهرة، 2007، ص 103.

الدول[1533]. كما اتجه المشرع الإماراتي إلى ذات العقوبة، وقرر أن تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها[1534].

لقد جعل المشرع القطري عقوبة إبعاد الأجنبي –مرتكب جريمة التعدي الإلكتروني- جوازيه، إذ أن للقاضي السلطة التقديرية في الحكم بالإبعاد، أما المشرع الإماراتي جعل عقوبة الإبعاد وجوبية، لأنه نص على "تقضي المحكمة بالإبعاد في حالة الإدانة، بل ذهب المشرع الإماراتي إلى أبعد من ذلك في التشدد، بأن يكون الأبعاد بعد تنفيذ العقوبة المحكوم بها، أما المشرع القطري لم ينص على ذلك صراحة.

المطلب الرابع: حالات تخفيف العقوبة أو الإعفاء منها

ويقصد بالظروف المخففة الوقائع أو الصفات التي قد تقترن بشخص المجرم أو بشخص المجني عليه أو تقترن بالنشاط الإجرامي في حد ذاته، حيث ترك المشرع تقديرها للقاضي وخوله حق تخفيف العقوبة في الحدود التي رسمها له، والظروف المخففة للعقوبة تتمثل في ألا يوقع القاضي على الجاني العقوبة الأصلية للجريمة المرتكبة، بل يوقع عقوبة أخرى مخففة[1535].

إذ نصت المادة (54) من القانون القطري بشأن الجرائم الإلكترونية على أن يعفى من العقوبات المنصوص عليها في هذا القانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأية معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقضى بوقف تنفيذ العقوبة، إذا حصل الإبلاغ بعد علم السلطات المختصة، وأدى إلى ضبط باقي الجناة.

وعليه يجوز للمحكمة أن تمتنع عن النطق بالعقوبة بالنسبة إلى الجاني الذي بادر بإبلاغ السلطات المختصة عن الجريمة وعن الجناة الآخرين المتورطين فيها، وأن يتم هذا الإبلاغ قبل أن يتصل علم السلطات المختصة بالجريمة ومرتكبيها، بل ذهب المشرع إلى وقف تنفيذ العقوبة ولو حصل الإبلاغ بعد علم السلطات المختصة بذلك، شريطة أن يؤدي الإبلاغ إلى ضبط باقي الجناة المتورطين في جريمة الاعتداء الإلكتروني لتشجيع الجناة على الإبلاغ عن هذه الجريمة.

وفقاً لنص المادة (45) من القانون الإماراتي بشأن مكافحة جرائم تقنية المعلومات، فأن المحكمة تقضي، بناء على طلب من النائب العام، بتخفيف العقوبة أو بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكام هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم.

نخلص إلى أن المشرع القطري والإماراتي قد نصا على حالات الإعفاء من العقوبة، إذ تتمثل في حالة الإبلاغ عن الجريمة إلى السلطات المختصة، وسواء كان ذلك الإبلاغ قبل أو بعد علم السلطات المعنية، بشرط أن يؤدي الإبلاغ إلى ضبط باقي الجناة المتورطين، إلا أن المشرع القطري لم ينص صراحة على تخفيف العقوبة كما نص عليها المشرع الإماراتي، إذ نص القانون الإماراتي على حالة تخفيف العقوبة إذا كان من شأن الابلاغ عن الجرائم المتعلقة بأمن الدولة، وأدى هذا الابلاغ إلى القبض على الجناة.

1533 المادة (52) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

1534 المادة (42) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

1535 فهد حمد آل سنيد، الظروف القضائية المخففة للعقوبة في قانون العقوبات القطري: دراسة مقارنة بالتشريعين الأردني والمصري، رسالة ماجستير، جامعة عمان العربية للدراسات العليا، الأردن، يونيو 2017، ص 28.

الخاتمة

بعد أن تناولنا جريمة التعدي الالكتروني على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية في القانون القطري والمقارن، توصلنا إلى مجموعة من النتائج والتوصيات، والتي نأمل من المشرع القطري الأخذ بها، لتحقيق الحماية الجنائية الأفضل للحد من جرائم التعدي، والتي تتمثل في:

أولاً: النتائج:

1. المشرع القطري أورد تعريفاً خاصاً للجريمة الإلكترونية، ويقصد بها أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة. بينما لم يورد المشرع الإماراتي تعريفاً خاصاً بالجريمة الإلكترونية.
2. جرم المشرع القطري والإماراتي جريمة التعدي الإلكتروني، بصورها المتعددة، وذلك نظراً لأهمية توفير الحماية الجنائية من تلك الجرائم المستحدثة التي لا يمكن مواجهتها بالقوانين الجنائية التقليدية وحدها.
3. اتضح لنا أن صور جرائم التعدي الإلكتروني في التشريع القطري والإماراتي تتضمن ثلاثة جرائم وهي جريمة الدخول غير المصرح به، وجريمة تجاوز الدخول المصرح به أو البقاء غير المصرح به، وجريمة الالتقاط والاعتراض والتنصت على البيانات المرسلة إلكترونياً أو بيانات المرور.
4. نستنتج أن المشرع القطري والإماراتي أقرا عقوبتي الحبس والغرامة معاً في المادة (2)، كجزاء جنائي لصور التعدي على النظام الإلكتروني والمتمثلة في مجرد الدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة الحكومية، ويعد هذا التشدد في تطبيق كل من عقوبتي الحبس والغرامة من قبيل الحماية المشددة للأمن الإلكتروني للدولة وأجهزتها، والتي تستوجب طبيعة هذه الأنظمة التشدد في العقوبة.
5. حدد المشرع الإماراتي الحد الأدنى والأقصى للغرامة، كما لم يشمل النص محل الحماية البيانات الحكومية فقط، بل شملت الحماية البيانات السرية الخاصة بالمنشأة المالية، والتجارية، والاقتصادية.
6. لم يحدد المشرع القطري الحد الأدنى لعقوبة الحبس والغرامة، إذ حدد المشرع الحد الأقصى لعقوبة الحبس التي لا تتجاوز الثلاث سنوات، كما منح المشرع للقاضي تحديد مقدار الغرامة بشرط ألا تتجاوز مبلغ (500,000) ريال قطري.
7. أقر المشرع القطري الحماية الإلكترونية للدولة وأجهزتها الحكومية، ولم يشمل النص المؤسسات الخاصة ذات الميزانية المستقلة، كالبنوك الخاصة، والمنشآت المالية والتجارية.
8. جرم القانون القطري في المادة (3) الدخول العمدي للموقع الإلكتروني أو النظام المعلوماتي أو تقنية معلومات أو جزء منها أو تجاوز الدخول المصرح به، أو الاستمرار في التواجد فيه بعد علمه بذلك بأية وسيلة، وجعل عقوبة الحبس لمدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين.
9. عاقب المشرع الإماراتي بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة
10. عاقب المشرع القطري في المادة (4) على فعل الالتقاط أو الاعتراض أو التنصت العمدي، ودون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور، بتقرير عقوبة الحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على مائة ألف ريال، أو بإحدى هاتين العقوبتين.

11. سار المشرع الإماراتي على نفس اتجاه المشرع القطري، إذ يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط أو اعترض عمداً وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية.

12. القانون القطري ضاعف عقوبة جريمة التعدي الإلكتروني، إذا ترتب على ذلك الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة.

13. رفع المشرع الإماراتي الحد الأدنى لعقوبة الدخول غير المشروع للنظام المعلوماتي الحكومي أو للمنشأة المالية أو التجارية أو الاقتصادية، بحيث لا تقل عقوبة السجن عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

14. نص القانون القطري والإماراتي على العقوبات التكميلية لجريمة التعدي الإلكتروني، والمتمثلة في مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة أو الأموال المتحصلة منها على أن يحكم بإغلاق المحل أو حجب الوقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم، وإبعاد الأجنبي في حالة الإدانة.

15. قيد القانون الإماراتي الحد الأدنى لعقوبة الحبس بمدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات

16. اتجه المشرعين القطري والإماراتي إلى أن الحكم بإغلاق المنشأة أو حجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته الجريمة الإلكترونية، كعقوبة تكميلية لجريمة التعدي الإلكتروني، لكن المشرع الإماراتي تميز عن المشرع القطري في تحديد المدة الزمنية لحجب الموقع الإلكتروني، فقد يكون حجب كلياً أو مؤقتاً وذلك حسب الأحوال التي تقدرها المحكمة.

17. جعل المشرع القطري عقوبة إبعاد الأجنبي جوازيه، إذ أن للقاضي السلطة التقديرية في الحكم بالإبعاد، أما المشرع الإماراتي جعل عقوبة الإبعاد وجوبية، لأنه نص على "تقضي المحكمة بالإبعاد في حالة الإدانة

18. نص المشرعان القطري والإماراتي على حالات الإعفاء من العقوبة، إذ تتمثل في حالة الإبلاغ عن الجريمة إلى السلطات المختصة، وسواء كان ذلك الإبلاغ قبل أو بعد علم السلطات المعنية، بشرط أن يؤدي الإبلاغ إلى ضبط باقي الجناة المتورطين، إلا أن المشرع القطري لم ينص صراحة على تخفيف العقوبة كما نص عليها المشرع الإماراتي، إذ نص القانون الإماراتي على حالة تخفيف العقوبة إذا كان من شأن الابلاغ عن الجرائم المتعلقة بأمن الدولة، وأدى هذا الابلاغ إلى القبض على الجناة.

ثانياً: التوصيات

1. نقترح على المشرع القطري أن يضيف عبارة " أو بأي وسيلة أخرى" بعد عبارة (كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات) الواردة في المواد (2و4) محل البحث، لتشمل الحماية الجنائية المواقع الإلكترونية والنظم المعلوماتية من جرائم التعدي الإلكتروني، وذلك نظراً للتقدم التكنولوجي الذي نشهده في عصرنا

الحالي، إذ أنه من الممكن أن تكتشف وسيلة أخرى يتم بواسطتها الاعتداء على النظام المعلوماتي غير وسيلة الإنترنت أو الوسائل التقنية.

2. نوصي بتحديد الحد الأدنى لعقوبتي الحبس والغرامة المنصوص عليها في المادة (2) من القانون القطري محل الدراسة، ليكون النص كالتالي: " يعاقب بالحبس لمدة لا تقل عن سنة ولا تتجاوز الثلاث سنوات غرامة لا تقل عن مائتين وخمسين ألف ريال ولا تتجاوز مبلغ خمسمائة ألف ريال، وذلك لحماية الأجهزة الحكومية من جرائم التعدي، ولتقييد سلطة القاضي في تقرير عقوبة الغرامة حتى لا ينزل عن الحد الأدنى للغرامة.

3. تعديل نص المادة (2) من القانون المشار إليه، ليشمل النص الحماية من الاعتداء الالكتروني على المؤسسات الخاصة ذات الميزانية المستقلة، كالبنوك الخاصة، والمنشآت المالية والتجارية والاقتصادية، إذا تستوجب هذه القطاعات حماية خاصة من التعدي الالكتروني شأنها شأن الجهات الحكومية.

4. نقترح أيضاً، بوجوب تحديد الحد الأدنى للعقوبة والغرامة في الظروف المشددة للجريمة التعدي الالكتروني، في كل من المادتين (2) و(3) في القانون القطري سواء كان ذلك التعدي على الجهات الحكومية وغير الحكومية، أو الافراد، كما حددها المشرع الإماراتي، وعدم ترك السلطة التقديرية للحد الادنى في يد القاضي، وذلك نظراً لجسامة فعل التعدي الالكتروني والاثار المترتبة عليه، ولتحقيق الردع الخاص في نفس الجاني، وتحقيق أفضل حماية النظام المعلوماتي من عمليات التعدي.

5. نرى أن على المشرع القطري أن يقوم بتعيين مدة حجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته الجريمة الإلكترونية كما نص عليها القانون الإماراتي، كعقوبة تكميلية لجريمة التعدي الإلكتروني، ليكون حجب كلياً أو مؤقتاً وذلك حسب الأحوال التي تقدرها المحكمة.

المراجع والمصادر

أولاً: الكتب:

1. أحمد عوض بلال، محاضرات في الجزاء الجنائي، دار النهضة العربية، القاهرة، 2001.
2. أوزدن حسين دزه يي، جريمة غسل الأموال، ط1، المكتب الجامعي الحديث، الإسكندرية، مصر، 2012.
3. حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، ط1، دار الفكر والقانون، مصر، 2015.
4. سيد حسن البغال، الظروف المشددة والمخففة في قانون العقوبات فقهاً وقضاءً، دار الفكر العربي، القاهرة، بدون سنة.
5. علي حسين خلف وسلطان عبدالقادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت،1982.
6. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، مصر، 2013.
7. محمد عيد الغريب، شرح قانون العقوبات القسم العام، النظرية العامة للعقوبة والتدابير الاحترازية، بدون دار نشر، القاهرة، 2000.
8. محمد كمال الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية: دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، مصر، 2015.
9. محمود عبدالعزيز الشريف، مدى ملائمة الجزاءات الجنائية الاقتصادية في ظل السياسة الجنائية المعاصرة، النظرية العامة للجزاء الجنائي الاقتصادي، دار النهضة العربية، القاهرة، 2007.

10. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية،2005.

رابعاً: البحوث والمقالات:

1. عبد الإله محمد النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، وزارة العدل، قطر، العدد1، 2016.
2. علي عبدالقادر القهوجي، الجرائم المتعلقة باستخدام البطاقات الممغنطة، مجلة الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، كلية الحقوق، بيروت، العدد 1، 2002.

خامساً: الرسائل الجامعية:

1. شيماء عبدالغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية دراسة مقارنة بين النظامين اللاتيني والأنجلو أمريكي، رسالة دكتوراه، جامعة المنصورة، مصر، 2005.
2. فهد حمد آل سنيد، الظروف القضائية المخففة للعقوبة في قانون العقوبات القطري: دراسة مقارنة بالتشريعين الأردني والمصري، رسالة ماجستير، جامعة عمان العربية للدراسات العليا، الأردن، يونيو2017.

سادساً: التشريعات:

1. القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.

المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.