العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

"فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية"

"دراسة مقارنة"

إعداد الباحث:

د. مخلد ابراهيم الزعبي

استاذ مساعد في القانون الجنائي –كلية الشرطة – قسم العلوم الشرطية – قطر

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

ملخص البحث:

يهدف هذا البحث إلى معرفة فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية، ولتحقيق الهدف العام من هذا البحث تم اتباع المنهج التحليلي، والمنهج المقارن، وتوصل البحث إلى مجموعة من النتائج أهمها: اتفقت التشريعات المقارنة التي تعاقب على الجرائم الإلكترونية أنها جريمة عمدية لا تقوم بصورة الخطأ، وإنما جريمة متكاملة العناصر، وأن هنالك قصور تشريعي في القواعد والإجراءات الواجب اتباعها في مرحلة التحقيق ومرحلة المحاكمة في قوانين مكافحة الجرائم الإلكترونية، وتتم المحاكمة في الجرائم الإلكترونية ذات الإجراءات المتبعة في الجرائم التقليدية.

وتم التوصل في هذا البحث إلى ضرورة سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملاً للقواعد الموضوعية والإجرائية، وضرورة تفعيل التعاون الدولي ومبدأ المساعدة القانونية والقضائية المتبادلة وتسليم المجرمين على المستوى العربي، وتدريب أعضاء الضابطة العدلية، والنيابة العامة، والقضاة في التعامل مع الجرائم الإلكترونية.

المقدمة:

بات الانتشار الواسع والتطور التقني والإنترنت في مختلف أنحاء العالم، والاستخدام المتزايد لمواقع التواصل الاجتماعي مثل موقع (Face book) وموقع (Twitter) من الامور الحياتية المهمة وأداة مساعدة وفاعلة في تطوير وتنمية استراتيجيات المؤسسات العامة والخاصة، والأفراد وتمكنهم من التقدم، وقد كانت الدول المتقدمة سباقة في الاستفادة منها ومواكبتها، وأصبح من الصعوبة الاستغناء عنها.

ورغم هذه الإيجابيات التي وفرتها هذه البرامج والشبكات الإلكترونية، لكن في المقابل أفرزت أنواعاً جديدة من الجرائم ألا وهي الجرائم الإلكترونية، والسيبرانية ، التي تُعد خطراً يطال كل المجمعات البشرية بالأزمات السياسية والاقتصادية والاجتماعية، والثقافية والأمنية، فالهاكرز موجودون في كل مكان يخترقون أجهزة الحواسيب والهواتف الذكية، إما للسطو على معلومات وابتزاز الأفراد أو التشهير بهم سواءً كانوا أفراداً عاديين أو مؤسسات، إضافة إلى سرقة الحسابات البنكية والخروقات لتجنيد الفتيات والشباب وحتى الأطفال في الأعمال التخريبية.

وتعد الجرائم الإلكترونية من الجرائم الحديثة التي ظهرت نتيجة لظهور أنظمة المعلومات ذاتها، ويعتبر ذلك أمر طبيعي نتيجة لتطور مجالات الحياة بشكل عام، باعتبار أن كلما تطور المجتمع تكنولوجياً كلما ظهرت جرائم حديثة لم تكن موجودة في السابق.

وقد بذلت جهود دولية في مكافحة الجرائم الإلكترونية من خلال الاتفاقيات والمؤتمرات التي تحث الدول على تجريم الجرائم الإلكترونية، ونتيجة لذلك سارعت الكثير من بلدان العالم لسن تشريعات قانونية لمكافحة الجرائم الإلكترونية ومنها العديد من البلاد العربية، شأنها شأن باقي الدول في العالم التي تأثرت بموجة من التطور والتقدم، فمثلاً نجد أن المشرع القطري أصدر قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة (2014)، وهو من أحدث القوانين في هذا المجال، وتضمن (54) مادة، موزعة على خمسة فصول، حاول المشرع القطري من خلالها التطرق لمختلف صور الجريمة الإلكترونية، ووضع نصوص التجريم المناسبة لها،

من هذا المنطلق سنتناول فاعلية التشريعات والقوانين العربية في مكافحة الجرائم الإلكترونية بالبحث والتحليل، ودراسة فائدتها في مكافحة الجرائم الإلكترونية.

إشكالية البحث:

سـارعت العديد من الدول العربية لإيجاد تشريعات خاصة لمكافحة الجرائم الإلكترونية، فضلاً عن الاتفاقيات الدولية، والتي تهدف إلى تعزيز التعاون الدولي والإقليمي لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية، لذا يمكن صياغة مشكلة البحث بالتساؤل الرئيس الآتي: ما مدى فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية؟

ويتفرع عن هذه الإشكالية العناصر الآتية:

1. ما خصائص الجرائم الإلكترونية في التشريعات العربية؟
2. ما آليات مواجهة الجرائم الإلكترونية في التشريعات العربية؟

أهمية البحث:

تكمن أهمية البحث بالآتي:

1. تسليط الضوء على قانون مكافحة الجرائم الإلكترونية القطري بشأن النصوص الواردة، باعتباره قانون حديث نسبياً مقارنة بباقي التشريعات العربية.
2. بيان خطورة الجرائم الإلكترونية، وما قد تؤدي إليه من أخطار جسيمة على الأمن والنظام في الدول العربية.
3. بيان العوائق التي يمكن أن تحول دون فاعلية التشريعات العربية المتعلقة بمكافحة الجرائم الإلكترونية.
4. قلة الدراسات والبحوث العربية التي تناولت الجرائم الإلكترونية وفاعليتها في مكافحة الجرائم الإلكترونية.
5. إفادة الباحثين والمختصين والجهات المعنية بموضوع البحث.
6. يتأمل الباحث أن يضيف إضافة نوعية في هذا المجال.

أهداف البحث:

يهدف هذا البحث إلى التعرف على فاعلية التشريعات والقوانين العربية في مكافحة الجرائم الإلكترونية، إضافة إلى الطبيعة القانونية للجرائم الإلكترونية وأركانها، والمواجهة الإجرائية للجرائم الإلكترونية ابتداء من وقوع الجريمة مروراً بمرحلتي التحقيق والمحاكمة، إضافة إلى إثراء المكتبة القانونية العربية ودولة قطر فبشكل خاص في هذا النوع من الدراسات وذلك تعزيزاً للمراجع والكتب القانونية والكتب الفقهية التي تناولت هذا الموضوع الهام.

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

منهجية البحث:

لجأ الباحث إلى المنهج التحليلي لتحليل النصوص وأقوال الفقهاء ومناقشتها، ومن ثم مقارنتها من أجل الوقوف على جوانب القصور بهدف تلافيها، أو لإظهار ميزتها، ولتقوية ودعم موضوع الدراسة لجأت إلى المنهج المقارن في القوانين العربية المتعلق بمكافحة الجرائم الإلكترونية، ومنها قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة (2014) من خلال استقراء جميع النصوص القانونية والأحكام القضائية المتعلقة بهذا الموضوع في هذه الدول.

خطة البحث:

المبحث الأول: ماهية وخصائص الجرائم الإلكترونية في التشريعات العربية
المطلب الأول: مفهوم الجريمة الإلكترونية
المطلب الثاني: الطبيعة القانونية للجرائم الإلكترونية وأركانها
المطلب الثالث: خصائص الجرائم الإلكترونية
المطلب الرابع: أسباب الجرائم الإلكترونية
المبحث الثاني: مواجهة الجرائم الإلكترونية في التشريعات العربية
المطلب الأول: التحقيق في الجرائم الإلكترونية
المطلب الثاني: المحاكمة في الجرائم الإلكترونية
المطلب الثالث: المعوقات التشريعية لمواجهة الجرائم الإلكترونية
المطلب الرابع: رؤيا استراتيجية لمواجهة الجرائم الإلكترونية

المبحث الأول

ماهية وخصائص الجرائم الإلكترونية في التشريعات العربية

تطرقت العديد من التشريعات العربية ومن بينها المشرع القطري إلى توسيع نطاق التجريم في الجرائم الإلكترونية نظراً لخطورة هذه الجرائم، لما تسببه من أضرار وخسائر كبيرة سواءً على مستوى الدول، أو المؤسسات العامة والخاصة، أو الأفراد، وللتعرف على هذا النوع المستحدث من الجرائم تم تقسيم هذا المبحث إلى أربعة مطالب، نتناول في المطلب الأول مفهوم الجريمة الإلكترونية، أما المطلب الثاني الطبيعة القانونية للجرائم الإلكترونية وأركانها ، وفي المطلب الثالث خصائص الجرائم الإلكترونية، وأخيراً المطلب الرابع أسباب الجرائم الإلكترونية.

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

المطلب الأول

مفهوم الجريمة الإلكترونية

لم يستقر الفقه على وضع تعريف محدد للجريمة الإلكترونية، كون الجرائم المستحدثة تتطور من حين إلى آخر، وهنالك من أطلق على هذه الجريمة المعلوماتية، أو جرائم الحاسوب والكمبيوتر، أو جرائم الإنترنت، أو جرائم الشبكة العنكبوتية، أو جرائم تقنية المعلومات.

وقد عرفها جانب من الفقه بأنها ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعلها[1].

وعرفها آخر بأنها كل جريمة ترتكب في محيط أجهزة الحاسوب، أو كل سلوك غير مشروع أو غير أخلاقي، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها[2].

وعرفت أيضاً بأنها الجرائم التي يكون فيها الحاسوب وسيلة ارتكاب فعل غير مشروع، أو محل لوقوع الفعل غير المشروع، وذلك بالقيام بعمل أو الامتناع عن أدائه من شأنه الاعتداء على الأموال المادية أو المعنوية، شريطة أن يكون مرتكبها على معرفة بتقنية استخدام الحاسوب والتعامل مع معطياته[3].

وعرفها المشرع الكويتي على اسم هذه الجرائم بجرائم تقنية المعلومات، حيث جاء تعريف الجريمة المعلوماتية بأنها كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون [4]، وأوضح المشرع الكويتي في هذا القانون العديد من المصطلحات المرتبطة بالجريمة الإلكترونية مثل (البيانات الإلكترونية، الشبكة المعلوماتية، وسيلة تقنية المعلومات، الدخول غير المشروع، التوقيع الإلكتروني)، حيث نجد أن المشرع الكويتي حاول في هذا القانون شرح وتوضيح بعض النصوص المتعلقة بهذا النوع من الجرائم، وهو أمر يحقق مبدأ المشروعية.

وأطلق المشرع السعودي على هذه الجريمة مسمى "الجريمة المعلوماتية "وعرفها بأنها كل فعل يُرتكب متضمناً الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام[5]، أما القانون العماني أطلق على تسميتها " جرائم تقنية المعلومات، واكتفى بالقول بأنها الجرائم المنصوص عليها في هذا القانون.

(1) د. علي جبار الحسيني، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، ط1، عمان، الأردن، 2009، ص33.
(2) د. خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، ط1، الإسكندرية، مصر، 2011، ص357-358.
(3) د. خالد عياد الحلبي، إجراءات التحقيق والتحري في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2011، ص31.
(4) قانون مكافحة جرائم المعلومات التقنية رقم (63)، لسنة (2015).
(5) نظام مكافحة الجرائم المعلوماتية السعودي رقم (79) (1428هـ).

في حين أطلق المشرع القطري على هذه الجريمة بالجريمة الإلكترونية، وعرفها بأنها أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون[6]. وقد حدد المشرع القطري في هذا القانون المصطلحات المرتبطة بالجريمة الإلكترونية:

1. تقنية المعلومات: 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.
2. البيانات والمعلومات الإلكترونية: 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.
3. الشبكة المعلوماتية: ارتباط بين أكثر من وسيلة لتقنية المعلومات، للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة والعامة والشبكة العالمية "الإنترنت".
4. نظام معلوماتي: مجموعة برامج وأجهزة، تستخدم لإنشاء أو استخراج المعلومات، أو إرسالها، أو استلامها، أو عرضها، أو معالجتها، أو تخزينها.
5. البرنامج المعلوماتي: مجموعة من البيانات أو الأوامر، القابلة للتنفيذ باستخدام وسيلة تقنية المعلومات والمعدة لإنجاز مهمة ما.
6. معالجة المعلومات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات أو المعلومات، سواء تعلقت بأفراد أو خلافه، بما في ذلك جمع واستلام وتسجيل وتخزين وتعديل ونقل واسترجاع ومحو تلك المعلومات.
7. بيانات المرور: 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.
8. المحرر الإلكتروني الرسمي: المحرر الرسمي الذي يصدر عن الجهات الحكومية أو الهيئات أو المؤسسات العامة باستخدام إحدى وسائل تقنية المعلومات.
9. الموقع الإلكتروني: مكان إتاحة أو معالجة البيانات أو المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد.
10. بطاقة التعامل الإلكتروني: البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو غيرها من وسائل تقنية المعلومات والتي تحتوي على بيانات أو معلومات إلكترونية والتي تصدرها الجهات المُرخّص لها بذلك.

ونلاحظ في هذا المقام أن المشرع القطري توسع في ذكر المفاهيم المتعلقة بالجرائم الإلكترونية أكثر من أي قانون آخر، وبإجراء مقارنة بسيطة بين هذه المفاهيم وتلك الواردة في القانون الكويتي والسعودي نلاحظ الدقة في التعبير عن المفاهيم والدقة في شرحها.

ويرى الباحث أن الجريمة الإلكترونية هي كل فعل أو امتناع عن فعل غير مشروع مخالف لأحكام القانون، يرتكبه شخص أو أكثر باستخدام جهاز الحاسوب مما يتسبب ضرراً للغير يستوجب ايقاع العقوبة على الفاعل.

(6) المادة (1) من قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة (2014).

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

المطلب الثاني

الطبيعة القانونية للجرائم الإلكترونية وأركانها

للحديث عن الطبيعة القانونية للجريمة الإلكترونية وحول الوضع القانوني للبرامج والمعلومات، إضافة إلى أركانها، الركن الشرعي، والركن المادي، والركن المعنوي، سنتناول هذا المطلب من خلال فرعين.

الفرع الأول: الطبيعة القانونية للجريمة الإلكترونية

انقسم الفقه إلى اتجاهين لتحديد الطبيعة القانونية للجريمة الإلكترونية، الأول يرى أنه وفقاً للقواعد العامة أن الأشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ، وأن الشيء موضوع السرقة يجب أن يكون مادياً أي له كيان مادي ملموس حتى يمكن انتقاله وحيازته عن طريق الاختلاس المكون للركن المادي في جريمة السرقة، ولما كانت المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ، إلا في ضوء حقوق الملكية الفكرية، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة، ما لم تكن مسجلة على اسطوانة أو شريط ، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية، فلا تثور مشكلة قانونية في تكييف الواقعة على أنها سرقة مال معلوماتي ذو طبيعة مادية، وإنما المشكلة تثور عندما نكون أمام سرقة مال معلوماتي غير مادي[7].

والاتجاه الثاني يرى أن المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية ، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وأنها ترتبط كما يقول الأستاذان "Catala و Vivant" بمؤلفهما عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال[8].

وهنالك من يرى إنه يجب أن نفرق بأن هناك مالاً معلوماتياً ماديّاً فقط ولا يمكن أن يخرج عن هذه الطبيعة وهي آلات وأدوات الحاسب الآلي مثل وحدة العرض البصري ووحدة الإدخال ، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية وهي المال المادي كالشريط الممغنط أو الاسطوانة الممغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات من على بعد ، كما هو الحال في جرائم التجسس عن بعد ، إذن من المنطق القول إذا حدثت سرقة فإنه لا يُسرق المال المسجل عليه المعلومة والبرامج لقيمته المادية وهي ثمن الشريط أو ثمن الاسطوانة ، وإنما يسرق ما هو مسجل عليهما من معلومات وبرامج [9].

ويرى أصحاب هذا الرأي أن الاعتداد بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي البرامج والمعلومات، وأنها لا يمكن أن تكون شيئاً ملموساً محسوساً، ولكن لهما كيان مادي قابل للانتقال والاستحواذ عليه بتشغيل الجهاز ورؤيتهما على الشاشة مترجماً إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها

(7) د. مفتاح بوبكر المطردي، الجريمة الإلكترونية، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 2012، ص17.
(8) د. محمد عبدالله سلامة، موسوعة الجرائم المعلوماتية، المكتب العربي الحديث، ط1، الإسكندرية، مصر، 2007، ص43-44.
(9) د. جلال محمد الزعبي، وأسامة المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2013، ص36-37.

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

إلى معلومات معينة لها أصل صادرة عنه يمكن سرقته، وبالتالي لها كيان مادي يمكن الاستحواذ عليه (البرامج والمعلومات)، واستطرد أصحاب هذا الاتجاه في القول بأنه طالما أن موضوع الحيازة غير مادي فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادية، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر[10].

الفرع الثاني: أركان الجريمة الإلكترونية

للجريمة الإلكترونية أو الجريمة التقليدية هنالك أركان رئيسية لقيامها، وهي:

أولاً: الركن الشرعي (القانوني): يسود التشريعات الجنائية المعاصرة مبدأ أساسي مهم وهو "لا جريمة ولا عقوبة إلا بناءً على نص"، وهو ما يسمى بمبدأ شرعية الجريمة والعقوبة، ومفاد هذا المبدأ حصر نصوص مصادر التجريم والعقاب في القانون المكتوب[11]. ومن الدساتير الحديثة التي نصت على هذا المبدأ دستور دولة قطر الدائم لسنة 2004[12]؛ حيث جاء في المادة (40) منه: "لا جريمة ولا عقوبة إلا بقانون". ومدلول هذا النص أنَّه لا يُقضى بأي عقوبة لم يرد عليها نص في القانون وقت ارتكاب الجريمة.

لذا؛ يمكن القول بأنَّ كل فعل مُجَرَّم في القانون يجب أن يكون له نص قانوني مكتوب يحدد العقوبة الواجب تطبيقها، والمشرع هو الذي يملك سلطة بيان وتحديد الأفعال المُعاقَب عليها والعقوبات التي توقع على مُرتكِبيها، وهذا ما نص عليه المشرع القطري في قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، حيث حدد في الباب الثاني هذه الجرائم في الفصل الأول بجرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، وفي الفصل الثاني جرائم المحتوى، جرائم التزوير والاحتيال الإلكتروني، وجرائم بطاقة التعامل الإلكتروني، جرائم التعدي على حقوق الملكية الفكرية، والعقوبات المقررة لهذه الجرائم، وبهذه النصوص القانونية تتحدد سلطة القاضي الجزائي، فهو لا يستطيع أن يقرر عقوبة لفعل لم يرد نص بالعقاب عليه، ولا أن يوقع عقوبة غير منصوص عليها، وفي الحدود المبينة قانوناً.

ثانياً: الركن المادي: يتكون الركن المادي للجريمة من ثلاثة عناصر، السلوك الإجرامي، والنتيجة التي يعاقب عليها المشرع، ووجود علاقة سببية تربط بين كل من السلوك الإجرامي والنتيجة، كما أن الأصل أن يتطلب المشرع لقيام الجريمة النتيجة الإجرامية التي يحددها السلوك والنتيجة الإجرامية، لكن هنالك من الجرائم التي يُكتفى فيها السلوك الإجرامي للمعاقبة عليها دون إحداث نتيجة معينة، ويسمى النوع الأول بالجرائم المادية أو بجرائم ذات النتيجة، بينما تسمى الثانية بالجرائم الشكلية أو بجرائم السلوك المحض[13]، فالمشرع القطري أكتفى بالسلوك أو النشاط الإجرامي لكي يتحقق الركن المادي للجريمة، دون النظر إلى العلاقة السببية، والنتيجة، فيكتفي أن يباشر المجرم نشاطه الإجرامي ليتحقق الركن المادي للجريمة، وهذ ما ذهب إليه المشرع الأردني لقيام الركن المادي للجريمة، إلا إذا كانت الجريمة تتطلب تحقيق نتيجة معينة، وهذا ما نص عليه في المادة (65) من قانون العقوبات الأردني رقم (16)

(10) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، ط1، القاهرة، مصر، 1992، ص51-52.

(11) د. نظام توفيق المجالي، شرح قانون العقوبات– القسم العام– دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص122-142.

(12) دستور دولة قطر الدائم لسنة 2004.

(13) أ. خالد سليمان الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري – دراسة مقارنة، رسالة ماجستير، جامعة قطر، 2019، ص24.

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

لسنة 1960 حيث نص على أنه "لا عبرة للنتيجة إذا كان القصد أن يؤدي إليها ارتكاب الفعل إلا إذا ورد نص صريح على أن نية الوصول إلى تلك النتيجة تؤلف عنصراً من عناصر الجرم الذي يتكون كله أو بعضه من ذلك الفعل[14].

ويرى الباحث أنه لكي يتوفر الركن المادي للجرائم الإلكترونية لا بد من وجود بيئة رقمية تتمثل في جهاز حاسوب، أو هاتف ذكي، وأن يكون هذا الجهاز أو الهاتف متصل بالإنترنت، فبدون جهاز حاسوب أو هاتف ذكي، وإنترنت، لا يمكن أن يتحقق الركن المادي للجريمة الإلكترونية، وقد يكون السلوك ايجابياً بمباشرة الفعل من الجاني وهو أغلب صور الجرائم الإلكترونية، والذي يرتكب على هيئة فعل مادي باستخدام إحدى الوسائل الإلكترونية، وقد يكون السلوك سلبياً بالامتناع عن فعل كان من الواجب اتيانه.

وتتحقق النتيجة في الجرائم الإلكترونية مثلاً كالطبيب الذي يدخل إلى قاعدة بيانات المستشفى عن طريق الإنترنت من أي مكان آخر، ثم يقوم بتغيير معدل دواء لأحد المرضى بهدف قتله، فإذا مات المريض تحققت النتيجة الجرمية لسلوك الطبيب[15]، وتتمثل العلاقة السببية في الجرائم الإلكترونية أن يكون هنالك إنترنت متصل بجهاز حاسوب، ومن ثم تم اختراق هذا الجهاز من موقع آخر والوصول إلى البيانات، وعندها يتم نشر هذه البيانات أو الصور.

ثالثاً: الركن المعنوي: يقصد بالركن المعنوي أن تكون هنالك إرادة لدى الجاني بتحقيق النتيجة الجرمية، والمقصود هنا عنصري هذا الركن العلم والإرادة، وفي إطار ذلك نص المشرع القطري على الركن المعنوي صراحة في نص المادة رقم (32) من قانون العقوبات القطري: " يتكون الركن المعنوي للجريمة من العمد أو الخطأ ، يتوفر الخطأ باتجاه إرادة الجاني إلى ارتكاب فعل أو امتناع عن فعل، بقصد احداث النتيجة التي يعاقب عليها القانون بسبب خطأ الجاني، سواءً كان الخطأ بسبب الاهمال أو عدم الانتباه أو عدم الاحتياط أو الطيش أو الرعونة أو عدم مراعاة القوانين أو اللوائح، ويسأل الجاني عن الجريمة سواءً ارتكبها عمداً أو خطأ، ما لم يشترط القانون توفر العمد صراحة "[16]، فالجرائم الإلكترونية تُرتكب بشكل قصدي، وذلك بسبب طبيعة هذه الجرائم، حيث يكون لدى الجاني القدرة على استخدام الحاسوب، والبيئة الإلكترونية، وغالباً يكون مرتكب هذه الجرائم من أشخاص اذكياء لديهم مهارات عالية في استخدام الإنترنت، وبالتالي يكون لديه العلم والإرادة الكاملة بتحقيق النتيجة الجرمية.

المطلب الثالث

خصائص الجرائم الإلكترونية

مما لا شك فيه أن تطور التقنية ووسائل الاتصال الإلكتروني بمختلف أنواعه صاحبه تطور في الجريمة يتماشى وهذا التطور التكنولوجي، وبذلك أصبحت الجريمة الإلكترونية لا تقل خطورة عن الجريمة العادية، إذ تُعد جريمة ذات طابع خاص، ومن خصائص الجرائم الإلكترونية:

أولاً: الجريمة الإلكترونية عابرة للحدود: من أهم الخصائص التي تميز الجريمة الالكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، وبسبب السرعة الهائلة في تنفيذها

(14) المادة (65) من قانون العقوبات الأردني رقم (16) لسنة 1960
(15) د. خالد إبراهيم ممدوح، مرجع سابق، ص388.
(16) المادة (32) من قانون العقوبات القطري، لسنة (2004).

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

وحجم الأموال والأشخاص المستهدفة من خلالها، ومن أهم القضايا التي أكدت هذه الخاصية، قضية عرفت باسم مرض نقص المناعة المكتسبة إيدز، وتتلخص وقائعها عام (1989) ، حيث قام أحد الأشخاص وهو "جوزيف بيب" بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الإيدز، لكن في الحقيقة يحتوي هذا البرنامج على "فيروس" يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل فيقوم الفاعل أو الجاني بطلب مبلغ مالي للحصول على عنوان إلكتروني مضاد للفيروس، وفي الثالث من فبراير تم إلقاء القبض على الجاني في "أوهايو" بالولايات المتحدة الأمريكية وطلبت المملكة المتحدة تسليم الجاني لإرساله البرنامج على أراضيها، وبالفعل تمت محاكمته أمام القضاء الانجليزي [17].

لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم، وهذا ما تناوله المشرع القطري بموجب قانون رقم (14) لسنة (2014) المتعلق بمكافحة الجرائم الإلكترونية والمتضمن القواعد الخاصة للوقاية من الجرائم الإلكترونية ومكافحتها بسن أحكام خاصة بالتعاون والمساعدة القضائية والدولية المتبادلة عن طريق المواد من (23 إلى 34).

ثانياً: يتميز مرتكبو الجرائم الإلكترونية بصفات خاصة: يتميز المجرم في الجرائم الإلكترونية عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي النمطي بعدة خصائص عددها الأستاذ Parker فيما يلي[18]:

1. الجاني شخص متخصص ومحترف في تنفيذ جريمته الإلكترونية.
2. لا يقوم الجاني باللجوء إلى العنف في تنفيذ جرائمه، فهو مجرم ذكي يتمتع بالمهارة والمعرفة وبدرجة عالية من الثقافة.
3. هنالك عدة أنواع من مرتكبي هذه الجرائم:

أ. الأشخاص الذين يرتكبون الجرائم الإلكترونية بغرض التسلية والمزاح مع الآخرين دون إحداث أي ضرر ويسمونهم Pranskers.

ب. الأشخاص الذين يستهدفون الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بهدف الفضول أو اكتساب الخبرة أو لمجرد القدرة على اختراق هذه الأنظمة ويسمون Hackers.

ج. الأشخاص الذين يستهدفون الحاق خسائر بالمجني عليهم، دون ان يكون الحصول على مكاسب مالية ضمن هذه الأهداف، ويندرجون تحت طائفة مخترعي فيروسات الحاسبات الآلية وموزعيها ويسمون Malicieuses hackers.

د. الأشخاص الذين يهدفون إلى إلحاق الأذى بالمجني عليهم، ويكون الباعث إيجاد حلول لمشاكل مادية تواجه الجاني لا يستطيع حلها بالطرق العادية ويسمون بـ: Personnel probleme solvers .

هـ. الأشخاص الذين يهدفون إلى تحقيق ربح مادي بطريق غير مشروع ويسمون بـ: Creen criminals.

ثالثاً: صعوبة الإثبات في الجرائم الإلكترونية: من أهم خصائص الجرائم الإلكترونية أنها صعبة الإثبات لأسباب ترجع إلى الجاني أو إلى المجني عليه، وإلى وسيلة تنفيذها، حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة باستخدام الإنترنت، إضافة إلى أن الجاني مجرم محترف ذكي مثقف لا يترك آثاراً جانبية خارجية للجريمة مما يصعب إثباتها، كما أن المجني عليهم غالباً مؤسسات

(17) أ. سوير سفيان، الجرائم المعلوماتية، رسالة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010، ص12.

(18) د. جلال محمد الزعبي، وأسامة المناعسة، مرجع سابق، ص122-137.

عامة أو خاصة يحجمون عن الإبلاغ عنها تجنباً للإساءة إلى السمعة وهز الثقة، فضلاً عن إمكانية تدمير الدليل في مدة زمنية قياسية [19].

المطلب الرابع

أسباب الجرائم الإلكترونية

تتعدد الأسباب التي تكمن وراء الجرائم الإلكترونية، منها ما يكون بسبب الثروة المعلوماتية على الإنترنت، ومنها ما يكون على مستوى شخصي، إضافة إلى تفاوت ارتكابها وفق نوعها والجاني، ومستوى تنفيذها.

أولاً: الأسباب شخصية: حيث أن هنالك بعض الجرائم الإلكترونية التي يرتكبها شباب صغار السن، وذلك من باب التحدي، وحب الظهور، إضافة إلى البيئة ودورها في إنتاج الجريمة والخروج على قواعد الامتثال، وفي أي مكان وعدم وجود رقابة إذ كلها عوامل تزيد من فرصة ارتكاب الجريمة الإلكترونية، كذلك النشاط الروتيني للناس فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية والترفيه والتجارة ...الخ[20].

ثانياً: الأسباب المجتمعية: تُعد الأسباب المجتمعية من أهم أسباب ارتكاب الجرائم الإلكترونية، فالتحضر مثلاً من أسباب الجريمة الإلكترونية عامة كالهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة، حيث لا تستطيع فئة الشباب من تلبية متطلباتهم الحياتية، مما يجعلهم يلتقون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير، إضافة إلى البطالة، والظروف الاقتصادية الصعبة حيث تتركز البطالة بين قطاعات كبيرة من الشباب، ولذا فإن الشباب الذين يملكون المعرفة سيستثمرون ذلك في النشاط الإجرامي الإلكتروني، ولا يمكن أيضاً تجاهل حب الثراء، حيث يسعى الجميع إلى المتعة، والحصول على الأموال بطرق مشروعة وغير مشروعة[21].

ثالثاً: الرقمنة: التغير في كمية ومقدار المعلومات المتدفقة ونوعها، ووجود الشبكات حيث يتم تداول المعلومات بين جميع الأطراف مثل البريد الإلكتروني أو الجوال، لذا يُعد هذا العصر عصر الفضاء الإلكتروني أو العالم الافتراضي.

رابعاً: العولمة: إن ظهور العالم الافتراضي يخلق ظواهر جديدة متميزة عن وجود أنظمة الحاسوب نفسها والفرص المباشرة للجريمة والتي وفرتها أجهزة الحاسوب الآن ضمن الفضاء الإلكتروني قد يظهر الأشخاص الفروق في امتثالهم الخاص، أو وعدم الامتثال مقارنة مع السلوك التقليدي، فالأشخاص على سبيل المثال، قد يرتكبون جرائم في العالم الافتراضي لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم.

(19) د. يونس عرب، جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، 2002، ص8.
(20) د. محمد الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص81-92.
(21) د. ممدوح عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الحقوق، ط1، 2001، ص78.

خامساً: سرعة ارتكاب الجرائم الإلكترونية: لا يتطلب غالباً تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر، وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة[22].

ويضيف الباحث أيضاً إن من أسباب ارتكاب الجرائم الإلكترونية المعلومات المتوفرة في كل مكان، والمتعة في ارتكاب هذا النوع من الجرائم، وقلة الرقابة من قبل الأسرة على أفرادها ، إضافة إلى جذب الأموال لما تمثله سوق المعلومات والحاسب والإنترنت من ثروة كبيرة للمجرمين، فقد غدت أكثر جذباً لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكّن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات الإلكترونية.

المبحث الثاني

مواجهة الجرائم الإلكترونية في التشريعات العربية

نتيجة التطور المتسارع والانفتاح العالمي والعولمة ، فقد بات العديد من الجرائم يتم ارتكابها من خلال شبكة الإنترنت، ونتيجة التنظيم الإلكتروني لهذا النمط من الجرائم فقد أُضيفت صفة التعقيد، وصعوبة الملاحقة لمرتكبي هذه الجرائم، وكان لا بُد من وجود إطار تشريعي قانوني لمواجهة هذه الجرائم في الوطن العربي[23]، ولتحقيق الهدف من هذا المبحث سنتناول التحقيق في الجرائم الإلكترونية في المطلب الأول، وفي المطلب الثاني المحاكمة في الجرائم الإلكترونية ، أما المطلب الثالث فسيعرض للمعوقات التشريعية لمواجهة الجرائم الإلكترونية ، وفي المطلب الرابع تم اقتراح رؤيا استراتيجية لمواجهة الجرائم الإلكترونية.

(22) د. جلال محمد الزعبي، وأسامة المناعسة، مرجع سابق، ص143–152.

(23) نماذج لبعض القوانين العربية القائمة الخاصة بمكافحة الجرائم الإلكترونية:

- دولة قطر : قانون مكافحة الجرائم الالكترونية رقم (14) لسنة 2014.
- دولة الكويت: قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، صدر بتاريخ 7/ 7/ 2015م.
- الإمارات العربية المتحدة: القانون الاتحادي رقم (5) لسنة (2012) في شأن مكافحة جرائم تقنية المعلومات.
- المملكة العربية السعودية: نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقـم م/ 17 وتاريخ: 1428/3/8هـ.
- سلطنة عُمان: قانون مكافحة جرائم تقنية المعلومات بالرقم 2011/12م في 6/2/2011 .
- مملكة البحرين: قانون رقم (60) لسنة (2014) بشأن جرائم تقنية المعلومات.
- الأردن: قانون الجرائم الإلكترونية رقم (27) لسنة 2015م.

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

المطلب الأول

التحقيق في الجرائم الإلكترونية

يُعد التحقيق أول مرحلة من مراحل الدعوى الجزائية، وهو عبارة عن إجراءات تتخذها السلطات المختصة بالتحقيق من أجل جمع المعلومات والأدلة التي تساعد على التحقيق في الجريمة، وهنالك مجموعة من الإجراءات يجب اتباعها في هذا الإطار للحصول على الدليل على وقوع الجريمة، وسنتناول في هذا المطلب التفتيش والخبرة فقط لكونهما أكثر الإجراءات تماساً وأهمية في نطاق الجريمة الإلكترونية:

أولاً: التفتيش: يُقصد بالتفتيش البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ما له علاقة بها أو بفاعلها، والتفتيش في الجرائم الإلكترونية إما أن يكون عن المكونات المادية للحاسوب، أو يكون عن المكونات المعنوية مثل البيانات والمعلومات، ويختلف تفتيش الكيانات المادية وتفتيش الكيانات المعنوية في الآتي:

1. تفتيش المكونات المادية للحاسب الآلي: إن التفتيش المتعلق بالكيانات المادية في نطاق الجرائم الالكترونية يسهل إجراؤه وتنطبق عليه القواعد التقليدية للتفتيش، إذ لا خلاف على إن الولوج إلى المكونات المادية للحاسوب بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يُفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الأماكن العامة أو من الأماكن الخاصة، حيث إن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حرمة، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها التفتيش وبنفس الاجراءات المقررة قانوناً في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت مكونات الحاسوب المراد تفتيشها منعزلة عن غيرها من أجهزة الحاسوب الأخرى، أم إنها متصلة بحاسوب آخر أو بنهاية طرفيه في مكان آخر كمسكن غير المتهم مثلاً، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود التي يستلزمها المشرع لتفتيش هذه الأماكن، أما إذا وجد شخص يحمل مكونات الحاسوب المادية أو كان مسيطراً عليها أو حائزاً لها في مكان ما من الأماكن العامة سواءً كانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أم كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالة التي يجوز فيها تفتيش الاشخاص وبنفس القيود المنصوص عليها في هذا المجال[24].
2. التفتيش عن المكونات المعنوية للحاسب الآلي: أثار تفتيش الكيانات المعنوية خلافاً كبيراً في الفقه، فذهب رأي في الفقه إلى جواز تفتيش وضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي شيء)، فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة، بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح أصحاب هذا الرأي لمواجهة هذا القصور التشريعي بالنص صراحةً على جواز تفتيش المكونات المعنوية للكمبيوتر[25].

(24) د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ط1، الإسكندرية، مصر، 2010، ص195-196.
(25) المرجع نفسه، ص197.

AJSP
المجلة العربية للنشر العلمي
العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

وقد تعرض المشرع الأردني لموضوع التفتيش عن الكيانات المعنوية للحاسب الآلي حيث نص على أنه: يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلال إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم[26].

وإذا ما تصفحنا المواد الخاصة بالتفتيش في قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة (2014) سنجد أن المشرع القطري نص في المادة (14) "للنيابة العامة أو من تندبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة ... ويجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة ... فإذا 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[27]، إضافة إلى ما نصت عليه المادة (15) من ذات القانون بقولها " لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية بسبب طبيعة ذلك الدليل"[28]، لذا يُستدل من النص السابق أن المشرع القطري قد أحسن التوجه حين نص صراحة على جواز التفتيش على الكيانات المعنوية للحاسب الآلي، وتلاشى الخلاف الذي من الممكن أن يحصل لو نص على خلاف ذلك، وهذا أيضاً ما نص عليه المشرع الأردني .

ثانياً: الخبرة: يقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة وفاعلها باتخاذ الاجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه، ومن ضمن هذه الاجراءات الاستعانة بأهل الخبرة وذلك تحقيقاً لمبدأ هام وهو مبدأ التخصص نظراً لكون الخبرة هي تقدير مادي أو ذهني يُبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها وبمعلوماته الخاصة سواءً أكانت تلك المسألة الفنية متعلقة بشخص المتهم أم بجسم الجريمة أم المواد المستعملة في ارتكابها أم آثارها[29].

إن اختيار الخبير في الجرائم الالكترونية يتوقف على نوع الجريمة المرتكبة ومجال الخبرة المطلوبة وطبيعتها الفنية، فلا يكفي حصول الخبير على درجة علمية معينة، وإنما ينبغي أن تكون لديه خبرة علمية تخصصية وكفاءة فنية عالية في حقل أو أكثر من حقول تقنية المعلومات ونظمها ووسائلها، فقد تكون الجريمة المرتكبة تزوير مستندات أو تلاعباً في البيانات أو الغش أثناء نقل أو بث البيانات أو إطلاق الفيروسات أو قرصنة أو اعتداء على حرمة الحياة الخاصة أو التجسس[30]، وقد نص المشرع القطري في المادة (18) من قانون مكافحة الجرائم الإلكترونية على أنه "للنيابة العامة أن تأمر كل ذي صلة بتسليم الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو معلومات المحتوى ذات الصلة بموضوع الجريمة أو ما يفيد في كشف الحقيقة ... وللنيابة العامة أنت تأمر بالتحفظ على الأجهزة أو الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة".

(26) المادة رقم (12) الفقرة (أ) من قانون جرائم أنظمة المعلومات الأردني رقم (9) لسنة 2010.
(27) المادة رقم (14) من قانون مكافحة الجرائم الإلكترونية القطري لسنة (2014).
(28) المادة رقم (15) من قانون مكافحة الجرائم الإلكترونية القطري لسنة (2014).
(29) د. سليم حربة، شرح قانون أصول المحاكمات الجزائية، ج1، بيروت، لبنان، 2009، ص126.
(30) أ. راشد بشير ابراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، بحث منشور في مجلة دراسات استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد (131)، 2008، 69.

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

المطلب الثاني

المحاكمة في الجرائم الإلكترونية

تُعد السلطة القضائية هي السلطة المختصة للفصل في المنازعات التي قد تنشأ الأفراد، أو بين الأفراد والسلطة، وقد منحت القوانين الوطنية هذه السلطة الاستقلالية في إصدار أحكامها، وفي الوقائع إن إجراءات المحاكمة في الجرائم التقليدية لا تختلف عن إجراءات المحاكمة في الجرائم الإلكترونية، مع العلم أن القاضي ينظر في قضايا ليس لديه الخبرة فيها، فعلى سبيل المثال استعان قاضي في باريس بخبيرين أحدهما انجليزي، والثاني أمريكي، إضافة إلى خبير فرنسي لأعداد تقرير حول إمكانية رصد مسار الإنترنت[31]، وتختلف مرحلة المحاكمة عن مرحلة التحقيق، حيث أن السلطة المختصة بالتحقيق هي النيابة العامة، أما السلطة المختصة هي المحاكمة يمثلها قضاة مستقلون، ولتوضيح التحقيق والمحاكمة في الجرائم الإلكترونية، سنتناول مرحلة المحاكمة في الجرائم الإلكترونية من خلال الآتي:

أولاً: المحكمة المختصة في الجرائم الإلكترونية: يختص القضاء القطري في الدعاوى والطلبات المدنية والجزائية المعروضة عليه، إضافة إلى القواعد القانونية التي تحدد اختصاص كل محكمة في النظر بالدعوى، ونص المشرع الأردني على المحاكم النظامية، وجعلها صاحبة الاختصاص بالنظر في الدعاوى المدنية والجزائية، حيث نص المشرع الأردني على أنه "تمارس المحاكم النظامية في المملكة حق القضاء على جميع الاشخاص في جميع المواد المدنية والجزائية باستثناء المواد التي يفوض فيها حق القضاء إلى محاكم دينية، أو محاكم خاصة بموجب أحكام أي قانون آخر[32].

ثانياً: إجراءات المحاكمة في الجرائم الإلكترونية: الإحالة هو الإجراء الذي يترتب عنه دخول الدعوى في اختصاص المحكمة، والأصل في المحاكمة أن تكون علنية لضمان الصالح العام، إلا أن القانون أجاز النظر في بعض الدعوى بطريقة سرية لا يحضرها الجمهور، وذلك لاعتبارات المحافظة على النظام العام والآداب، وقد صنف المشرع الأردني الجرائم الإلكترونية إلى جنايات وجنح، واعتقد أن المشرع الأردني قد أصاب في ذلك، لأنه ليس من العدل أن تكون جريمة الدخول إلى موقع مثل جريمة الاستغلال الجنسي للأطفال، وأيضاً هذا ما نص عليه المشرع القطري في المادة (49) يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القانون، بذات العقوبات المقررة للفاعل الأصلي ... إضافة إلى المادة (50) يعاقب كل من شرع في ارتكاب جناية أو جنحة معاقباً عليها بموجب أحكام هذا القانون بالحبس مدة لا تجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة التامة[33].

إضافة إلى ذلك نصت المادة (19) من قانون مكافحة الجرائم الإلكترونية القطري "على الجهة المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على الأجهزة أو الأدوات أو وسائل تقنية المعلومات، أو الأنظمة المعلوماتية أو البيانات أو المعلومات الإلكترونية محل التحفظ، لحين صدور قرار من الجهات القضائية المعنية بشأنها[34]، كما أخذ المشرع السعودي بحجية الدليل

(31) أ. عمر محمد يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة عين شمس، القاهرة، 2004، ص73.
(32) المادة (2) من قانون تشكيل المحاكم النظامية الأردني رقم (17) لسنة (2001).
(33) المادة (19) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة (2014).
(34) المادة (49، 50) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة (2014).

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

الإلكتروني في الإثبات، فقد نص قانون التعاملات الإلكترونية السعودي في المادة (2) على أن أهداف هذا النظام: إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بواسطة سجلات الإلكترونية يعول عليها[35].

المطلب الثالث

المعوقات التشريعية لمواجهة الجرائم الإلكترونية

يتوجب التعرف على التحديات وإبراز جوانبها سعياً لتجاوزها، ووضع التشخيص الأمثل للظاهرة ومكافحتها على صعيد التجريم والعقاب من ناحية، وعلى صعيد الملاحقة الإجرائية من ناحية أخرى، وهذا يستلزم أمرين؛ الأول: الاقتناع بخطورة هذه الظاهرة ، ومحاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية، والثاني تطوير البنية التشريعية الجنائية بذكاء تشريعي متواصل يسد ثغرات القوانين الجنائية على نحو يجعلها قادرة على إخضاع هذه الجرائم لأوصافها ونصوصها، ومواكبة التطورات التي يتوسل بها مرتكبو هذه الجرائم، على أن يتم هذا التطور في إطار القانون وكفالة احترام مبدأ شرعية الجريمة والعقوبة من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى[36]، وسنتناول المعوقات التشريعية للجرائم الإلكترونية من خلال فرعين.

الفرع الأول: عدم قدرة النصوص القانونية التقليدية التعامل مع الجرائم الإلكترونية

الجرائم الإلكترونية مثلها مثل الجرائم التقليدية تقع على الأشخاص وتقع على الأموال، إلا أن الاختلاف يظهر من جانبين، الأول في أداة الجريمة، فالأداة في الجرائم الإلكترونية تكون ذات تقنية عالية فائقة الأداء، فمن يقوم بهذه الجريمة يكون عادة أشخاص ذات ذكاء حاد، يعلم بطرق وادوات استعمال هذه الأداة ويبتكر طرق جديدة ووسائل تساعد في ارتكاب جريمته، وفي تجريم هذا النوع من الجرائم قد يتم اللجوء إلى النصوص القانونية التقليدية، ومثال ذلك جرائم السرقة والرشوة والتحرش، أما الثاني نوع آخر من الجرائم الإلكترونية لم يكن موجوداً، وظهر نتيجة التطور التقني والتكنولوجي الهائل، وهذا النوع من الجرائم لا يمكن التعامل معه وفق النصوص القانونية التقليدية.

وتكمن المشكلة في عدم قدرة تطبيق النصوص القانونية التقليدية على الجرائم الإلكترونية، وعدم وجود التشريعات القادرة على التعامل مع هذا النوع من الجرائم، وبما أن القاعدة الشرعية تقول "لا جريمة ولا عقوبة إلا بقانون" ومدلول ذلك أن القاضي لا يستطيع أن يتوسع في تفسير النصوص التقليدية لتطبيقها على الجرائم الإلكترونية، وقد ثار هذا الموضوع في القضاء الفرنسي للنظر في مدى تطبيق النصوص التقليدية على مثيلاتها المرتكبة في الجرائم الإلكترونية، ومن ذلك صدور حكم من القضاء الفرنسي باعتبار قيام موظف بإحدى الشركات بتصوير التصميمات الخاصة بآلة لتصنيعها وتسويقها بمشروع آخر بالاستعانة بهذه التصميمات سرقة دون البحث فيما إذا كانت هذه التصميمات بحمية ببراءة الاختراع[37].

(35) المادة (2) من قانون التعاملات الإلكترونية السعودي.
(36) د. مفتاح بوبكر المطردي، مرجع سابق، ص20.
(37) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، مصر، 2000، ص18.

العدد السابع والثلاثون
تاريخ الإصدار: 2 – تشرين الثاني – 2021 م
www.ajsp.net
ISSN: 2663-5798

الفرع الثاني: التعابير الفضفاضة

ترتب قواعد الجزاء عقوبات على منتهكيها، ولذلك فإن المتفق عليه والمستقر أن التشريعات الجزائية تتسم بدقة العبارات ووضوحها، وتلقي تبعة هذه المسؤولية على المشرع، الذي يجتهد في وضع الصياغات والعبارات المحددة والدقيقة، والتي تسهل على القاضي تطبيقها وتحديد المقصود منها، ويترتب على ذلك أن أي تفسير يتوسع به يجب أن يكون دائماً لمصلحة المتهم، ويجب أن تغلب كفة البراءة على كفة الإدانة، فإذا ما تناهى الشك إلى ضمير القاضي، فإنه يميل دائماً للبراءة، فالشك يفسر لمصحة المتهم، ويحكم القاضي بناءً على الأدلة والقرائن، ولا يحكم على أي شك أو تخمين، ولكن هذه العبارات انتشرت بشكل واسع في نصوص بعضها، مما يعتبر من قبيل الجرائم التقليدية، وبعضها الآخر مما يعتبر من قبيل الجرائم المعاصرة المستحدثة، والأمثلة على ذلك كثرة: الغش المعلوماتي، التزوير المعلوماتي، المساس بالمعطيات أو البرامج، إدخال بيانات وهمية، إدخال معلومات مزورة، التلاعب بالبرامج، التجسس الصناعي، تغير برامج التشغيل، خلق برامج جديدة، الدخول والبقاء غير المشروع في نظام المعاجلة الآلية للمعطيات[38].

المطلب الرابع

رؤيا استراتيجية لمواجهة الجرائم الإلكترونية

واكب تطور المجتمعات البشرية عبر التاريخ تطور في نوع الجرائم التي تعانيها هذه المجتمعات، الأمر الذي كان يدعو إلى تبني التشريعات والقوانين التي تحد من الآثار السلبية لهذه الجرائم على الفرد والمجتمع، ووضع استراتيجيات لمكافحة الجرائم الإلكترونية والتصدي لها، وبناءً عليه يمكن صياغة استراتيجية لمواجهة الجرائم الإلكترونية من خلال ما يلي:

أولاً: بلورة النصوص الدولية وضعها موضع للتنفيذ، ولهذا الغرض أبرمت العديد من الدول الإتفاقيات الدولية، ومن أبرزها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، البرتوكولات الملحقة بها ثم بعض الإتفاقيات التي أفردت بعض الجرائم بالمعالجة كذلك المتعلقة بالمخدرات وتبييض الأموال والفساد، وتمثلت هذه الآليات كلها بالخصوص في تدعيم التعاون الدولي لمواجهة فعالة لهذه الظاهرة التي أصبحت عالمية.

ثانياً: التعاون الدولي لمواجهة الجرائم الإلكترونية، يقتضي أولاً وضع قواعد جديدة للاختصاص خارج الحدود الوطنية، وثانياً وضع قواعد جديدة للتعاون الدولي على المستويين القضائي والأمني، والأهم من ذلك تفعيل دور التعاون الدولي بتعاون حقيقي بين الدول العربية لمواجهة الجريمة الإلكترونية.

ثالثاً: قيام الدول العربية باتخاذ عدد من التدابير والإجراءات لتجريم وعقاب مرتكبي تلك الجريمة وتعزيز الجانب الوقائي لمكافحة أنشطة الجريمة الإلكترونية، وتفعيل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك بتاريخ 2010/12/21، كما أدت هذه

(38) أ. مداوي سعيد القحطاني، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، جائزة الأمير نايف للبحوث الأمنية، بحث فائز بالمركز الأول، 2016، ص37.

الاتفاقية كذلك لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في قطر والأردن والسعودية والإمارات والعراق وسلطنة عُمان.

رابعاً: تعزيز مؤسسات العدالة الجنائية وزيادة الخبرات المهنية لدى الأخصائيين الممارسين في مجال مكافحة الجريمة الإلكترونية من خلال تحديد مجالات تدخُّل رئيسية لدعم الكشف المبكر عن التهديدات الجديدة والناشئة التي تثيرها الجريمة الإلكترونية، واعتماد وتنفيذ سياسات تكفل التصدّي بفعالية لتلك التهديدات.

خامساً: تعزيز القوانين الوطنية لمكافحة الجرائم الإلكترونية من خلال نقل معارف المحاكم الجنائية العربية وممارساتها والمساهمة في مكافحة الجريمة الإلكترونية.

سادساً: إنشاء منصَّة لإتاحة الوصول إلى البحوث المستندة إلى الأدلة للوقوف على أفضل الممارسات الدولية فيما يتعلق بالوقاية من الجرائم الإلكترونية، ونشر تلك الممارسات.

سابعاً: بناء القدرات في مجال منع الجريمة الإلكترونية والعدالة الجنائية، من خلال وضع نماذج متكاملة لإدارة المعارف، ونقل المعارف بأسلوب منهجي، وبناء الشبكات مع المؤسسات الأكاديمية والمنظمات الدولية ومراكز البحوث، والترويج لزيادة فهم حقوق الإنسان ومنع الجريمة الإلكترونية والعدالة الجنائية بهدف تعزيز سيادة القانون.

ثامناً: الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي: ويشمل ذلك الوعي بخطورة التهديدات وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية، مع الاهتمام بالاستعداد المسبق بما يشمل الخطط الاستراتيجية والتنفيذية وخطط الطوارئ وآليات التنسيق العرضي واعداد الكوادر والتجهيزات التقنية واللوجستية.

تاسعاً: وضع الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم الإلكترونية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات، وذلك بمشاركة عربية من وذوي الخبرة في القطاع الخاص ومؤسسات المجتمع المدني، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة، واعداد وتدريب المتخصصين في انفاذ القانون في الجهات القضائية والشرطية.

الخاتمة

بعد دراسة فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية وفق التشريع القطري، وبعض التشريعات العربية، توصلنا في ختام هذا البحث إلى مجموعة من النتائج والتوصيات.

أولاً: النتائج

1. تتميز الجرائم الإلكترونية بعدة خصائص لا نجدها في الجرائم الإلكترونية، مثل الطابع التقني، وكونها جريمة عابرة للحدود.
2. اتفقت التشريعات المقارنة التي تعاقب على الجرائم الإلكترونية أنها جريمة عمدية لا تقوم بصورة الخطأ، وإنما جريمة متكاملة العناصر.
3. تصدى المشرع القطري للجرائم الإلكترونية من خلال قانون خاص بمكافحة الجرائم الإلكترونية رقم (14) لسنة (2014).

4. وجود قصور تشريعي في القواعد والإجراءات الواجب اتباعها في مرحلة التحقيق ومرحلة المحاكمة في الجرائم الإلكترونية.
5. يتم الاستعانة في الخبراء في الجرائم الإلكترونية في جميع مراحل الدعوى (التحقيق، والمحاكمة).
6. تتم المحاكمة في الجرائم الإلكترونية ذات الإجراءات المتبعة في الجرائم التقليدية.

ثانياً: التوصيات

1. سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملاً للقواعد الموضوعية والإجرائية.
2. ضرورة منح سلطات الضبط والتحقيق إجراء تفتيش وضبط أي تقنية خاصة بالجريمة الإلكترونية تفيد في إثباتها.
3. ضرورة تفعيل التعاون الدولي ومبدأ المساعدة القانونية والقضائية المتبادلة وتسليم المجرمين على المستوى العربي.
4. تدريب أعضاء الضابطة العدلية، والنيابة العامة، والقضاة في التعامل مع الجرائم الإلكترونية.

المراجع

د. جلال محمد الزعبي، وأسامة المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2013.

د. خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، ط1، الإسكندرية، مصر، 2011.

د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ط1، الإسكندرية، مصر، 2010.

د.خالد عياد الحلبي، إجراءات التحقيق والتحري في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2011.

د. سليم حربة، شرح قانون أصول المحاكمات الجزائية، ج1، بيروت، لبنان، 2009.

د. علي جبار الحسيني، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، ط1، عمان، الأردن، 2009.

د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، ط1، القاهرة، مصر، 1992.

د. محمد الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

د. محمد عبدالله سلامة، موسوعة الجرائم المعلوماتية، المكتب العربي الحديث، ط1، الإسكندرية، مصر، 2007.

د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، مصر، 2000.

د. ممدوح عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الحقوق، ط1، 2001.

د. نظام توفيق المجالي، شرح قانون العقوبات– القسم العام– دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

خالد سليمان الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري – دراسة مقارنة، رسالة ماجستير، جامعة قطر، 2019.

راشد بشير ابراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، بحث منشور في مجلة دراسات استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد (131)، 2008.

سوير سفيان، الجرائم المعلوماتية، رسالة ماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010.

عمر محمد يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة عين شمس، القاهرة، 2004.

مداوي سعيد القحطاني، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، جائزة الأمير نايف للبحوث الأمنية، بحث فائز بالمركز الأول، 2016.

د. مفتاح بوبكر المطردي، الجريمة الإلكترونية، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 2012.

د. يونس عرب، جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، 2002

-القوانين

1. دستور دولة قطر الدائم لسنة 2004.
2. قانون مكافحة الجرائم الالكترونية القطري رقم (14) لسنة (2014).
3. قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (63) لسنة (2015).
4. قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (5) لسنة (2012).
5. قانون جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقــم م/ 17 (1428هـ).
6. قانون مكافحة جرائم تقنية المعلومات العماني الرقم (12) لسنة (2011).
7. قانون جرائم تقنية المعلومات البحريني رقم (60) لسنة (2014).
8. قانون جرائم أنظمة المعلومات الأردني رقم (9) لسنة (2010).
9. قانون مكافحة الجرائم الإلكترونية الأردني رقم (27) لسنة (2015).

Abstract:

The study aims to identify the effectiveness of the laws and regulations of the Arab countries in combatting cyber-crimes. To do so, we have adopted the analytical and comparative approach. The study reached a number of conclusions, the most important of which are: the compared laws incriminating cyber-crimes agreed that cyber-crime is an intentional crime that cannot occur accidentally and that it is a complete and integrated crime. Some shortcomings exist in the cyber crime combatting laws in terms of the rules and procedures to be followed during the investigation and the trial phases and cyber crimes are tried according to the same procedures followed in the conventional crimes.

The study concluded the necessity to fill the legislative gap in the arena of cyber crime combatting to include procedural and objective rules. The study pointed out the importance of activating the international cooperation and the principle of mutual legal assistance, the extradition of criminals between the Arab countries, the training of the judicial police officers, the public prosecution and the judges in dealing with cyber-crimes.