الضوابط القانونية للمحتوى الرقمي باستخدام الذكاء الاصطناعي

"دراسة مقارنة"

بين التشريع القطري والتشريع المصري

د. وائل خالد محمد قاسم

حاصل على الدكتوراه في القانون العام- كلية الحقوق- جامعة أسيوط

(ISSN: 2537- 0758)

الضوابط القانونية للمحتوى الرقمي باستخدام الذكاء الاصطناعي "دراسة مقارنة" بين التشريع القطري والتشريع المصري

د. وائل خالد محمد قاسم

الملخص:

في ظل الثورة الرقمية المتسارعة، أصبح المحتوى الرقمي هدفًا رئيسيًا للجرائم الإلكترونية التي تتجاوز مجرد اختراق الأنظمة وسرقة البيانات لتشمل التلاعب بالمحتوى نفسه. أدرك المشرع القطري خطورة هذه الظاهرة وسعى لوضع إطار قانوني لحماية المحتوى الرقمي. يهدف هذا البحث إلى تسليط الضوء على فعالية التشريعات القطرية، وخاصة قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤، في التصدي لهذه الجرائم. يتناول البحث مفهوم هذه الجرائم وأركانها وصور التجريم والعقوبات المقررة لها. كما يقيم مدى انسجام التشريع القطري مع الاتفاقيات الدولية ذات الصلة. ويكشف البحث عن التحديات التي تواجه التطبيق العملي لهذه النصوص القانونية.

In light of the accelerating digital revolution, digital content has become a primary target for cybercrimes that go beyond mere system breaches and data theft to include manipulation of the content itself. The Qatari legislator has recognized the seriousness of this phenomenon and has sought to establish a legal framework to protect digital content. This research aims to shed light on the effectiveness of Qatari legislation, particularly Law No. (14) of 2014 on Combating Cybercrimes, in addressing these crimes. The research discusses the concept of these crimes, their pillars, forms of criminalization, and prescribed penalties. It also evaluates the extent of consistency between Qatari legislation and relevant international agreements. The research also reveals the challenges facing the practical application of these legal texts.

المقدمة

في ظل الثورة الرقمية المتسارعة التي يشهدها العالم، أضحى المحتوى الرقمي جزءً أساسيًا من الحياة اليومية للأفراد والمؤسسات على حد سواء، مما جعله عرضة لتهديدات متزايدة من قبل مرتكبي الجرائم الإلكترونية، ولم تعد هذه الجرائم تقتصر على اختراق الأنظمة وسرقة البيانات، بل امتدت لتشمل التلاعب بالمحتوى الرقمي، سواء من خلال حذفه أو تغييره أو تزويده، بما يخل بمصداقية المعلومات ويهدد الثقة في البيئة الرقمية.

فالأمن الاجتماعي ضرورة من ضرورات بقاء وتطور المجتمعات الإنسانية للوقاية من الجريمة والحد من انتشارها، فالجرائم الإلكترونية تعد من أخطر الظواهر الاجتماعية وأشدها تأثيرًا على المجتمع، الأمر الذي يترتب عليه تنامي بعض المظاهر والسلوكيات السلبية والأخلاقية والفكرية وغيرها لأفراد المجتمع.

وقد أدرك المشرع القطري خطورة هذه الظاهرة فسعى إلى وضع إطار قانوني يهدف إلى حماية المحتوى الرقمي عن الجرائم الإلكترونية، وذلك من خلال سن تشريعات متخصصة أبرزها قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤ الذي يعد من القوانين المتقدمة في المنطقة من حيث شمولية وتغطيته لمختلف صور الجرائم الرقمية.

أهداف البحث:

يهدف هذا البحث إلى تسليط الضوء على الإطار القانوني الذي وضعه التشريع القطري لمواجهة الجرائم الإلكترونية التي تستهدف المحتوى الرقمي من حيث المفهوم والأركان وصور التجريم والعقوبات مع بيان مدى فعالية هذه التشريعات في التصدي لهذا النوع من الجرائم، ومدى انسجامها مع الاتفاقيات الدولية ذات الصلة.

إشكالية البحث:

بالرغم من التطور التشريعي الذي شهده القانون القطري في مجال مكافحة الجرائم الإلكترونية لا تزال الجرائم التي تستهدف المحتوى الرقمي يثير العديد من التساؤلات القانونية سواء من حيث تحديد طبيعتها، أو تكييفها القانوني، أو حدود الحماية التي يقرها القانون لهذا النوع من المحتوى كما تبرز إشكالية الموازنة بين حماية المحتوى الرقمي وحرية التعبير في الفضاء الإلكتروني، بالإضافة إلى

(ISSN: 2537- 0758)

التحديات التقنية والقانونية التي تواجه إنفاذ النصوص القانونية في الواقع العملي ومن هنا تتمثل الإشكالية الرئيسية لهذا البحث في:

إلى أي مدى وفرت التشريعات القطرية وخاصة قانون مكافحة الجرائم الإلكترونية رقم ١٤ لسنة ٢٠١٤، حماية فعالة للمحتوي الرقمي من الجرائم الإلكترونية، وما هي أوجه القصور أو التحديات التي تعترض التطبيق العملي لتلك النصوص؟

خطة البحث:

- المقدمة
- أهداف البحث
- إشكالية البحث
- **المبحث التمهيدي: ماهية الجريمة الإلكترونية**
- المطلب الأول: مفهوم الجريمة الإلكترونية وخصائصها
- المطلب الثاني: أسباب الجريمة الإلكترونية
- المطلب الثالث: أنواع الجرائم الإلكترونية
- **المبحث الأول: نطاق الجريمة الإلكترونية وأركانها وعقوبتها**
- المطلب الأول: نطاق الجريمة الإلكترونية
- المطلب الثاني: أركان الجريمة الإلكترونية التي تستهدف المحتوى الرقمي
- المطلب الثالث: العقوبة
- **المبحث الثاني: الجهود التشريعية المبذولة لمكافحة الجريمة الإلكترونية**
- المطلب الأول: الجهود التشريعية الأوروبية
- المطلب الثاني: الجهود التشريعية العربية
- المطلب الثالث: جهود دولة قطر لمواجهة الجريمة الإلكترونية
- **الخاتمة**
- **النتائج**
- **التوصيات**

المبحث التمهيدي
ماهية الجريمة الإلكترونية

أصبحت الأجهزة الإلكترونية جزءً مهماً في الحياة اليومية للإنسان: الحواسيب بأنواعها، وأجهزة الاتصالات على تنوعها التي يُعدها الكثيرون إحدى أعمدة الحضارة التي نعيش فيها اليوم، والتطور الذي نشهد ومنها كذلك، أجهزة البث والاستقبال الفضائي وآلات التصوير وأجهزة التسجيل الصوتي وغيرها. ولا شك أن تلك الأجهزة تتكامل فيما بينها في الوظيفة، فضلاً عن التناسق التام في الصناعة حيث أُدمجت آلات التصوير مع الحواسيب والهواتف النقالة بشكل واسع. وترافق مع هذا التطور ظهور جرائم الكمبيوتر والإنترنت، وشاع مصطلح الجريمة الإلكترونية، أو جرائم التقنية العالية، وبدأت الدول المتقدمة بسن التشريعات والقوانين التي تكفل مواجهة هذه الجرائم.

ولا مناص من الاعتراف بأن للجرائم الإلكترونية خصوصية تميزها عن غيرها من الجرائم، ففي هذه الجرائم يلتقي القانون مع علم نظم المعلومات، ويندمجان مع بعضهما البعض مما يثير الصعاب الكبيرة أمام رجل القانون المنفذ الأحكام فنية بحتة، وأمام خبراء الحاسوب الذين لا يلمون بطبيعة الحال بالأحكام والقواعد القانونية، وهذا ما حداً بالعديد من التشريعات الخليجية إلى اللجوء لوضع عدد كبير من التعريفات في بداية التشريع، سعياً منهم للتغلب على هذه النقطة، ومحاولة شرحها لمنفذي القانون وهيئاته المختلفة.

وعلى هذا الأساس نقسم ذلك المبحث إلى المطالب التالية:

المطلب الأول
مفهوم الجريمة الإلكترونية وخصائصها

في بادئ الأمر لا بد أن نشير إلى أنه لا يوجد مصطلح موحد، بخصوص توصيف الاعتداءات التي تنال النظام المعلوماتي، ذلك أن من الصعب عزل المكونات المادية للنظام المعلوماتي عن مكوناته غير المادية[1]، والتي تتمثل في البرامج والمعلومات التي يتم تخزينها. ومن المصطلحات التي تطلق على هذه

[1] محمد حماد مرهج الهيئتي، الجريمة المعلوماتية نماذج من تطبيقها دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، مصر، ٢٠١٤، ص ٤٣.

(ISSN: 2537- 0758)

النوعية من الاعتداءات نذكر منها على سبيل المثال لا الحصر (جرائم الكمبيوتر، مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية، جرائم تقنية المعلومات، جرائم إساءة استخدام الحاسب، جرائم التقنية العالية، جرائم المعلوماتية، وغيرها)[٢]. وعموماً تعرف الجريمة بأنها فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازيًا.

وتجد الإشارة إلى أن وضع تعريف محدد للجريمة الإلكترونية ليس بالأمر السهل، فمن غير الممكن وضع تعريف جامع مانع لها نظراً لطبيعتها المعقدة، ومع ذلك توجد محاولات التعريف الجريمة الإلكترونية نشير إلى بعض منها على النحو الوارد أدناه:

أ. من حيث وسيلة ارتكاب الجريمة

هناك جانب من الفقه عرف الجريمة الإلكترونية على أنها: "كل أنواع السلوك غير المشروع الذي يرتكب عن طريق الحاسب الآلي أو بمساعدته أو أن تكون أداة رئيسة في ارتكابه أو له دوراً هاماً إيجابياً في هذا الارتكاب".

ب. من حيث موضوع ارتكاب الجريمة

هناك من يرى بأن الجريمة الإلكترونية هي: "كل فعل متعمد أيًا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه"[٣].

ج. من حيث وسيلة ارتكابها وموضوعها

يرى جانب من الفقه بأن يمكن تعريف الجريمة الإلكترونية على أنها: "أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسب".

د. من حيث سمات الشخصية.

اتجه جانبًا من الفقه في تعريف الجريمة الإلكترونية بأنها: "الجريمة التي يرتكبها شخصًا ما بتقنيات الحاسب ونظم المعلومات".

---

[٢] هلالي عبداللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة، ص ١١٤.

[٣] محمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، مصر، ٢٠١٥، ص ٣٢.

ولقد تعددت تعريفات الجرائم الإلكترونية نذكر منها الآتي:

وتعرف الجرائم الإلكترونية بأنها: "ذلك النشاط الإجرامي الذي يتم ارتكابه عن طريق استخدام الإنترنت".

وهي: "ذلك النوع من الجرائم الذي يهدف إلى التحرش أو إيذاء الآخرين عن طريق توظيف تكنولوجيا المعلومات والاتصالات، كالكمبيوتر والهواتف الخلوية والكمبيوترات اللوحية.. وغيرها من التكنولوجيا الحديثة".

وهي الاعتداء غير القانوني الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الربح.

وهي أيضاً: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".

عرفت بأنها: "الممارسات التي توقع ضد فرد أو مجموعة مع توفر باعث إجرامي بهدف التسبب بالأذى لسمعة الضحية عمداً، أو إلحاق الضرر النفسي والبدني به سواء أكان ذلك بأسلوب مباشر أو غير مباشر بالاستعانة بشبكات الاتصال الحديثة كالانترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحادثة، والهواتف المحمولة".

وعرفت بأنها "كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها".

أما بالنسبة لموقف المشرع القطري من تعريف الجريمة الإلكترونية، فقد عرف المشرع القطري الجريمة الإلكترونية بأنها: "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي، أو الشبكة المعلوماتية، بطريقة غير مشروعة بما يخالف أحكام القانون".

ويعد الفعل غير مشروع إذا خالف أحكام القانون، وتشمل أحكام القانون أحكام قانون مكافحة الجرائم الإلكترونية وكذلك أحكام أي قانون آخر ينص على جريمة إلكترونية مثل قانون العقوبات الصادر بالقانون رقم (١١) لسنة ٢٠٠٤.

وتقنية المعلومات هي أي وسيلة مادية أو غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقًا للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع

(ISSN: 2537- 0758)

المدخلات والمخرجات المرتبطة بها سلكيًا أو لاسلكيًا في نظام معلوماتي أو شبكة معلوماتية.

ومن جانبنا نؤيد عدم ادراج التشريعات تعريفاً للجريمة الإلكترونية، ذلك لأن لا يوجد تعريف جامع مانع لهذه النوعية من الجرائم، وهذا يرجع إلى تنوع الوسائل التي ترتكب بها هذه الجرائم وسرعة تطورها، حيث نرى الاكتفاء بتجريم الأفعال التي تشكل جريمة إلكترونية دون النص على تعريف للجريمة الإلكترونية على وجه التحديد[٤].

رأي الباحث:

وبعد الاطلاع على التعريفات المختلفة وبغية أن يكون التعريف جامعاً مانعاً لكل أوجه النشاط الإجرامي الإلكتروني، فإن الدراسة ترى أن الجريمة الإلكترونية هي نشاط غير مشروع، يتخذ نظم المعلومات ووسائل الاتصال الحديث أداة له، يصدر عن إرادة آثمة ويقرر له القانون عقوبة أو تدبير احترازي.

خصائص الجريمة الإلكترونية:

للجريمة الإلكترونية خصائص متعددة نجملها فيما يلي:

- من السهل ارتكابها، وذلك لاستخدام وسائل ذات طابع تقني.
- من السهل إخفاء معالم الجريمة، وفي ذات الوقت من الصعب ملاحقة مرتكبيها.
- يتطلب ارتكاب هذه النوعية من الجرائم قدراً من المعرفة في الأنظمة المعلوماتية.
- السرعة في ارتكاب الجريمة الإلكترونية لاعتمادها على الوسائل الحديثة.
- تؤثر هذه الجريمة على اقتصاد الدول.

جريمة تتسم بالغموض، نظراً لصعوبة إثباتها والتحقيق فيها بعكس الجرائم التقليدية.

- جريمة تكون مواجهتها بنفس أساليب وإجراءات ارتكابها حتى وإن كانت غير مشروعة.

---

[٤] راجع المادة (١) من قانون مكافحة الجرائم الإلكترونية القطري الصادر بالقانون رقم (١٤) لسنة ٢٠١٤.

- عولمة هذه الجرائم التي تؤدي إلى التحرك الدولي نحو مواجهتها[٥].

ومن أهم الخصائص التي تتسم بها الجريمة الإلكترونية هي أنها جريمة عابرة للحدود، ومكافحتها لا يكون إلا بتضافر الجهود الدولية وتعاونها، من خلال الاتفاقيات الدولية التي لن يكون لها فعالية على أرض الواقع إلا بتنفيذها، والتعامل معها بجدية تامة دون أن يشكل الجانب السياسي عائق أمام تقديم المساعدة.

المطلب الثاني
أسباب الجريمة الإلكترونية

إن موضوع السبب الذي يدفع لارتكاب الجريمة ليس من المواضيع ذات الأهمية في عالم القانون، فالسبب أو الباعث أو الدافع على ارتكاب الجريمة ليس عنصراً فيها، كما أن القاضي لا يعتد به في نطاق التجريم، فالدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانوني الجنائي، تتصل بما يعرف بالقصد في الجريمة، وهي مسألة تثير جدلاً فقهياً وقضائياً واسعاً، ذلك أن: "القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي وأن الباعث لا أثر له في وجود القصد الجنائي"، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية.

ولذلك فإن سبب ارتكاب الجريمة أو الباعث عليها هو: "العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام، أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات، أما الغاية، فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام أو سلب المجني عليه في جريمة القتل".

والأصل أن الباعث والغاية ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين، علم الجاني بعناصر الجريمة، واتجاه إرادته إلى تحقيق هذه العناصر أو إلى قبولها، ولا تأثير للباعث أو الغاية على قيام الجريمة أو العقاب

---

[٥] عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والانترنت (الجرائم الالكترونية): دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محلياً وعربياً ودولياً، منشورات الحلبي الحقوقية، بيروت، ٢٠١٧، ص ٣١-٣٣.

(ISSN: 2537- 0758)

عليها، "فالجريمة تقوم بتحقق عناصرها سواء أكان الباعث نبيلاً أم رزيلًا وسواء أكانت الغاية شريفة أم دنيئة. وإذا كانت القاعدة أن الباعث أو الغاية لا أثر لهما على قيام الجريمة، فإن القانون يبني عليهما في بعض الأحيان أهمية قانونية خاصة"، إذ قد: "يهتم القانون بالباعث فيشترط توافره على نحو معين في بعض الجرائم، وفي هذه الحالة يدخل الباعث في عناصر القصد الجنائي ويسمى بالقصد الخاص ويتأثر القاضي في تقدير العقوبة بالباعث الذي دفع الجاني إلى ارتكاب الجريمة، فالباعث هنا هو عنصر في الخطورة الإجرامية للجاني".

ويرى البعض في معرض تحديد الهدف أو الدافع على ارتكاب جرائم الحاسوب تستهدف أكثر الجرائم المعلوماتية إدخال تعديل على عناصر الذمة المالية، ويكون الطمع الذي يشبعه الاستيلاء على المال دافعها، وبريق المكسب السريع محرك مرتكبها، وقد ترتكب أحياناً لمجرد قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، أو بدافع الانتقام من رب العمل أو أحد الزملاء. وفي هذا السياق فإن دوافع ارتكاب جرائم الحاسوب، ويعبر عنها بالأسباب الرئيسة الظاهرة الغش المعلوماتي، تتمثل بالشغف بالإلكترونيات، والسعي إلى الربح، والدوافع الشخصية أو المؤثرات الخارجية، والأسباب الخاصة بالمنشأة.

ويمكننا بيان الدوافع التالية التي يتمثل بعضها بالباعث للجريمة وفق التحديد السابق في حين يمثل بعضها غاية مرتكب الفعل:

أولاً: السعي إلى تحقيق الكسب المالي

حقيقة الأمر أن إشباع غريزة حب التملك والحصول على المال بأقصر الطرائق وأسهلها، السبب الرئيس للعديد من الجرائم، ومنها الجرائم الإلكترونية، حيث أشارت إحدى المحلات المتخصصة في الأمن المعلوماتي securite informatique إلى أن الرغبة في تحقيق الشراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت إلى أن ٤٣٪ من حالات الغش المعلن عنها قد بُوشرت من أجل اختلاس الأموال و٢٣٪ من أجل سرقة المعلومات، و١٩% أفعال إتلاف، و١٥% سرقة وقت الآلة؛ أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية[٦].

[٦] انظر في ذلك: عبدالعال الديري، الجريمة المعلوماتية: تعريفها، أسبابها، خصائصها، دراسة منشورة على موقع المركز العربي الأبحاث القضاء الإلكتروني، الأحد ١٣ يناير ٢٠١٣، ويمكن الوصول لهذه الدراسة عبر الرابط التالي: http://accronline com/article_detail.aspx?id=7509

ثانياً: التحدي وإظهار البراعة

يميل مرتكبو هذه الجرائم إلى: "إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم (شغف الآلة) يحاولون إيجاد، وغالباً ما يجدون الوسيلة إلى تحطيمها (والصواب التفوق عليها)، ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي جرائم الحاسوب، الذين يمضون وقتاً طويلاً أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات، ولإظهار تفوقهم على وسائل التقنية، ولا بد أن نشير هنا إلى أن هذا الدافع (مجرد قهر النظام) دفع بالعديد من الدارسين والفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الذي يتمثل باعثهم بإظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة. هذه أبرز الدوافع إلى ارتكاب جرائم الحاسوب، وهذا لا يعني توقفها عند هذه الدوافع، إذ تنطوي النفس الإنسانية على بواعث نفسية متعددة ونتجه الإرادة البشرية إلى تحقيق غايات متناهية، فقد تبعث على ارتكاب الجريمة مشاعر الحقد والكراهية، أو يحركها شعور الفاعل مجنون العظمة، أو كسب المنافسة التجارية أو الصناعية عبر التحسس على مقدرات الغير، أو استخدام النظام لمصالح وأغراض شخصية أو غير ذلك.

المطلب الثالث
أنواع الجرائم الإلكترونية

يمكن تقسيم تلك الجرائم إلى قسمين:

القسم الأول: وينتمي إلى الجرائم التي يتم استخدام الكمبيوتر كأدوات التنفيذ والقيام بالجرائم الإلكترونية

- وهي تنتمي إلى الجرائم المادية مثل استخدام الأطفال في عرض المواد الإباحية من خلال عرض كتب ونصوص أو مواد مرئية تحتوي على مواد مخلة، الغرض منها إثارة الرغبات الجنسية لدي الآخرين من خلال عرض المواد غير الأخلاقية المتعلقة بالأطفال.
- التحرش الإلكتروني بالغير من خلال إرسال رسائل إلكترونية إلى الغير والغرض منها التخويف والتهديد، ويتنوع هذا التحرش الإلكتروني فقد يكون تحرشًا جنسيًا أو دينيًا أو غيرها من الأمور التي تسعى إلى مضايقة وإخافة الغير.

(ISSN: 2537- 0758)

- الاحتيال على الآخرين من خلال الهويات المزيفة التي يكون الغرض الرئيسي منها استنزاف وسرقة أموال الغير.
- انتهاك الملكية الفكرية للغير من خلال عرض المنتجات الفكرية باسم مغاير لاسم المؤلف الحقيقي.
- تشويه السمعة وهو نوع من الجرائم الإلكترونية يسعى القائم على تلك الجرائم إلى تحقيقها من خلال نشر بعض التعليقات أو الصور التي تعمل على إهانة الطرف الآخر، مما يجعله في حاله اضطراب أو قلق ويؤدي به الحال إلى الانعزال عن الأسرة والأصدقاء.

القسم الثاني: وينتمي إلى الجرائم التي يكون فيها الكمبيوتر هو الهدف الذي يسعى إليه مرتكبو الجرائم الإلكترونية

هناك نوعية جديدة من الجرائم والمرتبطة بشكل أساسي بالكمبيوتر والإنترنت على سبيل المثال القرصنة والاستخدام الغير مرخص للبرامج وتطبيقات الكمبيوتر والقيام بنشر الفيروسات الضارة بأجهزة الآخرين، أو التجسس على محادثات الآخرين على الإنترنت وغيرها من السلوكيات غير اللائقة والتي تضر بالغير معنويًا وماديًا وهي:

١. **القرصنة الرقمية:** أن تطوير الكمبيوتر أدى إلى الانتشار الواسع استخدام الإنترنت، والذي سمح بتبادل المعلومات بين الناس مما أدي لاحقا إلى بعض السلوكيات الإجرامية من بينها القرصنة الرقمية.
٢. **التدمير المتعمد:** ويقصد به استخدام الإنترنت للولوج إلى الشركات والمنظمات ومن ثم القيام بمسح أو نسخ بعض المعلومات الهامة التي تضر بالمنظمة وبعملائها.
٣. **الرسائل الضارة:** وهو يعتبر من أهم أشكال الجرائم الإلكترونية وأكثرها انتشاراً والتي يمكن من خلالها اختراق كمبيوتر الضحية عن طريق تلك الرسائل التي تكون في ظاهرها أنها رسائل إعلانية وعند القيام بفتحها يتم إصابة كمبيوتر الضحية بزرع الفيروسات أو برامج التجسس.

المبحث الأول
نطاق الجريمة الإلكترونية وأركانها وعقوبتها

تمهيد وتقسيم:

كما أسلف القول أنه يقصد بالجريمة الإلكترونية التي تستهدف المحتوى الرقمي كل فعل غير مشروع يتم عبر الوسائل الإلكترونية أو التقنية، ويستهدف التلاعب أو الإضرار بالمحتوى الرقمي سواء بحذفه أو تعديله أو نسخه أو نشره دون إذن ولقد نظم القانون القطري هذه الأفعال من خلال قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤ والذي شمل عدداً من الجرائم.

وعلى هذا الأساس نقسم ذلك المبحث إلى المطالب التالية:

المطلب الأول: نطاق الجريمة الإلكترونية التي تستهدف المحتوى الرقمي

المطلب الثاني: أركان الجريمة الإلكترونية

المطلب الثالث: عقوبة الجريمة الإلكترونية

المطلب الأول
نطاق الجريمة الإلكترونية

في التشريع القطري تحظر الجرائم الإلكترونية التي تستهدف المحتوى الرقمي باهتمام خاص حيث يتم تنظيمها بموجب قانون مكافحة الجرائم الإلكترونية رقم ١٤ لسنة ٢٠١٤ إضافة إلى قوانين أخرى مثل قانون حماية خصوصية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦.

أهم الجرائم الإلكترونية التي تستهدف المحتوى الرقمي

أولاً: جرائم اختراق الأنظمة والتلاعب بالمحتوى الرقمي

حيث يجرم القانون الوصول غير المشرع إلى الأنظمة الإلكترونية بقصد تعديل أو حذف أو تشويه البيانات الرقمية

ثانياً: نشر أو تزييف المحتوى الرقمي

يعاقب القانون القطري رقم ١٤ لسنة ٢٠١٤ الخاصة بالجرائم الإلكترونية على نشر أخبار أو بيانات مزيفة عبر الإنترنت بقصد تضليل الجمهور أو الإضرار بالمصالح العامة، ويشمل ذلك إنتاج أو ترويج محتوي غير صحيح عبر وسائل التواصل الاجتماعي والمواقع الإلكترونية.

(ISSN: 2537- 0758)

ثالثاً: الاعتداء على حقوق الملكية الفكرية الرقمية

حيث يجرم القانون نسخ أو إعادة نشر المحتوى الرقمي المحمي دون إذن مثل البرامج الإلكترونية والمقالات والأعمال الفنية الرقمية.

رابعا: الاحتيال الرقمي والتزوير الإلكتروني

يعاقب على تزوير الوثائق أو البيانات الرقمية بقصد الاحتيال أو انتحال الصفة ويشمل ذلك التلاعب بالقوانين الرقمية أو الشهادات الإلكترونية أو الهويات الرقمية.

خامسا: الجرائم المتعلقة بالخصوصية وحماية البيانات الرقمية

يمنع جمع أو نشر بيانات شخصية دون موافقة أصحابها خاصة إذا كان ذلك يسبب ضررًا حيث يشمل ذلك اختراق الحسابات الشخصية أو تسريب المعلومات المصرفية أو الصور الخاصة.

وفي النظام القضائي القطري تم التعامل مع العديد من القضايا المتعلقة بالجرائم الإلكترونية التي تستهدف المحتوى الرقمي وفيما يلي بعض الأمثلة على هذه القضايا والأحكام الصادرة فيها:

١- قضية انتحال الهوية عبر الإنترنت

- **الوقائع:** حيث قام أحد الأفراد باستخدام الشبكة المعلوماتية لانتحال هوية شخص آخر بهدف الاستيلاء على أمواله.
- **الحكم:** حكم على المتهم بالحبس لمدة لا تتجاوز ثلاث سنوات وبغرامة لا تزيد على ١٠٠٠٠٠ ريال قطري أو بإحدى هاتين العقوبتين وفقا للمادة (١١) من قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤.

٢- قضية نشر أخبار وصور تمس خصوصية المجني عليها

- **الوقائع:** قام المتهم بنشر أخبار وصور عبر الإنترنت تمس حياة المجني عليها الخاصة واستمر في ذلك حتى بعد تنازلها عن القضية.
- **الحكم:** أكدت محكمة التمييز أن الجرائم الإلكترونية المتعلقة بنشر أخبار وصور تمس حياة الأفراد الخاصة لا يجوز التصالح فيها وأعادت النظر في القضية لإصدار الحكم المناسب.

ويبرر هذا الحكم التزام القضاء القطري بتطبيق قانون مكافحة الجرائم الإلكترونية رقم ١٤ لسنة ٢٠١٤ وحماية حقوق الأفراد في القضاء الرقمي، ولكن التساؤل الذي

يثور هنا ما هي إجراءات التفتيش والضبط في الجرائم الإلكترونية في التشريع القطري؟[٧]

يجوز تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة. طبقًا لنص (المادة (١٤) من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية. والنيابة العامة هي الجهة الأصيلة المختصة بالتفتيش.

ويجوز للنيابة العامة ندب أحد مأموري الضبط القضائي للقيام بالتفتيش. طبقًا لنص المادة (١٤) من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية، ويجب أن يكون أمر التفتيش مسببًا ومحدداً من حيث نطاقه الزمني والمكاني والأشخاص المشمولين بالتفتيش وكذلك الأشياء المراد التفتيش عنها أو تفتيشها.

ويجوز تجديد أمر التفتيش أكثر من مرة ما دامت مبررات هذا الإجراء قائمة. وطبقا لنص المادة (١٤) من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية، وإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.

المطلب الثاني

أركان الجريمة الإلكترونية التي تستهدف المحتوى الرقمي

تتكون هذه الجريمة من ثلاثة أركان رئيسة على النحو التالي:

أولاً: الركن القانوني

وهو وجود نص قانوني يجرم الفعل المرتكب وقد تضمن قانون مكافحة الجرائم الإلكترونية القطري عدة نصوص تجرم الأفعال التي تستهدف المحتوى الرقمي مثل المادة (٣) والتي تجرم الدخول غير المشروع إلى نظام معلوماتي وتعديل أو حذف أو إفشاء البيانات. وأيضاً المادة (٦) حيث تجرم تزوير أو تقليد مستندات إلكترونية أو محتوي رقمي. والمادة (٨) من ذات القانون تجرم نشر أو إعادة نشر محتوي غير مشروع (كالصور أو البيانات الخاصة) دون إذن ووجود مثل هذه النصوص هو ما يمنح الفعل وصف الجريمة ويحدد إطارها القانوني.

---

[٧] Al-sharq.com تاريخ دخول الموقع ٢٠٢٥/٣/١.

(ISSN: 2537- 0758)

ثانياً: الركن المادي للجرائم الإلكترونية

يعبر الركن المادي عن ماديات الجريمة التي تبرز بها إلى العالم الخارجي كأثر للسلوك الإجرامي[٨] والذي يقيد به القانون فيجعله عنصراً من العناصر المؤلفة لجريمة معينة فلا تتوافر الجريمة[٩]، إلا بتوافره مع بقية العناصر الأخرى فهذا الركن يُرتكب في بيئة تكنولوجيا المعلومات، ويحتاج في ارتكابه إلى مهارات تقنية، كزرع الفيروسات والفرصة الإلكترونية وغيرها من صور السلوك الإجرامي الإلكتروني إذ يتطلب وجود بيئة رقمية واتصالات بشبكة المعلومات الدولية فالجرائم الإلكترونية من جرائم السلوك المحض أو التي تسمى بالجرائم الشكلية[١٠] إذ يعد هذا السلوك قرينة قانونية على توافر الخطر وهو ما أقره المشرع الأمريكي الذي توسع في فكرة النتيجة المحتملة لتشمل الجريمة التي ليس لها ضحية على الإطلاق فأخذ المشرع بمعيار موسع للخطر ففي أحد القضايا التي أخذت صدى في القضاء الأمريكي والمعروفة باسم USAV ROOTS ومسلم فيها بوجود النتيجة المحتملة والتوسع فيها في الجرائم الإلكترونية[١١]، والمشرع هنا يتجه إلى تجريم السلوك الإجرامي في إطار هذه

---

[٨] المحامي/ عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائل الالكترونية دراسة قانونية، مقارنة، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، سنة ٢٠١٩، ص ١٨٧، ص ١٨٨.

[٩] د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠١٨، ص ٥٢.

[١٠] تعرف الجرائم الشكلية بأنها: "الجرائم التي لا يترتب عليها تغير في العالم الخارجي كأثر السلوك الإجرامي". أو أنها "الجرائم التي لا تتوافر فيها نتيجة مادية، وإنما تتوافر فيها نتيجة قانونية تتمثل في مجرد الخطر الذي يهدد المصلحة المحمية سواء أكانت خاصة أن عامة"، د. أحمد فتحي سرور الوسيط في قانون العقوبات، دار النهضة العربية، الطبعة السادسة، ٢٠١٥، ص ٥٢٠.

[١١] تلخص وقائع القضية في أن المدعو Roots قام في إحدى حلقات الكلام عبر غرفة الدردشة (الشات) بأن تحدث مع فتاة لم تتجاوز الرابعة عشر من عمرها في موضوعات جنسية وتناول الكلام عرضه لها بممارسة الأفعال الجنسية معها وتحديد موعد للقاء بينهما وعندما حل الموعد للقاء بينهما في أحد المحال التجارية تم القبض عليه، وتبين بالتحقيق أن الفتاة الصغيرة لم تكن سوى عضو في فريق مكافحة جرائم الانترنت وهي في حالة تذكر تم تكليفها من قبل الفريق وعندما دفع Roots بعدم وجود المجني عليه في هذه الدعوى أمام محكمة الموضوع رفضت المحكمة هذا

النوعية من الجرائم إذا تمت بطريق المراسلة، أو عبر الإنترنت بصرف النظر عن وجود الضحية من عدمه، أي التي ليس فيها ضحية على الإطلاق ولا يكون لها وجود مادٍ وإنما رقمي، فمثلاً لا يصح ضبط الجاني في منزلة بمجرد الكلام في الجنس عبر الإنترنت وإنما يجب أن يكون الجاني اتخذ خطوات المقابلة المجني عليه بأن تحرك في الواقع متجهاً إليه محدداً هدفه طبقاً للمشرع والقضاء الأمريكي. ليس كل جريمة تستلزم وجود أعمال تحضيرية ففي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية إلا أنه في مجال جرائم التقنية يختلف الأمر بعض الشيء[١٢] فيأت التعامل مع البرامج المختلفة الخاصة بالتقنية الحديثة أمر هام فنجد أنها تعطي العلاقة السببية طابع آخر فبالإضافة إلى أنها مادية فهي تأخذ الطابع التقني فتكون علاقة السببية مادية تقنية في إطار الجرائم المتعلقة بالكمبيوتر فمثلاً شراح برامج الاختراق وبرامج الفيروسات، ومعدات فك الشفرات وكلمات المرور، وحيازة صور مخلة بالآداب فهذه تمثل جريمة مستقلة في ذاتها.

ثالثاً: الركن المعنوي للجرائم الإلكترونية:

إن تحقق الركن المادي للجريمة لا يكفي وحدة لقيام المسؤولية الجنائية عنها وإنما ينبغي توافر الركن المعنوي للجريمة التي جوهرها الإرادة الإجرامية، ويتخذ الركن المعنوي إحدى صورتين القصد الجنائي، والخطأ غير العمدي، فيعرف القصد الجنائي على أنه علم الجاني بالعناصر المكونة للجريمة واتجاه إرادته إلى إحداث هذه العناصر أو إلى قبولها فالقصد الجنائي المتطلب القيام الجرائم الإلكترونية هو القصد الجنائي العام، الذي يفترض علم الجاني بعناصر الجريمة واتجاه إرادته نحو

الدفع مستندة إلى ما هو مقرر في القسم uscsec. ٢٤٢٢١٨، وفي الاستئناف قررت الدائرة الحادية عشر أنه لا داعي للوجود المادي للمجني عليه في إطار المادة المذكورة، إذ يكفي أن يكون هناك احتمال ارتكاب هذه الجريمة، المستشار الدكتور ربيع محمود الصغيرة، القصد الجنائي في الجرائم المتعلقة بالانترنت– دراسة تطبيقية مقارنة مركز الدراسات العربية للنشر والتوزيع، الجيزة ٢٠١٧، ص ١٠٧، ١٠٨.

[١٢] د. يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين الإماراتي والمصري، دار النهضة العربية، القاهرة، ٢٠١٧م، ص ٣٥٨.

(ISSN: 2537- 0758)

تحقيق هذه العناصر أو قبولها كما تطلب المشرع إلى جانب القصد الجنائي العام قصداً خاصاً يتمثل في اتجاه الإرادة إلى غاية معينة وهي نية التملك وغيرها من النوايا، فالركن المعنوي يتعلق بالإرادة التي يصدر عنها الفعل فهو يتمثل الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم فهو تراه يستخدم الإرادة في قانون العلامات التجارية في القانون الفيدرالي الأمريكي وأحياناً أخرى بالعلم كما في الاستنساخ الأمريكي[١٣]، أما المشرع الفرنسي فإن بيان سوء النية يكتسح النصوص القانونية لديه التي تطبق بشأن الإنترنت فان هذه الجرائم لديه لا يمكن أن تدخل حيز التطبيق ما لم يتوافر سوء النية في القصد الخاص، وإرادة الإضرار ذلك أن قانون العقوبات الفرنسي يشترط سوء النية حين يكون هناك اعتداء على البريد الإلكتروني كما ألزم تقنين البريد والاتصالات واحترام مبدأ سرية الاتصالات فالشرط الأساسي لتطبيق ذلك مع الالتزام بضرورة توافر سوء النية هو وجود اعتداء على حق الخصوصية بالاتصالات مما يستدعي الأمر أن يكون أولاً هناك وسيلة اتصال تتمتع بالخصوصية كالبريد الإلكتروني حيث بعد من وسائل الاتصال الخاصة الذي يتطلب توافر حماية قوية له[١٤].

المطلب الثالث

العقوبة

ما هي جريمة الدخول غير المشروع على موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية؟ وما هي عقوبتها؟

هي جريمة عمدية، يتمثل ركنها المادي في الدخول بأي وسيلة إلى موقع إلكتروني، أو نظام معلوماتي، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء

---

[١٣] د. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، ٢٠١٢، ص ٦٧.

[١٤] د. محمد عبدالله إبراهيم: المواجهة الأمنية الجرائم شبكة المعلومات الدولية، أكاديمية الشرطة، القاهرة، ٢٠١٦، ص ٩٤. على عدنان الفيل، الإجراءات التحري وجمع الأدلة والتحقيق الابتدائي، مرجع سابق، ص ١٧.

منها، أو تجاوز الدخول المصرح به أو الاستمرار في التواجد بها بعد العلم بذلك، ويجب القيام الجريمة أن يكون الدخول بغير وجه حق.

وتختلف هذه الجريمة عن سابقتها في أنها لا تختص فقط بالمواقع والأنظمة التابعة للدولة. بل تشمل جميع المواقع والنظم والشبكات المعلوماتية. كما أنه في هذه الجريمة يتساوى الدخول غير المشروع مع تجاوز حدود الدخول المصرح به أو الاستمرار في التواجد بعد علمه بهذا التجاوز رغم عدم تعمده ذلك في البداية.

وتكون عقوبة مرتكب هذه الجريمة الحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين. أي إن الجمع بين عقوبتي الحبس والغرامة جوازي في هذه الجريمة وليس إلزاميًا، أي أنه يجوز الحكم بالحبس فقط أو الغرامة فقط أو كليهما بحسب سلطة القاضي التقديرية المقدار الإثم المرتكب طبقًا لنص المادة (٣) من القانون رقم (١٤) لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية.

وتضاعف العقوبة إذا ترتب على الدخول:

١. 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 مخزنة في النظام المعلوماتي.
٢. إلحاق ضرر بالمستخدمين أو المستفيدين.
٣. تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية.
٤. تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية مالكه أو القائم على إدارته.

فما هي جريمة التقاط أو اعتراض أو التنصت على البيانات؟

- هي جريمة عمدية، يتمثل ركنها المادي في التقاط أو اعتراض أو التنصت على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو

(ISSN: 2537- 0758)

على بيانات المرور. ويجب القيام الجريمة أن يكون فعل الالتقاط أو الاعتراض أو التنصت دون وجه حق[١٥].

- وتكون عقوبة مرتكب هذه الجريمة الحبس مدة لا تجاوز سنتين وبالغرامة التي لا تزيد على (١٠٠,٠٠٠) مائة ألف ريال، أو بإحدى هاتين العقوبتين أي إن الجمع بين عقوبتي الحبس والغرامة جوازي في هذه الجريمة وليس إلزاميًا، أي إنه يجوز الحكم بالحبس فقط أو الغرامة فقط أو كليهما بحسب سلطة القاضي التقديرية المقدار الإثم المرتكب.

الأحكام المشتركة للعقاب في الجرائم الإلكترونية

يكون الشخص المعنوي مسئولًا عن الجريمة الإلكترونية إذا ارتكبت باسمه أو لحسابه، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

ويعاقب الشخص المعنوي في هذه الحالة بالغرامة التي لا تزيد على (١,٠٠٠,٠٠٠) مليون ريال.

وذلك طبقاً لنص (المادة (٤٨) من قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤).

ويعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القانون، بذات العقوبات المقررة للفاعل الأصلي.

(المادة (٤٩) من قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤)

وتضاعف العقوبة المقررة إذا ارتكبها أو سهل ارتكابها، موظف عام مُستغلًا صلاحياته وسلطاته في ذلك.

(المادة (٥١) من قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤)

ويري الباحث أن المشرع القطري أدرك خطورة الجرائم الإلكترونية لذلك فرض لها عقوبات متعددة في قانون مكافحة الجرائم الإلكترونية رقم ١٤ لسنة ٢٠١٤.

[١٥] المادة (٤) من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

المبحث الثاني
الجهود التشريعية المبذولة لمكافحة الجريمة الإلكترونية

تمهيد وتقسيم:

إن مكافحة الجرائم الإلكترونية يحتاج إلى منظومة تشريعية متكاملة، أساسها القانون الجنائي، ولكنها لا تقتصر عليه، فلنظم المعلومات وتكنولوجيا المعلومات أثرها على كافة فروع القانون، وهذا يتطلب وجود منظومة تشريعية متكاملة تغطي كافة هذه الأوجه، فإذا انطلقنا من القانون الجنائي فالحاجة ماسة لوجود قانون لمكافحة الجرائم الإلكترونية وفي المجال المدني هناك حاجة لتنظيم التعاقد الإلكتروني، والإثبات الإلكتروني، والمرافعات الإلكترونية، بالإضافة إلى موضوع التجارة الإلكترونية. وفي مجال الملكية الفكرية فالحاجة ماسة لتنظيم قواعد حماية البرامج وقواعد المعلومات، وفي مجال البنوك ظهرت البطاقات الإلكترونية والبنوك الإلكترونية والتحويلات الإلكترونية، والدفع الإلكتروني، وفي مجال حقوق الإنسان هناك حرية الرأي وحماية الخصوصية، هذا بالإضافة إلى أن الأسواق المالية والجمارك، ومصالح الضرائب والهجرة أصبحت تنجز معاملاتها بالطرائق الإلكترونية، مما يحتم وجود القواعد القانونية التي تنظم مثل كل هذه التعاملات.

ولذلك فإن المنظومة القانونية الإلكترونية لا بد أن تتكامل، ويكون تكاملها بوجود التشريعات المقننة التي تعالج كل هذه الحالات، وما يجري على أرض الواقع أن التكنولوجيا قد سبقت التشريع في كافة مناحي الحياة، والأمور لا تتزن بهذا الشكل، فلا بد أن يسير التشريع جنباً إلى جنب مع كافة المظاهر التكنولوجية الحديثة، حتى أنه لا بد أن يستشرف المستقبل في كثير من الأحيان.

وفي سبيل تحقيق ذلك مرت العملية التشريعية في مجال مكافحة الجريمة التقنية بالعديد من الجهود المتطورة على المستويين الأوروبي والعربي، ووضع نصوص عقابية وإجرائية رادعة، وهو ما سنبينه من خلال التقسيم التالي.

سوف نقوم بتقسيم هذا المبحث إلى المطالب التالية:

المطلب الأول: الجهود التشريعية الأوروبية

المطلب الثاني: الجهود التشريعية العربية

المطلب الثالث: جهود دولة قطر لمواجهة الجريمة الإلكترونية

(ISSN: 2537- 0758)

المطلب الأول
الجهود التشريعية الأوروبية

لقد اهتم المجتمع الدولي الأوروبي والأجنبي بتنظيم مجال تقنية المعلومات وبذل العديد من الجهود التشريعية من أجل التصدي لظاهرة الإجرام المعلوماتي[١٦].

- **بريطانيا:** بإصدارها لقانون مكافحة التزوير والتزييف عام ١٩٨٦م، وعرف أداة التزوير بأنها عبارة عن وسائط التخزين الحاسوبية المتنوعة، أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى.
- **فرنسا:** أصدرت القانون الفرنسي رقم ١٩ لسنة ١٩٨٨م الخاص بالتصدي للتزوير المعلوماتي.
- **الولايات المتحدة الأمريكية:** أصدرت العديد من التشريعات المتعلقة مجال تقنية وتكنولوجيا المعلومات، وكان من بينها القانون رقم ٤٧٤-٩٩-١٠٠ وهو قانون تشريعي عام شمل القانون التشريعي رقم ١٢١٣ لسنة ١٩٨٦ والمعدل للقانون (١٨ s, s, u ١٠٣٠) الخاص بمواجهة جرائم الحاسوب.

ولم يقف الأمر عند هذا الحد بل لقد اجتمع المجلس الأوروبي عام ٢٠٠١ في العاصمة المجرية بودابست في ٢٣ نوفمبر ٢٠٠١، للتشاور حول هذه الظاهرة الإجرامية المستحدثة والاتفاق على بنود واضحة لمكافحة هذه جرائم تقنية المعلومات، وقد أبرمت الاتفاقية الأوروبية الدولية لمكافحة الإجرام السيبراني الإجرام عبر الإنترنت، ووقعت عليها ٣٠ دولة، ثم انضم إليها العديد من الدول من خارج المجلس الأوروبي، وكان من أبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في ٢٢ سبتمبر ٢٠٠٦، ودخلت حيز النفاذ في الأول من يناير ٢٠٠٧، واشتملت

---

[١٦] يراجع في ذلك: د. ربيع محمود الصغير- القصد الجنائي- دراسة تطبيقية على الجرائم المتعلقة بالانترنت، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ٢٠١٥، ص ٩٦، هامش ٣. ويراجع في ذلك أيضاً: ورقة بحثية بعنوان دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول- إدارة الدراسات والبحوث- مقدمة ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة الفترة من ٢٣-٩/٢٥ الموافق ٧-١٤٣٣/١١/٩هـ، ص ١١ وما بعدها.

على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

المطلب الثاني
الجهود التشريعية العربية

وعلى الجانب التشريعي العربي فهناك العديد من الدول العربية التي واكبت هذا التطور التقني الحاصل في مجال تكنولوجيا المعلومات وعملت على محاولة التصدي لمكافحة الجرائم الإلكترونية الناشئة عنه بإصدارها عدد من التشريعات الخاصة، **ومن بين هذه الدول ما يلي:**

- **سلطنة عمان:** أصدرت عام ٢٠٠١ جملة من التشريعات لمكافحة الجريمة المعلوماتية تحت مسمى قانون مكافحة جرائم الحاسب الآلي (قانون مكافحة الجرائم الإلكترونية، وكان من أهمها الأتي:

المرسوم السلطاني رقم ٧٢ لسنة ٢٠٠١م الصادر بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي (الكمبيوتر) وذلك بإضافة فصل في الباب السابع من قانون الجزاء العماني تحت عنوان (جرائم الحاسب الآلي).

كما أنه تم إضافة مواد إلى قانون الاتصالات العماني تحرم تبادل الرسائل التي تخدش الحياء العام وتحرم استخدام أجهزة الاتصالات للإهانة أو الحصول على معلومات سرية أو إفشاء الأسرار أو إرسال رسائل تهديد، ثم ووضعت السلطنة قانونًا ينظم المعاملات الحكومية الإلكترونية والتوقيع الإلكتروني وحوادث اختراق الأنظمة.

- **دولة المغرب:** سعي المشرع المغربي لوضع نصوص تشريعية تعمل على تنظيم المعالجة القانونية للجريمة المعلوماتية في التشريع المغربي عن طريق إدخاله لبعض الفصول التشريعية التي تعاقب على الأفعال التي تشكل جرائم تحت عنوان المس بنظام المعالجة الآلية للمعطيات وذلك بموجب القانون رقم ٧. ٠٠٣. الصادر بتاريخ ١٦ رمضان ١٤٢٤ الموافق ١١ نوفمبر ٢٠٠٣.
- **دولة الإمارات العربية المتحدة:** لقد كان اهتمام دولة الإمارات العربية بمكافحة الجريمة المعلوماتية والتصدي لأخطارها اهتماماً واضحاً، حيث أصدرت العديد

(ISSN: 2537- 0758)

من التشريعات المتعلق بهذه النوعية من الجرائم المعلوماتية عالية التقنية من بينها:

القانون العربي الاسترشادي الصادر عام ٢٠٠٣ بشأن مكافحة جرائم تقنية المعلومات وما في حكمها المعتمد بموجب قرار مجلس وزراء العدل العرب المنعقد في دورته التاسعة عشرة رقم (٤٩٥-د١٩-٨/١٠/٢٠٠٣) ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (٤١٧-د ٢١/٢٠٠٤).

وفي عام ٢٠٠٦ أصدرت القانون رقم ٢ لسنة ٢٠٠٦ الخاص بمكافحة جرائم تقنية المعلومات، ثم تلاه إصدار القانون رقم ٣ لسنة ٢٠١٢ الخاص بإنشاء الهيئة الوطنية للأمن الإلكتروني، وفي عام ٢٠١٢ أصدرت المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢ المتعلق بمكافحة جرائم تقنية المعلومات، وفي عام ٢٠١٨ قامت بإصدار المرسوم الاتحادي رقم ٢ لسنة ٢٠١٨، الخاص بتعديل المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢.

وبذلك تعتبر دولة الإمارات أول دولة عربية تقوم بإصدار تشريع قانوني مستقل يتعلق بمكافحة الجرائم المعلوماتية هو القانون رقم ٢ لسنة ٢٠٠٦.

- **المملكة العربية السعودية:** حيث أصدرت عام ٢٠٠٧ أولي قوانينها في مجال المكافحة التشريعية لجرائم تقنية المعلومات تحت عنوان نظام مكافحة الجرائم المعلوماتية، وأثره مجلس الوزراء بالقرار رقم ٧٩ بتاريخ ١٤٢٨/٣/٧هـ، وتم التصديق عليه بالمرسوم الملكي رقم ١٧م بتاريخ ١٤٢٨/٣/٨هـ، وصدر بالقرار رقم ١١٥٦٧/ ب-بتاريخ ١٤٢٨/٣/٩هـ، وكان الهدف منه الحد من نشوء هذه الجرائم المعلوماتية، فقد جاء في المادة الثانية من هذا النظام: يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، بما يؤدي إلى ما يلي: (١-المساعدة على تحقيق الأمن المعلوماتي-حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية-حماية المصلحة العامة، والأخلاق والآداب العامة. ٤-حماية الاقتصاد الوطني).
- **دولة الكويت:** نظمت دولة الكويت استخدام وسائل التقنية الحديثة وتجريم الانتهاكات التي تحدث منها أو عليها بإصدار حزمة من التشريعات كان من

بينها: (القانون رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية، والقانون رقم ٩ لسنة ٢٠٠١ بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت والقوانين المعدلة له القانون رقم ٣ لسنة ٢٠٠٦ بشأن المطبوعات والنشر، القانون رقم ٦١ لسنة ٢٠٠٧ بشأن الإعلام المرئي والمسموع، القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية، القانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، قانون مكافحة جرائم تقنية المعلومات رقم ٦٣ لسنة ٢٠١٥).

- **جمهورية مصر العربية:** لقد كان حرص المشرع المصري عظيماً في مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العالم في العصر الحديث بإصداره العديد من التشريعات اللازمة لمواجهة هذا الغزو التقني ودخول الرقمية فضائها المعلوماتي، ومن هذه التشريعات قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣م الخاص بتأمين نقل وتبادل المعلومات[١٧]، والقانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية "الإنترنت"[١٨]، القانون رقم ١٤٣ لسنة ١٩٩٤ بشأن الأحوال المدنية والدستور المصري لعام ٢٠١٤ والذي تضمن العديد من المواد التي تهدف إلى إقرار حماية خاصة لمختلف نواحي التعاملات التقنية والرقمية وتنظيمها[١٩].

---

[١٧] وعرفت المادة الأولي من هذا القانون وسائل الاتصالات بأنها (آية وسيلة لإرسال أو استقبال الرموز، أو الإشارات، أو الرسائل، أو الكتابات أو الصور، أو الأصوات، وذلك أيا كانت طبيعتها، وسواء كان الاتصال سلكيا أو لاسلكيا)، وقد أقر المشرع في الباب السابع من هذا القانون مجموعة من العقوبات التي تطبق إزاء التعرض أو الاعتداد على تلك الخدمات أو استغلالها بطرق غير مشروعة.

[١٨] راجع القرار بقانون رقم ١٥ لسنة ٢٠٠٤ الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١٠٩ لسنة ٢٠٠٥ بشأن إصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[١٩] حيث نصت المادة ٣١ من الدستور المصري لعام ٢٠١٤ على أن "أمن الفضاء المعلوماتي جزء من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليها، على

(ISSN: 2537- 0758)

وقد أنشأت مصر[٢٠] بموجب قرار مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤ مجلس أعلى للأمن السيبراني[٢١]، لتكون مهمته وضع استراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية والإشراف على تنفيذها وتحديثها تمشياً مع التطورات التقنية، وبتاريخ ٢٠١٤/٩/١٩ أصدر السيد رئيس الجمهورية القرار رقم ٢٧٧ لسنة ٢٠١٤[٢٢]، بشأن الموافقة على انضمام مصر إلى الاتفاقية العربية المكافحة الجريمة المنظمة عبر الحدود الوطنية الموقعة في القاهرة بتاريخ ٢٠١٠/١٢/٢١.

النحو الذي ينظمه القانون. كما تنص المادة ٥٧ من ذات الدستور على أن "للحياة الخاصة حرمة، وهي مصونة لا تمس وللمراسلات البريدية، والبرقية والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمه، وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك".

[٢٠] من بين هذه الجهود والمحاولات التشريعية الأخرى ما يلي: "قرار وزير الاتصالات ١٠٧ لسنة ٢٠٠٥ بشأن مكتب حماية برامج الحاسب الآلي وقواعد البيانات قرار وزير الاتصالات ١٢٨ لسنة ٢٠٠٦ بشأن اختصاص الجهاز القومي لتنظيم الاتصالات بنظر المنازعات المتصلة بالاتصالات وإنشاء إدارة تسمى (إدارة فض المنازعات) بالجهاز، قرار وزير الاتصالات رقم ١٠٨ لسنة ٢٠٠٥ بشأن تحديد الخدمات والأعمال الخاضعة لرسم تنمية صناعة تكنولوجيا المعلومات والاتصالات".

[٢١] نشر هذا القرار بالجريدة الرسمية في ديسمبر ٢٠١٤، العدد الخمسون، بتاريخ ٢٠١٤/١٢/١٥. وتضمن على أن ينشأ مجلس أعلي لأمن البنية التحتية للاتصالات وتكنولوجيا المعلومات يتبع رئاسة مجلس الوزراء ويسمي المجلس الأعلى للأمن السيبراني، ويشكل برئاسة وزير الاتصالات وتكنولوجيا المعلومات وعضوية ممثلي وزارات: (الدفاع، الخارجية، الداخلية البترول، الثروة المعدنية، الكهرباء والطاقة المتجددة، والصحة والسكان، الموارد المائية والري، والتموين والتجارة الداخلية، الاتصالات، وتكنولوجيا المعلومات) وجهاز المخابرات العامة، والبنك المركزي المصري، وعدد ٣ من ذوي الخبرة في الجهات البحثية والقطاع الخاص يرشحهم المجلس، ويصدر بتعيينهم قرار من وزير الاتصالات وتكنولوجيا المعلومات.

[٢٢] منشور بالجريدة الرسمية، العدد ٤٧، بتاريخ ٢٠ نوفمبر ٢٠١٤.

وكان أخر هذه التطورات التشريعية وأهمها القانون رقم ٢٠١٨/١٧٥ الصادر بشأن مكافحة جرائم تقنية المعلومات[٢٣] ولائحته التنفيذية رقم ٢٠٢٠/١٦٩٩[٢٤].

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠، ووافقت مصر على الانضمام إليها بموجب قرار رئيس الجمهورية رقم ٢٧٦ لسنة ٢٠١٤ بتاريخ ١٩ أغسطس ٢٠١٤ والمنشور بالجريدة الرسمية بالعدد ٤٦ في ١٣ نوفمبر ٢٠١٤، وذلك مع التحفظ على شرط التصديق، وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

وتعد هذه الاتفاقية من أهم الاتفاقيات العربية التي أبرمت في مجال مكافحة الجريمة التقنية بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، مثل الاعتداء على سلامة البيانات، وجرائم إساءة استخدام وسائل تقنية المعلوماتية والتزوير والاحتيال والإباحية والاعتداء على حرمة الحياة الخاصة، والجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات مثل نشر أفكار جماعات إرهابية والدعوة لها، وتمويل العمليات الإرهابية ونشر طرق صناعة المتفجرات، وأيضاً ما يتعلق بالجريمة المنظمة مثل غسل الأموال والترويج للمخدرات والاتجار بالبشر والأعضاء البشرية والأسلحة.

وكان ذلك عرض سريع لأهم التطورات التشريعية التي حدثت على المستويين العالمي والإقليمي في مجال مكافحة الجريمة التقنية، ولكن ما يهمنا هنا هو ما صدر مؤخراً من تشريعات عربية في هذا الشأن، وعرض لما جانبها من صواب أو شابها من عيوب وانتقادات، وهو ما سوف تنصب عليه دراستنا الماثلة تباعاً.

المطلب الثالث

جهود دولة قطر لمواجهة الجريمة الإلكترونية

في هذا المطلب سنتطرق للحديث عن التشريعات الداخلية وذلك في الفرع الأول منه، أما الفرع الثاني نخصصه لبيان الأجهزة المختصة في دولة قطر.

---

[٢٣] منشور بالجريدة الرسمية– العدد ٣٢ مكرر (ج) بتاريخ ٢٠١٨/٨/١٤.

[٢٤] المنشور بالجريدة الرسمية في العدد ٣٥ تابع (ج)– بتاريخ ٢٧ أغسطس سنة سنة ٢٠٢٠.

(ISSN: 2537- 0758)

الفرع الأول
التشريعات الداخلية

وفيما يلي نشير إلى التشريعات القطرية التي نظمت مسألة التعاون الدولي المكافحة الجريمة الإلكترونية

أولاً: الدستور الدائم لدولة قطر

بإمعان النظر في نصوص الدستور القطري، يمكن أن نستنبط منها الأحكام التي يفهم منها حرص دولة قطر على التعاون الدولي بشكل عام، وهي كالآتي:

- نصت المادة (٦) من الدستور القطري على أنه: "تحترم دولة قطر المواثيق والعهود الدولية، وتعمل على تنفيذ كافة الاتفاقيات والمواثيق والعهود الدولية التي تكون طرفاً فيها".
- كما نصت المادة (٧) من الدستور القطري على ما تقوم عليه السياسية الخارجية الدولة قطر وذكرت من بينها التعاون مع الأمم المحبة للسلام.

ثانياً: قانون العقوبات الصادر بالقانون رقم (١١) لسنة ٢٠٠٤

نص قانون العقوبات القطري على جرائم الحاسب الآلي، وأدرجها ضمن الجرائم الواقعة على المال، ونضمها في ١٨ مادة تبدأ بالمادة (٣٧٠) وتنتهي بالمادة (٣٨٧)، حيث احتوت على أحكام تتعلق بنظام المعالجة الآلية للبيانات، وفيروس الحاسب الآلي، وبطاقات الدفع الممغنطة، وتعتبر دولة قطر من أوائل الدول العربية التي وضعت أحكاماً في قانون العقوبات تتعلق بالجرائم ذات الصلة بالحاسب الآلي.

وفيما يتعلق بسريان القانون القطري على الجرائم العابرة للحدود، تجدر الإشارة إلى أن المشرع القطري أخذ بمبدأ العالمية، وحدد جرائم على سبيل الحصر تخضع لهذا المبدأ، ولم يذكر من بينها الجرائم الإلكترونية، حيث نصت المادة (١٧) من قانون العقوبات على أنه: "تسري أحكام هذا القانون على كل من وجد في الدولة بعد أن ارتكب في الخارج، بوصفه فاعلاً أو شريكاً، أيا من جرائم الاتجار في المخدرات أو في الأشخاص أو جرائم القرصنة أو الإرهاب الدولي"[٢٥]، وفي هذا الجانب يرى

[٢٥] مبدأ العالمية يعد استثناء على القواعد العامة، بمقتضاه يمتد تطبيق القانون الوطني على وقائع تمت بالخارج وعلى جناة لا يحملون الجنسية الوطنية، ويشترط لتطبيقه عدة شروط:-١- انتفاء اختصاص القانون القطري وفقاً لمعايير الاختصاص الأخرى-٢ تكون الجريمة من الجرائم

الدكتور بشير سعد من الضروري ادراج الجرائم الإلكترونية ضمن الجرائم التي يُطبق عليها (مبدأ العالمية)، لكونه يُساهم في تفعيل التعاون الدولي لمكافحة هذه النوعية من الجرائم[٢٦].

ثالثاً: قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية:

بعد عشرة أعوام من إصدار قانون العقوبات الصادر بالقانون رقم (١١) لسنة ٢٠٠٤، فطن المشرع القطري بأنه احتراماً لمبدأ شرعية الجرائم والعقوبات لا يمكن الاكتفاء بما ورد في قانون العقوبات فكان لا بد من التدخل لإصدار تشريع جنائي خاص يواجه الاعتداءات التي يتعرض لها النظام المعلوماتي، ويواكب الوسائل الحديثة التي ترتكب بها هذه النوعية من الجرائم عليه تم إصدار قانون مكافحة الجرائم الإلكترونية الصادر بالقانون رقم (١٤) لسنة ٢٠١٤.

وتجدر الإشارة بأن هناك عدة دول أصدرت تشريعات خاصة تنظم مسألة مكافحة الجرائم الإلكترونية، كالتشريع الإماراتي، والبحريني، والمصري، والأردني والسوداني، والفلسطيني، وغيرها. وقد اختلفت التشريعات في التسميات التي أطلقتها على القانون الذي يُجرم الاعتداءات التي تتم على الأنظمة المعلوماتية.

ولم يكتف المشرع القطري بالأحكام العامة المتعلقة بالتعاون الدولي الواردة في قانون الإجراءات الجنائية بل جاء ليؤكد ذلك بأحكام تفصيلية أوردها في قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤، حيث أفرد الباب الرابع منه لتنظيم المسائل المتعلقة بالتعاون الدولي، وقسمها إلى ثلاثة فصول وهي القواعد العامة، المساعدة القانونية المتبادلة، تسليم المجرمين.

وكانت خطة المشرع القطري في مجال التعاون الدولي لمواجهة الجرائم الإلكترونية واضحة، **نعرضها على النحو التالي:**

المنصوص عليها على سبيل الحصر،-٣- تواجد الجاني في دولة قطر. انظر: أشرف توفيق شمس الدين، شرح قانون العقوبات القطري، جامعة قطر، ٢٠١٠، ص ١٨٤-١٨٧.

[٢٦] بشير سعد، محاضرة ضمن مقرر الجرائم المعلوماتية (غير منشورة)، ألقيت على طلبة ماجستير القانون العام بكلية القانون بجامعة قطر، بتاريخ ١٠/أبريل /٢٠١٩م.

(ISSN: 2537- 0758)

أ- القواعد العامة

- أوجب القانون على الجهة المختصة (يقصد بها الوحدة الإدارية المختصة بوزارة الداخلية وهي إدارة الجرائم الاقتصادية والإلكترونية)، تقديم العون للجهات النظيرة في الدول الأخرى، بغية تقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات والإجراءات الجنائية ذات صلة بالجرائم المنصوص عليها في قانون مكافحة الجرائم الإلكترونية، وذلك وفقاً للقواعد المقررة في قانون الإجراءات الجنائية، والاتفاقيات التي تكون الدولة طرفاً فيها، أو تطبيق مبدأ المعاملة بالمثل بشرط أن لا يتعارض ذلك مع أحكام قانون مكافحة الجرائم الإلكترونية أو أي قانون آخر. واشترط القانون لتنفيذ طلب المساعدة القانونية أو طلب تسليم المجرمين ازدواجية التجريم[٢٧].

١. أعطى القانون للنائب العام مسؤولية وصلاحية تلقي طلبات المساعدة القانونية المتبادلة وتسليم المجرمين من الجهات الأجنبية المختصة بالجرائم الإلكترونية، ويتوجب عليه أن ينفذ هذه الطلبات أو إحالتها إلى الوحدة الإدارية المختصة بوزارة الداخلية لتنفيذها بأسرع وقت ممكن. وفي الحالات المستعجلة يجوز إرسال تلك الطلبات من خلال المنظمة الدولية للشرطة الجنائية (الإنتربول) أو بشكل مباشر من الجهة المختصة في الدولة الأجنبية إلى الجهة المختصة في دولة قطر، وفي هذه الحالات يتوجب إبلاغ النائب العام[٢٨].
٢. نص قانون مكافحة الجرائم الإلكترونية على البيانات التي يتعين تضمينها في طلبات المساعدة القانونية أو طلبات تسليم المجرمين وهي: "تحديد هوية الجهة التي تطلب اتخاذ التدابير، اسم ووظيفة الجهة التي تتولى التحقيق أو الاتهام في الدعوى، وتحديد الجهة إلى يوجه إليها الطلب، وبيان الغرض من الطلب الوقائع المساندة للطلب النص القانوني الذي يجرم الفعل أي تفاصيل تسهل عملية تحديد هوية الشخص المعني، أية معلومات لازمة لتحديد الأشخاص المعنيين تفاصيل المساعدة المطلوبة"[٢٩].

---

[٢٧] راجع المادة (٢٣) من قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

[٢٨] راجع المادة (٢٤) من نفس القانون.

[٢٩] راجع المادة (٢٥) من نفس القانون.

ب-المساعدة القانونية المتبادلة:

١. نص القانون على صور المساعدة القانونية المتبادلة وهي: "الحصول على الأدلة من الأشخاص أو أخذ أقوالهم المساعدة على مثول المحتجزين والشهود الطوعيين أو غيرهم، أمام الجهات القضائية للدولة الطالبة من أجل تقديم الأدلة أو المساعدة في التحقيقات تسليم الأوراق القضائية، تنفيذ عمليات التفتيش والحجز التحفظ العاجل على البيانات والمعلومات الإلكترونية ومعلومات المشترك، الجمع والتسجيل الفوري لبيانات المرور[٣٠]، معاينة الأشياء والأماكن وأنظمة المعلومات توفير المعلومات والأشياء المثبتة للتهمة وتقارير الخبراء، مصادرة الموجودات أي صور أخرى من صور المساعدة القانونية المتبادلة بما لا يتعارض مع القوانين المعمول بها في الدولة"[٣١].

٢. نص القانون بأنه لا يجوز رفض طلب المساعدة إلا في حالات معينة ذكرها القانون على سبيل الحصر وهي: "١-إذا لم يصدر الطلب من الجهة المختصة حسب قانون الدولة طالبة المساعدة أو الطلب يخالف حكم جوهري في القانون أو لم يرسل الطلب وفقاً للقوانين المعمول بها. ٢-إذا كان من المحتمل أن يمس الطلب أمن الدولة أو سيادتها أو نظامها العام أو مصالحها الأساسية في حال تنفيذه. ٣-إذا كان الطلب يتعلق بدعوى جنائية منظورة أو فصل فيها بحكم قضائي في الدولة. ٤-إذا كان هناك أسباب جوهرية تدعو إلى الاعتقاد بأن السبب في هذا التدبير المطلوب اتخاذه يستهدف الشخص بسبب عنصره أو ديانته أو جنسيته أو عرقه أو آرائه السياسية أو جنسه أو حالته. ٥-إذا كانت الجريمة محل الطلب لم يتم النص عليها في قوانين الدولة أو ليس لها جريمة مماثلة منصوص عليها في قوانين الدولة، ليس من الممكن إصدار أمر باتخاذ التدابير المطلوبة أو تنفيذها بسبب قواعد التقادم، الأمر المطلوب تنفيذه غير قابل للنفاذ بمقتضى القانون. ٦-إذا كان إصدار القرار في الدولة الطالبة قد جرى في ظروف لم تتوافر فيها الضمانات الكافية فيما يتعلق بحقوق المتهم"[٣٢].

---

[٣٠] راجع المواد (٢٦)، (٢٧)، (٢٨) من قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

[٣١] راجع المادة (٣٠) من نفس القانون.

[٣٢] راجع المادة (٣١) من قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(ISSN: 2537- 0758)

٣. بشكل عام لا يجوز رفض المساعدة القانونية المتبادلة لأسباب مبالغ فيها، ويمكن الطعن على قرار الرفض وفقاً للقواعد المقررة في القانون. وإذا رفضت دولة قطر تقديم المساعدة يتوجب على النائب العام أو الجهة المختصة إبلاغ الجهة الأجنبية المعنية بأسباب الرفض[٣٣].

٤. تدابير التحقيق يتم تنفيذها من خلال القواعد الإجرائية المعمول بها في دولة قطر إلا إذا طلبت الدولة الأجنبية إتباع إجراءات معينة بشرط أن لا تتعارض مع القواعد المطبقة في دولة قطر، وقد أجاز المشرع أن تفوض الجهة الأجنبية المختصة موظف عام لحضور إجراءات التحقيق[٣٤].

٥. تطرق المشرع إلى مسألة مصادرة الأشياء المتحصلة من الجريمة الإلكترونية، ونص على أنه إذا تلقت الجهة المختصة بدولة قطر طلب إصدار أمر بالمصادرة فإنه يتعين إحالة الطلب إلى النيابة العامة لإصدار أمر بالمصادرة وتنفيذه، وإن محل أمر المصادرة يشمل الأجهزة وأنظمة المعلومات والبرامج وغيرها من الوسائل المستخدمة في ارتكاب الجريمة والمتواجدة في دولة قطر والواردة في أحكام المصادرة المنصوص عليها في قانون مكافحة الجرائم الإلكترونية، كما يتعين على الجهة المختصة عند تنفيذها لأمر المصادرة أن تلتزم بالوقائع التي تم الاستناد إليها لتوقيع أمر المصادرة. كما أن لدولة قطر التصرف في الموجودات المصادرة والموجودة على أراضيها بناء على طلب الدولة الأجنبية، ما لم يوجد اتفاق على خلاف ذلك[٣٥].

ج- تسليم المجرمين

أما بخصوص التعاون الدولي في مجال تسليم مرتكبي الجرائم الإلكترونية فقد نظمها المشرع القطري على النحو التالي:

---

[٣٣] راجع المادة (٣٢) من نفس القانون.

[٣٤] راجع المادة (٣٣) من نفس القانون.

[٣٥] راجع المادتين (٣٥) و(٣٦) من قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية السالف الذكر.

١. أجاز المشرع القطري تسليم مرتكبي الجرائم الإلكترونية المنصوص عليها في قانون مكافحة الجرائم الإلكترونية، حيث إن هذه الجرائم لا تعتبر جرائم سياسية أو جرائم مرتبطة بجريمة سياسية أو جرائم ذات دوافع سياسية[٣٦].

٢. نص المشرع على الحالات التي لا يجوز فيها تسليم المجرمين وهي[٣٧]:"١- إذا كانت هناك أسباب جوهرية تدعو للاعتقاد بأن طلب التسليم قد تم تقديمه لغرض اتهام شخص أو معاقبته بسبب جنسه أو عنصره أو ديانته أو جنسيته أو آرائه السياسية، أو بأن تنفيذ الطلب سيؤدي إلى المساس بوضعه لأي من تلك الأسباب. ٢-إذا كانت الجريمة موضوع طلب التسليم، تمثل موضوع دعوى فصل فيها بحكم نهائي في الدولة، ٣-إذا كان الشخص المطلوب تسليمه قد أصبح، بمقتضى قانون أي من البلدين، غير خاضع للمحاكمة أو العقوبة لأي سبب، بما في ذلك التقادم أو العفو.-إذا كانت هناك أسباب جوهرية تدعو للاعتقاد بأن الشخص المطلوب تسليمه قد تعرض أو سيتعرض للتعذيب أو المعاملة قاسية أو غير إنسانية أو مهينة، أو إذا لم يتوفر أو لن يتوفر لذلك الشخص في الإجراءات الجنائية حد أدنى من الضمانات طبقاً للمعايير الدولية المعتبرة في هذا الشأن. ٤-إذا كان الشخص المطلوب تسليمه مواطناً قطرياً"[٣٨].

رابعاً: قانون رقم (٢٠) لسنة ٢٠١٩ بإصدار قانون مكافحة غسل الأموال وتمويل الإرهاب

نظراً لكون أن جرائم غسل الأموال وتمويل الإرهاب من الجرائم العابرة للحدود فقد أفرد المشرع القطري الفصل العاشر من قانون رقم (٢٠) لسنة ٢٠١٩ بإصدار قانون مكافحة غسل الأموال وتمويل الإرهاب للأحكام المتعلقة بالتعاون الدولي وقد نظمها في ١٧ مادة تبدأ من المادة (٥٨) وحتى المادة (٧٤)، واشتملت على قواعد تتعلق بتسليم المجرمين والمساعدة القانونية المتبادلة، وتتشابه هذه الأحكام مع ما جاء به قانون مكافحة الجرائم الإلكترونية من قواعد تتصل بالتعاون الدولي.

---

[٣٦] راجع المادة (٣٩) من نفس القانون.

[٣٧] راجع المادة (٤٠) من نفس القانون.

[٣٨] راجع المادة (٤١) من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية السالف الذكر.

(ISSN: 2537- 0758)

وفي هذا الصدد نشير إلى المادة (٥) من قانون رقم (١٤) لسنة ٢٠١٤ بشأن مكافحة الجرائم الإلكترونية والتي نصت على أنه يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠ ٠٠٠) خمسمائة ألف ريال كل من أنشأ أو أدار موقعاً لجماعة أو تنظيم إرهابي على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو سهل الاتصال بقيادات تلك الجماعات أو أي من أعضائها، أو الترويج لأفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية". تجدر الإشارة إلى أن هذا النص يطبق إذا تم تمويل الإرهاب باستخدام إحدى الوسائل التكنولوجية الحديثة.

وبناء على ما تقدم، وبعد عرض القوانين سالفة الذكر يمكن القول بأن المشرع الفطري يدرك ضرورة التعاون الدولي للتصدي للجريمة الإلكترونية.

يرى الباحث أن مما تقدم يتضح لنا بأن المشرع القطري أولى اهتماماً كبيراً للتعاون الدولي في مجال مواجهة الجريمة الإلكترونية وهذا يتجلى من خلال القواعد التفصيلية التي اتسمت بالشمول والوضوح مما يعطي دلالة بأن المشرع القطري لديه يقين تام بأن هذه الجرائم لا يمكن مكافحتها والوقاية منها إلا من خلال تعاون المجتمع الدولي[٣٩].

الفرع الثاني
الأجهزة المختصة في دولة قطر

أولاً: النيابة العامة:

أ- نيابة الجرائم الإلكترونية

أصدر سعادة النائب العام قراره رقم (٧٢) لسنة ٢٠١٨م، بشأن إنشاء نيابة الجرائم الإلكترونية وتحديد اختصاصاتها، وبموجبه تم إنشاء نيابة الجرائم الإلكترونية

[٣٩] راجع المادة (٤٢) من قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية السالف الذكر.

بتاريخ ٢٠١٨/٦/٢١م[٤٠]، وتختص بالتحقيق والتصرف في الجرائم المذكورة أدناه[٤١]:

١. الجرائم التي تقع بالمخالفة لأحكام القانون رقم (٨) لسنة ١٩٧٩ بشأن المطبوعات والنشر، عدا ما كان من اختصاص نيابة أمن الدولة ومكافحة الإرهاب.
٢. الجرائم الموجودة بنصوص المواد (٢٠٣، ٢٩٣، ٣٣١، ٣٣٢، ٣٣٣)، والفصل الخامس–جرائم الحاسب الآلي من قانون العقوبات رقم (١١) لسنة ٢٠٠٤م.
٣. الجرائم التي تقع بالمخالفة لأحكام القانون رقم (٣٤) لسنة ٢٠٠٦ بإصدار قانون الاتصالات والمعدل بالقانون رقم (١٧) لسنة ٢٠١٧.
٤. الجرائم التي تقع بالمخالفة لأحكام القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية، عدا ما كان من اختصاص نيابة أمن الدولة ومكافحة الإرهاب.
٥. الجرائم التي تقع بالمخالفة لأحكام القانون رقم (١٦) لسنة ٢٠١٠ بإصدار قانون المعاملات والتجارة الإلكترونية، عدا ما كان من اختصاص نيابة التجارة وشؤون المستهلك.
٦. الجرائم التي تقع بالمخالفة لأحكام القانون رقم (١٣) لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية.

وتجدر الإشارة بأن يكون اختصاص نيابة الجرائم الإلكترونية شاملاً جميع أنحاء الدولة.

وفي إطار التعاون الدولي تختص نيابة الجرائم الإلكترونية بتطبيق الأحكام المنصوص عليها في الباب الرابع المعنون بعنوان "التعاون الدولي" من قانون رقم

---

[٤٠] أحمد يوسف الكواري، محاضرة ضمن مقرر الجرائم الإلكترونية (غير منشورة)، ألقيت على طلبة ماجستير القانون العام بكلية القانون بجامعة قطر، بتاريخ ٢٠١٩/٤/٣م.

[٤١] انظر الموقع الإلكتروني للنيابة العامة في دولة قطر على الرابط التالي: https://www.pp.gov.qa تاريخ الزيارة ٢٠٢٥/٣/٥

(ISSN: 2537- 0758)

(١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية، والتي تم التطرق إليها سابقاً.

ب- نيابة التعاون الدولي:

وبشكل عام تختص نيابة التعاون الدولي في مجال تسليم المتهمين أو المحكوم عليهم أو الأشياء المتحصلة من الجريمة، كما تختص في النظر بطلبات الإنابة القضائية والتحقيق فيها، بالإضافة إلى النظر في تبادل التنفيذ القضائي، كما تقوم بدراسة مشاريع الاتفاقيات الدولية ومذكرات التفاهم.

ثانياً: إدارة مكافحة الجرائم الاقتصادية والإلكترونية:

تعد إدارة مكافحة الجرائم الاقتصادية والإلكترونية إحدى الوحدات الإدارية بوزارة الداخلية، لها دور بارز في التعاون الدولي لمكافحة الجريمة الإلكترونية، من خلال الأحكام الواردة في الباب الرابع من قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية- والتي أشرنا إليها سابقاً- كما تختص إدارة مكافحة الجرائم الاقتصادية والإلكترونية في التحقيق بالجرائم وعرضها على النيابة العامة، وكذلك البحث والتحري في المواقع الإلكترونية المشبوهة، والبحث والتحري في البلاغات المقدمة من قبل المتضررين، وعلى الصعيد الدولي هناك تعاون بينها وبين الإنتربول وشركات الأمم (كالسناب شات والانستغرام) للتصدي للجريمة الإلكترونية[٤٢].

ثالثاً: إدارة الاتصال للشرطة العربية والدولية (الإنتربول) بوزارة الداخلية:

إدارة الاتصال للشرطة العربية والدولية (الإنتربول) تتبع مكتب معالي رئيس مجلس الوزراء وزير الداخلية في الهيكل التنظيمي، وكانت تسمى في السابق شعبة الاتصال والانتربول، تعمل على تنمية علاقات التعاون والتنسيق في مجال مكافحة الإجرام عربياً ودولياً.

---

[٤٢] عبدالرحمن عبدالله البوعينين، محاضرة ضمن مقرر الجرائم الإلكترونية (غير منشورة)، ألقيت على طلبة ماجستير القانون العام بكلية القانون بجامعة قطر، بتاريخ: ٢٠١٩/٣/١٣م.

وتضم شعبة اتصال مجلس وزراء الداخلية العرب بالدوحة، والتي تم إنشائها بموجب النظام الأساسي للمجلس الذي نص على إنشاء شعبة اتصال في كل دولة عربية، وتضم الإدارة المكتب المركزي الوطني (الانتربول) الذي نشأ بموجب النظام الأساسي للمنظمة حيث ينص على إنشاء مكتب مركزي وطني في كل دولة.

ومن الأمثلة العملية لتعاون دولة قطر مع الإنتربول في مجال مكافحة الجريمة الإلكترونية هو الحكم الصادر عن المحكمة الابتدائية بدولة قطر بتاريخ ٢٠١٨/١٠/٣٠م، حيث تتلخص وقائع الدعوى في أنه وردت معلومات للشرطة الجنائية الدولية (الإنتربول) بأن المتهم متواجد بدولة قطر ويقوم بتحميل ورفع مواد إباحية تخص الأطفال وبعد البحث والتحري تبين أن المتهم هو الذي يملكها ويستخدمها، وتمت إدانته بتهمة نشر وتداول مقاطع إباحية خاصة بالأطفال بواسطة تقنية المعلومات.

رابعاً: اللجنة الوطنية لأمن المعلومات:

أنشأت اللجنة الوطنية لأمن المعلومات بموجب القرار الأميري رقم (١٩) لسنة ٢٠١٦، برئاسة رئيس مجلس الوزراء ووزير المواصلات والاتصالات، نائباً للرئيس، وتضم في عضويتها ممثل عن كل من الجهات التالية: (وزارة الداخلية، وزارة الدفاع، وزارة الخارجية، وزارة التجارة والصناعة، وزارة المالية، وزارة العدل، وزارة المواصلات والاتصالات، النيابة العامة، جهاز أمن الدولة، مصرف قطر المركزي)[٤٣].

ونص القرار أعلاه في المادة (٣) منه على أنه: تهدف اللجنة إلى تعزيز أمن المعلومات في الدولة بما يحقق خطط التنمية الشاملة في جميع المجالات، وذلك من خلال التوجيه الاستراتيجي للجهود الوطنية اللازمة لتنفيذ الأهداف المحددة في الاستراتيجية الوطنية لأمن المعلومات، وتحقيق التعاون مع الجهات المختصة أو المعنية في هذا المجال. كما نص القرار بأن للجنة أن تمارس كافة الاختصاصات والصلاحيات اللازمة لتحقيق أهدافها، وأشار إلى بعض منها على وجه الخصوص

[٤٣] والجدير بالذكر بأنه تم إعادة هيكلة بعض وزارات الدولة بموجب القرار الأميري رقم (٥٧) لسنة ٢٠٢١ بتعيين اختصاصات الوزارات ومن بين ذلك التعديل إنشاء وزارة الاتصالات وتكنولوجيا المعلومات ووزارة المواصلات وحل وزارة الاتصالات والمواصلات.

(ISSN: 2537- 0758)

ومن بينها إنشاء قنوات الاتصال مع المؤسسات الدولية والجهات الخارجية المختصة ووضع أطر التعاون معها ومتابعة التطورات والمستجدات في هذا المجال.

خامساً: الوكالة الوطنية للأمن السيبراني:

لقد نصت المادة (٣) من القرار الأميري رقم (١) لسنة ٢٠٢١ بإنشاء الوكالة الوطنية للأمن السيبراني على أن الهدف من إنشاء الوكالة هو المحافظة على الأمن الوطني السيبراني وتنظيمه وتعزيز المصالح الحيوية للدولة وحمايتها في مواجهة تهديدات الفضاء السيبراني وفي سبيل كشف ذلك منحت الوكالة كافة الاختصاصات والصلاحيات، منها إعداد الاستراتيجية الوطنية للأمن السيبراني، وضع وتحديث السياسات المتعلقة بتعزيز الأمن السيبراني، وضع أطر لكيفية إدارة المخاطر السيبرانية، رفع مستوى الوعي بالأمن السيبراني، ولم نجد نصاً صريحاً خاص بالتعاون الدولي لمكافحة الجرائم الإلكترونية إلا أن المادة سالفة الذكر نصت على بنود يستفاد منها اتخاذ الوكالة التعاون الدولي كآلية للمحافظة على الأمن السيبراني تعزيز التعاون الدولي لمكافحة أشكال الجريمة الجديدة مثل الجرائم السيبرانية والتي تعتبر من الجرائم العابرة للحدود، حيث أنها تتزايد تعقيداً، وتشارك فيها مجموعات إجرامية منظمة قادرة على التأقلم مع الظروف المتغيرة بوتيرة أسرع من وتيرة تكيف سلطات إنفاذ القانون، لذلك أصبحت الحاجة ملحة لإعداد صك دولي جديد له صفة إلزامية لسد الثغرات التي تشوب التشريعات الداخلية، وهناك من رأى بأنه لا حاجة لصك دولي جديد حيث إن اتفاقية مجلس أوروبا كافية لا سيما وإن باب التصديق عليها مفتوح للدول من خارج المنطقة.

الخاتمة

لكل ما تقدم نخلص إلى عدد من النتائج والتوصيات، على النحو التالي:

أولاً: النتائج:

١. لا يمكن وضع تعريف جامع مانع لمصطلح الجريمة الإلكترونية.
٢. لا يوجد اتفاقية عالمية خاصة بمكافحة الجرائم الإلكترونية.
٣. الجريمة الإلكترونية جريمة عابرة للحدود ولا يمكن مكافحتها إلا بتضافر المجتمع الدولي.
٤. القانون القطري غني بالأحكام التي تنظم مسألة التعاون الدولي في مكافحة الجريمة الإلكترونية، مما يكشف عن وعي المشرع وتيقنه بضرورة مكافحة الجريمة الإلكترونية عن طريق آليات دولية.
٥. توجيه دولة قطر أجهزتها الداخلية بالتعاون الدولي مع الأجهزة المعنية في الدول الأخرى.

ثانياً: التوصيات:

١. وضع اتفاقية عالمية خاصة بمكافحة الجريمة الإلكترونية تحت مظلة هيئة الأمم المتحدة.
٢. وضع لجان دولية مهمتها مراقبة تنفيذ الدول لالتزاماتها المنبثقة من الاتفاقيات الدولية الخاصة بمكافحة الجريمة الإلكترونية.
٣. إدخال المشرع القطري الجريمة الإلكترونية ضمن الجرائم التي يطبق عليها مبدأ العالمية.
٤. مجرد وجود القوانين والاتفاقيات الدولية المتعلقة بالتعاون الدولي لمواجهة الجريمة الإلكترونية لا يكفي بل لا بد من تفعيلها من خلال تنفيذ ما جاء بها من أحكام.
٥. زيادة الوعي لدى الأشخاص عن مخاطر الجريمة الإلكترونية وكيفية الوقاية منه.

(ISSN: 2537- 0758)

قائمة المراجع

أولاً: الكتب

١. د. أحمد فتحي سرور الوسيط في قانون العقوبات، دار النهضة العربية، الطبعة السادسة، ٢٠١٥.

٢. أشرف توفيق شمس الدين، شرح قانون العقوبات القطري، جامعة قطر، ٢٠١٠.

٣. د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠١٨.

٤. المستشار الدكتور/ ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالانترنت– دراسة تطبيقية مقارنة مركز الدراسات العربية للنشر والتوزيع، الجيزة ٢٠١٧.

٥. المحامي/ عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائل الإلكترونية دراسة قانونية، مقارنة، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، سنة ٢٠١٩.

٦. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية): دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محلياً وعربياً ودولياً، منشورات الحلبي الحقوقية، بيروت، ٢٠١٧.

٧. د. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، ٢٠١٢.

٨. محمد حماد مرهج الهيئتي، الجريمة المعلوماتية نماذج من تطبيقها دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، مصر، ٢٠١٤.

٩. د. محمد عبد الله إبراهيم: المواجهة الأمنية الجرائم شبكة المعلومات الدولية، أكاديمية الشرطة، القاهرة، ٢٠١٦.

١٠. محمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، مصر، ٢٠١٥.

١١. هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة.

١٢. د. يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين الإماراتي والمصري، دار النهضة العربية، القاهرة، ٢٠١٧م.

ثانياً: الرسائل العلمية

١. د. ربيع محمود الصغير – القصد الجنائي– دراسة تطبيقية على الجرائم المتعلقة بالانترنت، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ٢٠١٥.

ثالثاً: المجلات والدوريات

١. أحمد يوسف الكواري، محاضرة ضمن مقرر الجرائم الإلكترونية (غير منشورة)، ألقيت على طلبة ماجستير القانون العام بكلية القانون بجامعة قطر، بتاريخ ٢٠١٩/٤/٣م.

(ISSN: 2537- 0758)

٢. بشير سعد، محاضرة ضمن مقرر الجرائم المعلوماتية (غير منشورة)، ألقيت على طلبة ماجستير القانون العام بكلية القانون بجامعة قطر، بتاريخ ١٠/أبريل/٢٠١٩م.
٣. عبد الرحمن عبد الله البوعينين، محاضرة ضمن مقرر الجرائم الإلكترونية (غير منشورة)، ألقيت على طلبة ماجستير القانون العام بكلية القانون بجامعة قطر، بتاريخ: ١٣/٣/٢٠١٩م.
٤. عبد العال الديري، الجريمة المعلوماتية: تعريفها، أسبابها، خصائصها، دراسة منشورة على موقع المركز العربي الأبحاث القضاء الإلكتروني، الأحد ١٣ يناير ٢٠١٣.

رابعا: المواقع الإلكترونية

1- http://accronline com/article_detail. aspx?id=7509.
2- Al-sharq. com.
3- https://www. pp. gov. qa.