الأحكام العامة للمواجهة الجنائية لظاهرة جرائم تقنية المعلومات
دراسة مقارنة بين قانوني مكافحة جرائم تقنية المعلومات الكويتي والإماراتي

الدكتور/ بدر أحمد الجاسر الراجحي
أستاذ مساعد - قسم القانون الجزائي
كلية الحقوق - جامعة الكويت

ملخص:

الجريمة بذاتها لا تعد ظاهرة جديدة، وإنما هي ظاهرة قديمة قدم التاريخ إلا أن هذه الظاهرة بشكلها التقليدي أقل خطورةً وتطوراً عما هو قائم بالنسبة للجريمة المستحدثة التي ترتكب عبر شبكة الإنترنت بشكل متلاحق وسريع ومتطور نتيجة ظهور أدوات تقنية المعلومات مثل الحاسب الآلي والهاتف المحمول وغيرها، الأمر الذي أدى إلى ظهور ما يسمى بالجريمة الإلكترونية أو المعلوماتية والتي تشكل خطراً شديداً على الفرد وعلى المجتمع، ليس هذا فحسب بل يمتد أثر هذا النوع من الجرائم إلى أمن وأمان واستقرار الدول، ولذلك سلطنا الضوء في دراستنا على مكافحة هذه الجرائم من خلال القانون ٦٣ لسنة ٢٠١٥ الكويتي في شأن مكافحة جرائم تقنية المعلومات، وكذلك المرسوم بقانون رقم ٥ لسنة ٢٠١٢ الإماراتي تحت عنوان "الأحكام العامة للمواجهة الجنائية لظاهرة جرائم تقنية المعلومات: دراسة مقارنة بين قانوني مكافحة جرائم تقنية المعلومات الكويتي والإماراتي" ولابد من بيان خلاصة موجزة لما احتواه هذا البحث، والذي قسمناه إلى ثلاثة مباحث رئيسية يسبقها مطلب تمهيدي تناولنا فيه ظاهرة جرائم تقنية المعلومات على شبكة الإنترنت، من حيث مفهومه وتطوره والمصلحة محل الحماية. أما المبحث الأول فقد ناقشنا من خلاله أهم الأحكام الموضوعية لجرائم تقنية المعلومات عبر شبكة الإنترنت، فتطرقنا لبيان ركني الجريمة المادي والمعنوي في مطلب أول، ثم انتقلنا لمناقشة المساهمة الجنائية في مطلب ثانٍ. أما المبحث الثاني فتناولنا فيه أهم الأحكام الإجرائية لضعف تناولها من خلال التشريعات، كما أضفنا تطبيقاً لجرائم تقنية المعلومات وكيفية مكافحتها طبقاً لأحكام القوانين الصادرة في هذا الصدد فعرضنا جريمة الدخول غير المشروع للنظام المعلوماتي كمثال للجريمة المستحدثة لأهمية هذه الجريمة المستحدثة وذلك في مبحثٍ ثالث.

مقدمة:

لقد أدى التطور المتلاحق والمتجدد لدور الحاسب الآلي في المجتمع المعلوماتي إلى تزايد الوعي لدى الشعوب عن أهمية المعلومة باعتبارها مصدراً للقوة والثراء أحياناً، ومما ساعد على ذلك عمومية استخدام شبكة الإنترنت على مستوى العالم كله، وقد قدمت شبكة الاتصالات وأدوات تقنية المعلومات العديد من المزايا والتي ساعدت على القيام بالكثير من الأمور التي تعودنا على القيام بها بشكل معتاد، وإمكانية التواصل بين الأفراد دون أي اعتبار للقيود المكانية والزمانية، وكان لما يبث على شبكة الإنترنت ما يمثل خطورة وضرراً غير محدود على مستخدمي هذه الشبكة وبخاصة الشباب الذي يمكنه استخدام هذه الشبكة بشكل غير مشروع، مما جعلنا نعيش في فوضى معلوماتية عبر العالم الافتراضي، كما أدى إلى انتشار الجرائم المعلوماتية التي لا توجد رقابة حاسمة بصددها، حيث إن القوانين الجزائية لا تفي بالغرض المطلوب ولا يمكنها ملاحقة التطور الهائل في هذا العالم الافتراضي وخلال تلك الشبكة المعلوماتية سريعة التطور، ومن ثم فإن المشرع في التشريعات المقارنة قد اهتم بهذا الأمر وتدخل بوضع تشريع لمكافحة جرائم تقنية المعلومات سواء تشريعات الكويت أو الإمارات العربية المتحدة أو غيرها من التشريعات المقارنة، وذلك لملاحقة التطورات الحديثة والهائلة في هذا العالم الافتراضي.

أولاً – سبب اختيار موضوع الدراسة:

ترجع أسباب اختيار الدراسة والمشاكل التي تدور حولها إلى محاولة وضع مفهوم واضح لتعريف ماهية الجريمة المعلوماتية وتحديد المشكلات الخاصة بالأحكام الموضوعية والإجرائية المرتبطة بجرائم تقنية المعلومات في التشريعين الكويتي والإماراتي، والمساهمة في إيجاد الحلول للمشكلات العملية والتشريعية، وبيان نواحي القصور في التشريعات المقارنة محل الدراسة (الكويتي – الإماراتي) في هذا الصدد، ووضع ما توصلت إليه الدراسة بين يدي المشرع سواء في الكويت أو الإمارات العربية المتحدة، على أمل أن يكون هناك من يهتم بهذه التوصيات، سواء من المشرع الكويتي أو المشرع الإماراتي؛ وذلك لوضع تشريع متكامل في كل من البلدين موضوع الدراسة بهدف مكافحة جرائم تقنية المعلومات والحد منها، وذلك للمحافظة على حقوق الأشخاص والحكومات سواء على المستوى الدولي أو الداخلي، ولملاحقة التطور السريع لجرائم تقنية المعلومات.

ثانياً – أهمية الدراسة:

لهذه الدراسة أهمية متزايدة بسبب استغلال وسائل الاتصال الحديثة من جانب مرتكبي الجرائم، وذلك بهدف تسهيل ارتكابهم لهذه الجرائم، فموضوع الدراسة له أهميته النظرية والعملية حيث إنه يمس كثيراً من مصالح المجتمع الدولي أو الداخلي، كما تظهر أهميته في تحديد مصادر المخاطر التي تهدد النظام المعلوماتي وتحديد صور الاعتداء على المعلومات عبر شبكة الإنترنت، وكذلك الأنماط المختلفة للجرائم المستحدثة المرتبطة بتقنية المعلومات، ليس هذا فحسب، فالموضوع له أهميته من حيث التعرف على الاتجاهات التشريعية الدولية والإقليمية لحماية المعلومات ونظمها الإلكترونية، ومحاولة وضع الحلول للمشكلات التي تثيرها الجرائم المعلوماتية في التشريعين الكويتي والإماراتي، حيث إن كلاً من المشرع الكويتي والإماراتي قد يستفيدان من نتائج هذه الدراسة المتواضعة، وإظهار بعض المشكلات العملية والقانونية بشقيها الموضوعي والإجرائي التي تثيرها هذه الجرائم المتجددة، كما تظهر أهمية الدراسة بالنسبة لاستفادة الباحثين ورجال القضاء الجالس أو الواقف من نتائجها وتوصياتها والبناء عليها وتطويرها لإجراء دراسات متعمقة في مجال تقنية المعلومات.

ثالثاً – مشكلة الدراسة:

إن التطور التقني لأساليب ارتكاب الجرائم خاصة تلك التي ترتكب وتتم عبر شبكة الإنترنت والحاسب الآلي تتطلب من الجهات المختصة أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي، ومن ثم تكمن مشكلة الدراسة في كيفية تقديم دليل رقمي إلكتروني مقبول وذي حجية أمام القاضي الجزائي، كما أن هناك إشكالية أخرى تتعلق بمدى كفاية القواعد التقليدية في التشريع الجزائي سواء الكويتي أو الإماراتي لمواجهة المشكلات الناجمة عن الجرائم الإلكترونية في ظل القصور التشريعي في التشريع الجزائي لكلا البلدين، ليس هذا فحسب فهناك مشكلة تتعلق بطبيعة المشكلات الموضوعية والإجرائية التي يثيرها هذا النوع من الجرائم ومدى كفاية معالجة كل من المشرع الكويتي والإماراتي لها في ظل قوانين مكافحة جرائم تقنية المعلومات التي ما زال ينقصها الكثير من التعديل، والذي لم يسعفنا هذا البحث المتواضع لتناولها.

رابعاً – منهجية البحث:

إن هذه الدراسة تتبع المنهج التحليلي والوصفي المقارن من خلال إيراد النصوص ذات الصلة بموضوع الدراسة في كل من التشريع الكويتي والإماراتي وتحليلها ومقارنتها للوصول إلى نتائج وتوصيات تبين أوجه القصور في كل من

التشريع الكويتي والتشريع الإماراتي بخصوص مواجهة تحديات ومشكلات جرائم تقنية المعلومات.

خامساً – خطة البحث:

قسمنا هذه الدراسة إلى ثلاثة مباحث رئيسية يسبقهما مطلب تمهيدي: تناولنا في المطلب التمهيدي ظاهرة جرائم تقنية المعلومات على شبكة الإنترنت، والذي قسمناه إلى فرعين: الفرع الأول: مفهوم الإنترنت وتطوره. أما الفرع الثاني فشرحنا من خلاله تعريف الجريمة المعلوماتية وماهية المصلحة المحمية في الجرائم المستحدثة على شبكة الإنترنت.

وفي المبحث الأول تناولنا أهم الأحكام الموضوعية الخاصة بجرائم تقنية المعلومات. والذي قسمناه إلى مطلبين: المطلب الأول: تناولنا فيه ركني الجريمة المادي والمعنوي. أما المطلب الثاني: فقمنا بتخصيصه لمناقشة المساهمة الجنائية.

وفي المبحث الثاني: تناولنا أهم الأحكام الإجرائية لجرائم تقنية المعلومات عبر شبكة الإنترنت. وقد قسمناه إلى مطلبين: المطلب الأول: مرحلة ما قبل المحاكمة. والمطلب الثاني: مرحلة المحاكمة.

وفي المبحث الثالث: ناقشنا تطبيقاً لإحدى جرائم تقنية المعلومات والذي يتمثل في جريمة الدخول غير المشروع للنظام المعلوماتي كمثال على الجريمة المستحدثة.

المطلب التمهيدي
ظاهرة جرائم تقنية المعلومات على شبكة الإنترنت

تمهيد وتقسيم:

لما كان مجال الدراسة في التكنولوجيا المعلوماتية من ناحية حمايتها جنائياً ومواجهة ما تم إفرازه من ظواهر إجرامية يستلزم بطبيعة الحال استخدام بعض المصطلحات المستحدثة، فقد لزم الأمر أن نعرضها فنياً ومن ثم مناقشة كيفية تطورها حتى أصبحت ظاهرة إجرامية تشكل خطراً على المجتمع والدولة، فضلاً عن تعريف الجريمة المعلوماتية وماهية المصلحة محل الحماية في الجريمة المستحدثة تمهيداً لاستكمال البحث وذلك على النحو الآتي:

الفرع الأول: مفهوم الإنترنت وتطوره.

الفرع الثاني: تعريف الجريمة المعلوماتية وتحديد المصلحة المحمية في الجرائم المستحدثة على شبكة الإنترنت.

الفرع الأول
مفهوم الإنترنت وتطوره

الإنترنت عبارة عن شبكة تتضمن عدداً غير محدود من الحاسبات الآلية المرتبطة ببعضها، إما عن طريق خطوط[١] أو عن طريق الأقمار الصناعية، وتمتد عبر العالم بحيث تمكن المستخدم من الدخول إليها في كل وقت ومن أي مكان في العالم، ولكن يجب أن يكون الجهاز مزوداً بمودم يربطه بخط الهاتف لتلقي وإرسال البيانات عبر مزود الخدمة[٢]. ويمكن تمييز الشبكات لنظامين مختلفين وهما نظام الشبكات المحلية، ونظام الشبكات واسعة النطاق.

أما عن نشأة فكرة الإنترنت وتطورها، فقد نشأت فكرة الإنترنت في أواخر الخمسينيات من القرن الماضي، عندما طلبت وزارة الدفاع الأمريكية من خبراء

---

(١) أ. شمس الدين إبراهيم أحمد، وسائل مواجهة الاعتداءات على الحياة الخاصة في مجال تقنية المعلومات، دار النهضة العربية، ط١، ٢٠٠٥م، ص٨٥ وما بعدها.

(٢) د. محمود عبد العزيز أبا زيد، الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص١٢.

(٣) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط/ ٢٠٠٠م، ص٣.

الكمبيوتر، إيجاد أفضل طريقة للاتصال بين عدد غير محدود من أجهزة الكمبيوتر دون الاعتماد على جهاز واحد ينظم حركة السير(٣)، وذلك لظروف التأمين، ولهذا السبب أنشأ البنتاجون شبكة عرفت باسم أربانت عام ١٩٥٧، وتعد من أهم شبكات الكمبيوتر وكان استخدامها قاصراً على المهام العسكرية(٤)، واستمر هذا التطور إلى أن أنشأت جامعة ويسكونسن الأمريكية عام ١٩٨٣م نظاماً يسهل الدخول لبلوغ الخدمات المختلفة، ثم انتقلت أيضاً للتطبيقات التجارية(٥)، مما أدى كل ذلك إلى أن أصبح هناك الملايين من أجهزة الحاسب الآلي والآلاف من الشبكات، ومن خلال ترابط تلك الشبكات نشأت الإنترنت الحديثة(٦).

وقد عرف المشرع الكويتي في القانون ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات "الشبكة المعلوماتية بأنها ارتباط بين أكثر من منظومة اتصالات لتقنية المعلومات للحصول على المعلومات وتبادلها" (٧).

وهناك بعض المصطلحات التي سيتم استخدامها خلال البحث لما تشكله من أهمية خلال استخدام الشبكة، فمثلاً العنوان الإلكتروني وهو الذي يحدد هوية صاحبه على الشبكة المعلوماتية بحيث يتمكن أي مستخدم من الوصول إليه، والبريد الإلكتروني وهو خط مفتوح على كل أنحاء العالم يستطيع الفرد من خلاله إرسال واستقبال رسائله في أي مكان بالعالم وفي ثوان معدودة(٨)، والصحافة الإلكترونية وهي أبواب ثابتة مخصصة لوكالات الأنباء ومحطات الأخبار والصحافة بأنواعها(٩)، والتجارة الإلكترونية وهي مجموعة من المعاملات الرقمية المرتبطة بأنشطة تجارية

---

(٤) Sebine Marcellin - Taupenas, Internet et le droit international, lamy droit d'l'informatique, No. 74, Octobre 1995.

(٥) مارتن مور، المدخل إلى الإنترنت، ترجمة أ. عبد السلام رضوان، مجلة الثقافة العالمية، إصدار المجلس الوطني للثقافة والفنون والآداب، الكويت، العدد ٧٦ مايو ١٩٩٦م، ص٤٩ وما بعدها.

(٦) Janet Abbate, Inventing the Internet, Cambridge, Massachusetts: MIT Press, 1999, p.149-152.

(٧) انظر: نص المادة (١) من القانون ٦٣ لسنة ٢٠١٥ الكويتي في شأن مكافحة جرائم تقنية المعلومات الكويتي الصادر في ٧ يوليو ٢٠١٥، وهي المقابلة للمادة الأولى من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات والتي تنص على: "الشبكة المعلوماتية ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات".

(٨) د. محمود عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص١٣-١٤.

(٩) د. طارق سرور، جرائم النشر والإعلام، دار النهضة العربية، القاهرة، ط/٢٠٠٨م، ص٦٧ وما بعدها.

بين المشروعات بعضها بعضاً وبين المشروعات والإدارة[١٠]، حيث تعد شبكة الإنترنت سوقاً تجارياً مفتوحاً[١١]، وهناك عنوان بروتوكول الإنترنت وهو عنصر معرف لكل واجهة من أي جهاز يستخدم بروتوكول الإنترنت لإنجاز اتصالاته ووصوله بشبكة ما[١٢]. وقد نصت على عنوان بروتوكول الإنترنت، المادة الأولى من المرسوم بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الإماراتي، إلا أن هذا المصطلح لم يتعرض له قانون مكافحة تقنية المعلومات الكويتي، وهذا يعد قصوراً من المشرع الكويتي يتعين عليه تداركه وإضافته للمصطلحات الواردة بالقانون، حتى يتسنى للمهتمين بالإنترنت وشبكة المعلومات وجرائم المعلوماتية الوقوف على هذا المصطلح الذي يساعد في فهم كثير من وسائل تقنية المعلومات المشاركة في شبكة المعلومات، كما أنه يتم استخدامه لأغراض الاتصال.

هذا عن بعض المفاهيم المتعلقة بموضوع البحث حيث لا يسعفنا هذا البحث لدراسة كل المصطلحات المتعلقة بالقانون ٦٣ لسنة ٢٠١٥ الكويتي، والقانون رقم ٥ لسنة ٢٠١٢ الإماراتي.

الفرع الثاني
تعريف الجريمة المعلوماتية وتحديد المصلحة المحمية في الجرائم المستحدثة على شبكة الإنترنت

أولاً – تعريف الجريمة المعلوماتية:

تعريف الجريمة بصفة عامة يتأسس على بيان عناصرها التي يحددها القانون حيث إنه من دون النص على النموذج القانوني للجريمة لا يمكن المساءلة عنها وهو ما يستوجب التمييز بين مصطلحين وهما: الظاهرة الإجرامية والجريمة، فظاهرة الإجرام المعلوماتي هي الأفعال غير المشروعة المرتبطة بنظم الحاسبات، أما الجريمة المعلوماتية فقد اختلف الفقه الجنائي في تعريفها، فمنهم من عرفها على أساس السلوك الإجرامي بأنها سلوك غير مشروع معاقب عليه قانوناً، صادر عن إرادة

(١٠) د. عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ط/٢٠٠٢م، ص١٨، د. محمد سمير، الجرائم الاقتصادية في التشريعين المصري والإماراتي، دار النهضة العربية، القاهرة، ط/٢٠١٥م، ص١٢.

(١١) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، ط/٢٠٠٠م، ص٩.

(١٢) د. محمود عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص١٨.

إجرامية آثمة، محله معطيات الحاسب الآلي، فالسلوك يشمل الفعل والامتناع عن الفعل، وهذا السلوك غير المشروع معاقب عليه قانوناً، لأن إسباغ الصفة الإجرامية لا يتحقق في مجال القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفاً للأخلاق، ومحل الجريمة المعلوماتية هو دائماً معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة، معلومات معالجة ومخزنة، البرامج، المعلومات المستخرجة والمتبادلة بين النظم)(١٣).

ومنهم من عرفها على أساس وسيلة ارتكاب الجريمة حيث عرفها الفقيه "توم فورستر"(١٤) بأنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية، كما عرفها الفقيه "تيدمان" بأنها كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب(١٥)، ليس هذا فحسب بل هناك من عرف الجريمة المعلوماتية على أساس سمات شخصية الجاني كتعريف الفقيه الأمريكي دون باركر الذي عرفها على أنها "الجرائم التي يستخدم فيها الجاني معرفته الخاصة بتكنولوجيا الكمبيوتر والفضاء الإلكتروني"(١٦).

وإذا كانت تعريفات الجريمة عموماً تقوم على أساسين هما عناصر الجريمة (السلوك، ووصفه) والنص القانوني على تجريم هذا السلوك وإيقاع العقوبة، فإن الجديد في مجال الجرائم المعلوماتية هو إضافة عنصر ثالث يبرز محل الاعتداء في هذه الظاهرة المستحدثة متمثلاً في معطيات الحاسب الآلي(١٧).

وقد عرفها المشرع الكويتي في القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات بأنها: "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا

---

(١٣) د. يونس خالد عرب مصطفى، صور الجرائم الإلكترونية واتجاهات تبويبها، ورقة عمل (٣) مقدمة لورشة عمل عن تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، سلطنة عمان، المدة من ٢-٤/٤/٢٠٠٦م، ص٧.

(١٤) Tom Forester and Perry Morrison, Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, 2nd ed., Cambridge, Massachusetts: MIT Press, 1994, p.29.

(١٥) Klaus Tiedeman, Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, Rev. D.P.C. 1984, p.612.

(١٦) Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, 1998 Wiley computer Publishing, United States of America, p.72.

(١٧) د. يونس خالد عرب مصطفى، المرجع السابق، ص٦-٧.

القانون"[١٨]. وهذا التعريف الذي نص عليه المشرع الكويتي في المادة الأولى من القانون سالف الذكر قد تناوله المشرع على أساس وسيلة ارتكاب الجريمة.

ومن جانبنا نناشد المشرع الإماراتي بالنص على تعريف الجريمة المعلوماتية في قانون مكافحة جرائم تقنية المعلومات عند أقرب تعديل تشريعي؛ وذلك لمساعدة الباحثين في فهم ماهية الجريمة المعلوماتية، وذلك لاختلاف الفقهاء في تعريفهم ماهية الجريمة المعلوماتية. فمن وجهة نظرنا يمكننا تعريف الجريمة المعلوماتية بأنها "كل سلوك غير مشروع محله المعلومات المعالجة آلياً أو نظم ووسائل تقنية المعلومات بطريقة مباشرة أو غير مباشرة، مما ينتج عنه إلحاق ضرر بالضحية أو حصول الجاني على مكاسب لا يستحقها".

وقد اعتمدنا في هذا التعريف على عناصر الركن المادي للجريمة وهي، السلوك غير المشروع، ويشمل كافة صور السلوك الإجرامي المستحدثة في جرائم الاعتداء على المعلومات المعالجة آلياً سواء بطريقة مباشرة أو غير مباشرة (الفعل، الامتناع)، ومحل الجريمة، وهي كيانات معنوية متمثلة في المعلومات المعالجة آلياً أو نظم ووسائل تقنية المعلومات، وأخيراً اعتمدنا في التعريف على النتيجة الإجرامية وهي إما إلحاق ضرر بالضحية أياً كانت الضحية وأياً كان نوع هذا الضرر مادياً كان أو أدبياً، أو حصول الجاني على فوائد أو مكاسب لا يستحقها أياً كانت هذه المكاسب، وذلك بالإضافة إلى قيام علاقة السببية بين السلوك والنتيجة، مع توافر الركن المعنوي للقائم بارتكاب الجريمة.

ثانياً – تحديد المصلحة المحمية في الجرائم المستحدثة على شبكة الإنترنت:

لقد اهتم معظم فقهاء القانون بوضع تعريف للمعلومات حيث اعتبرها البعض مالاً، وهي المعلومات ذات القيمة الاقتصادية، وتعد المعلومات لدى فقهاء القانون حقيقة مجردة، فهي تدخل في فئة الأشياء، حيث إن الأشياء ليست كلها أموالاً، فالشيء كل ما يحوزه الشخص أو يملكه، إلا أن هناك كماً من الأشياء، كما هو الحال بالنسبة للمعلومات غير قابل للتملك بسبب طبيعتها كالأشياء المشتركة العامة[١٩]، وينظم القانون استعمالها، وحيث لا تكون المعلومة محمية بالنظام القانوني كحق خاص أو عن طريق السر أو التقنيات فإنه يتم تداولها بحرية وفق ما يبديه المجتمع

(١٨) وهو ما لم يتعرض له المشرع الإماراتي في قانونه رقم ٥ لسنة ٢٠١٢ وتعديلاته.

(١٩) د. عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، ط/١٩٨٦م، ص٤٣٤.

من حاجة لتنظيم تملكها المؤقت عن طريق شكل من أشكال حق الملكية الفكرية(٢٠)، وقيمة وفائدة المعلومة يبرران اعتبارها موضوعاً للملكية، فهي سلعة تباع وتشترى(٢١).

والتعريف القانوني للمعلومة نظراً لأهميتها القانونية فهي القاسم المشترك لكل الحقوق المستحدثة، وكذلك القاسم المشترك لكل المحاولات المختلفة لهذا المنتج الجديد من منتجات الصناعة الإنسانية(٢٢). وقد عرفها المشرع الإماراتي في المرسوم بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة تقنية المعلومات الإماراتي بأنها: "أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها" (٢٣).

وهناك اختلاف بين مصطلح "المعلومة" ومصطلح "المعلوماتية"، فالمعلومة كما سبق هي ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات، ولكن بعد أن يتم ذلك تصبح ما يسمى بمصطلح المعلوماتية، أما قبل ذلك فهي مجرد معلومة أو بيان، وفي ضوء التداخل بين المصطلحين والترابط الجريء بينهما حيث يستخدمان عادة بالتبادل، فالبيانات حقائق ونصوص ورسومات وصوت وقطاعات عروض مرئية متحركة لها معنى في بيئة المستخدمين، والمعلومات أو المعلوماتية هي الصورة المحولة للبيانات أو للمعلومة بكل معالجتها وهي محل الحماية القانونية في صدد مكافحة جرائم تقنية المعلومات(٢٤).

(٢٠) د. محمود كبيش، دروس في الجرائم المضرة بالمصلحة العامة، دار النهضة العربية، القاهرة، ط/٢٠٠٥م، ص١١٦.

(٢١) د. محمود عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص٢٧.

(٢٢) د. حسام الدين الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي، ط/١٩٩٤م، ص١٠٠ وما بعدها.

(٢٣) وهذا المصطلح يعد من أهم المصطلحات القانونية التي يجب أن يتعرض لها المشرع عند سنه لقوانين مكافحة جرائم تقنية المعلومات وهو ما لم يقم به المشرع الكويتي، لذا نناشده بأن يشير إليه في أول تعديل تشريعي للقانون ليساير في ذلك المشرع الإماراتي.

(٢٤) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م، ص٢٣.

المبحث الأول
أهم الأحكام الموضوعية لجرائم تقنية المعلومات عبر شبكة الإنترنت

تمهيد وتقسيم:

سنتناول في هذا المبحث أهم الأحكام الموضوعية الخاصة بجرائم تقنية المعلومات وذلك من خلال بيان أركان الجريمة (الركن المادي والركن المعنوي) في مطلب أول، ثم ننتقل بعد ذلك لمناقشة المساهمة الجنائية في مطلب ثانٍ، وذلك على التفصيل الآتي:

المطلب الأول
أركان الجريمة المعلوماتية

أولاً – الركن المادي:

يتمثل الركن المادي بأنه مجموعة العناصر المادية التي ينتج عنها الخطر أو تلحق الضرر بمصلحة يحميها القانون جنائياً، فلا يعرف القانون جريمة من دون ركن مادي حتى يكون إقامة الدليل عليها ميسوراً[٢٥]. ويقصد بالركن المادي للجريمة السلوك الإنساني الذي تترتب عليه نتيجة يعاقب عليها القانون الجنائي[٢٦]، ومن ثم فإن عناصر الركن المادي هي السلوك الإنساني والنتيجة وعلاقة السببية بينهما.

فالجريمة المعلوماتية تحتاج لارتكابها بالضرورة إلى منطق تقني، فمن دونه لا يمكن للشخص حتى الاتصال بالإنترنت سواء بقصد ارتكاب جريمة أو مجرد الدخول في الاتصال المباشر كالمحادثة وغيرها، وهذا السلوك الإيجابي الممثل في المنطق التقني، يجعل الجريمة المعلوماتية ذات طابع موحد بالضرورة، ومثل هذا الأمر قد فطن له كل من المشرع الكويتي والإماراتي عندما نصا على الجرائم التي يمكن أن ترتكب عبر الحاسب، ففي مثل هذه النصوص قد قرر المشرع صراحة أن كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية، ففي مثل هذه الحالات

---

(٢٥) د. يسر أنور علي، شرح قانون العقوبات، النظريات العامة، ١٩٩٨م، ص٢٧٦.

(٢٦) د. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، ط/ جامعة القاهرة، ١٩٧٨م، ص٢٧٩.

يكون المشرع مدركاً للقيمة الموحدة للشروع في ارتكاب الجريمة المعلوماتية أو ارتكاب الجرائم باستخدام الحاسب الآلي المرتبط بالإنترنت(٢٧).

حيث تنص المادة (٢) من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي على أنه: "يعاقب بالحبس... كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية"(٢٨). أما المشرع في التشريعات المقارنة فاستخدم عبارة "باستخدام الحاسب الآلي، أو عبارة باستخدام المعالجة الآلية للبيانات أو الدخول إلى موقع إلكتروني أو نظام معلومات أو وسيلة تقنية معلومات أو شبكة معلومات"، فكل هذه النماذج تعد نشاطاً تقنياً، ومن ثم يمكن القول حينئذ بوجود نشاط تقني ليمكن الوصول إلى الإنترنت ومن ثم ارتكاب جريمة معلوماتية حال الدخول غير المشروع وإلا فقدت الجريمة مقوماتها. ومن ثم يعد الدفع بعدم وجود نشاط تقني، حال الاتهام بارتكاب جريمة معلوماتية من الدفوع الموضوعية الجوهرية التي تلتزم محكمة الموضوع بالرد عليه تفصيلاً، وإلا عاب حكمها عيب في التسبيب مما يستوجب نقضه (تمييزه)(٢٩).

ومن الضروري لارتكاب جرائم المعلوماتية، أن تتم مباشرة النشاط التقني، فالجريمة في هذا النوع تعد من الجرائم التي يجب أن تتم بمعرفة شخص يتمتع بالتقنية الكافية في هذا الصدد لارتكاب الجريمة المعلوماتية وليس ارتباطها فقط باستخدام الحاسب الآلي أو الإنترنت(٣٠). والفعل الذي يقوم به مرتكب الجريمة المعلوماتية لابد أن يكون هو السبب الذي أدى إلى النتيجة التي توصل إليها بفعله

(٢٧) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، دار الجامعة الجديدة للنشر، ١٩٩٧م، ص٢٥-٢٦.

(٢٨) وهي المقابلة للمادة (٢) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الإماراتي والتي تنص على أنه: "يعاقب بالحبس... كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات من دون تصريح أو بتجاوز حدود التصريح أو بالبقاء فيه بصورة غير مشروعة".

(٢٩) د. علاء محمود يسن حراز، الحماية الجنائية للمعلومات المعالجة آلياً، دراسة مقارنة في القانون الوضعي والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص٢٠٢-٢٠٣.

(٣٠) د. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، ٢٠٠٣م، ص١٨٢.

بمعنى أن هناك علاقة سببية بين الفعل والنتيجة، ومن ثم توافر شرط أساسي لمسؤولية مرتكب الفعل عن النتيجة وهو علاقة السببية بينهما(٣١).

وكي يتم ثبوت الركن المادي في الجرائم المادية يلزم أن يثبت بالضرورة قيام علاقة السببية بين النشاط المادي وبين النتيجة الإجرامية، فمثلاً لقيام جريمة انتهاك الحق في الخصوصية عبر الإنترنت يجب أن يكون هناك دخول على الإنترنت باستخدام حاسب آلي عامل واختراق الخوادم المختلفة في مسارها، ثم بعد ذلك التعدي على خصوصية موقع ما أو إعداد موقع ما، ثم بعد ذلك يبث عليه صوراً ذات خصوصية لأشخاص مشهورين... إلخ(٣٢).

والعنصر الثاني من عناصر الركن المادي، هو النتيجة الإجرامية، وهي كل أثر للسلوك الإنساني يسفر عن تغيير في المحيط الخارجي(٣٣) وفي إطار بحث النتيجة في الجريمة المعلوماتية ينبغي التعرض لفكرة جرائم الضرر وجرائم الخطر والنتيجة المحتملة، فجرائم الضرر المعلوماتية هي التي يتحقق فيها هلاك المال القانوني أو الإنقاص منه أو التضحية بمصلحة إنسانية يحميها القانون، أما جرائم الخطر المعلوماتية فهي تلك الجرائم التي يكون الهدف فيها حماية المال القانوني من احتمال التعرض للخطر فهي جرائم وقائية(٣٤)، ومن المشاكل التي تواجه تحديد الضرر أو الخطر كنتيجة إجرامية عبر الإنترنت، تلك المتعلقة بجرائم العدوان الفيروسي، وفي هذا النوع من الجرائم يصعب تحديد المجني عليه(٣٥).

ومن حيث النتيجة المحتملة وهي حالة إذا ما ترتب على النشاط الإجرامي أكثر من نتيجة لا يسعى الجاني إلا إلى صورة واحدة منها وهي التي يتوقعها ويريدها(٣٦)، وتنتشر فكرة النتيجة المحتملة في جرائم المعلوماتية، ذلك أن النشاط التقني له منطق تفكيري واسع المجال يمكن أن يترتب عليه نتائج متعددة وليس مجرد

---

(٣١) د. محمود نجيب حسني، المرجع السابق، ص٢٩٣.

(٣٢) د. علاء محمود يسن حراز، رسالة دكتوراه، المرجع السابق، ص٢١٠.

(٣٣) د. محمد عمر مصطفى، النتيجة وعناصر الجريمة، مجلة العلوم القانونية والاقتصادية، ع٢، س٧، يوليو ١٩٦٥، كلية الحقوق، جامعة عين شمس، ص٣٢٤.

(٣٤) د. علي أحمد راشد، القانون الجنائي، المدخل والنظرية العامة، ١٩٨٤م، ص٢٥٩.

(٣٥) د. يونس خالد عرب مصطفى، تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، ورقة عمل مقدمة لورشة عمل عن تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، عمان، ٢-٤/٤/٢٠٠٦، ص٥.

(٣٦) د. عبد الأحد جمال الدين، د. جميل الصغير، المبادئ الرئيسية في القانون الجنائي.

النتيجة المقصودة من الجريمة، وهذا الأمر متوافق بالضرورة مع الطبيعة التي عليها تقنية المعلومات، فمن يقصد القرصنة ويتحقق معها انتشار فيروسات من أي نوع نتيجة لوجود دفاع فيروسي في البرمجة أو الموقع، فمثل هذه النتائج تتحقق مع النتيجة الأصلية وهي الشروع في القرصنة إلى جواز نتائج أخرى يبدو الاحتمال واضحاً في حدوثها كنتائج لكنها ليست النتائج المقصودة من النشاط الإجرامي(٣٧).

ثانياً – الركن المعنوي:

هو المسلك الذهني أو النفسي للجاني، وفي إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية(٣٨). والركن المعنوي في جرائم الاعتداء على المعلومات عبر الإنترنت له صور عديدة منها القصد الجنائي وهو علم الجاني واتجاه إرادته إلى مخالفة القانون الجنائي، ويكون ذلك في الجريمة العمدية، ولذا يجب على الجاني أن يكون عالماً بحقيقة ما يرتكبه، مدركاً أن عمله هذا يجرمه القانون ويعاقب عليه(٣٩).

وإذا كان ذلك هو المفهوم القانوني للقصد الجنائي، فهذا لا يعني أنه يمكن تطبيقه في إطار الجرائم المعلوماتية بسهولة كما هو الحال في الجرائم التقليدية عادة، حيث إنه في إطار الجرائم المستحدثة، هناك مشاكل تتعلق بمدى تطلب القصد الجنائي فيها وبشكل يمكن أن يحقق غرض المشرع في هيكلة الإدانة، وقد برز هذا الأمر عند طرح موضوع مدى إمكانية امتداد البحث في الركن المعنوي للجرائم الأخرى ذات الصلة بالجريمة الأولى في الجرائم المعلوماتية، ونعني بها جريمة الاختراق، أما ما عدا ذلك من جرائم تتعلق ببناء الركن المعنوي فيها فإن المشرع يتطلب العمد أو لا يتطلبه حسب الأحوال(٤٠).

وتتحقق جريمة الاختراق للنظام المعلوماتي في صورتها البسيطة بمجرد فعل الدخول غير المشروع(٤١)، وهذه الجريمة قد نص عليها المشرع الكويتي في المادة الثانية فقرة أولى، حيث نص على أنه: "يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين،

---

(٣٧) د. عمر يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، ٢٠٠٤م، ص٢٧٥.

(٣٨) د. محمود نجيب حسني، المرجع السابق، ص٩.

(٣٩) د. أحمد المجذوب، مشكلة تقنين القصد الجنائي، المجلة الجنائية القومية، العدد الأول، المجلد ١٣، ١٩٧٠م، ص٤١٠.

(٤٠) د. عمر يونس، المرجع السابق، ص٢٨٩-٢٩١.

(٤١) د. علي القهوجي، المرجع السابق، ص٥٤.

كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية"[٤٢].

وتتحقق هذه الجريمة في صورتها المشددة متى ترتب على الدخول غير المشروع محو أو تعديل البيانات التي يحتويها النظام، أو عدم قدرة النظام ذاته على تأدية وظيفته، وقد شدد كل من المشرع الكويتي والإماراتي العقاب في تلك الحالة نظراً لخطورة الأضرار الجسيمة المترتبة على تلك الأفعال[٤٣].

والصورة الثانية من صور الركن المعنوي، الخطأ غير العمدي في الجرائم المعلوماتية، ويتكون الركن المعنوي في هذه الجرائم من الخطأ بسبب الإهمال وعدم الاحتياط والرعونة، وهو المسلك الذهني للجاني الذي يؤدي لنتائج إجرامية لم يردها الجاني وكان بإمكانه أن يتوقاها، وكان يتوقع النتيجة الإجرامية ولكنه لم يبذل العناية الواجبة عليه لتلافيها[٤٤].

المطلب الثاني
المساهمة الجنائية في الجريمة المعلوماتية (تعدد الجناة)

قد يرتكب الفعل المعلوماتي المجرَّم شخص واحد، وقد يتعاون على ارتكابه جماعة يتفقون على الجريمة المعلوماتية فينفذها أحدهم أو بعضهم، أو يحرض بعضهم بعضاً عليها، أو يساعد بعضهم البعض الآخر ويعينه حال ارتكابها، وهذا ما يسمى بالاشتراك في الجريمة، أو المساهمة في الجريمة، والمساهمة الجنائية هي حالة تعدد الجناة الذين ارتكبوا الجريمة نفسها، ويتضح بذلك أن الجريمة لم تكن ثمرة لنشاط شخص واحد ولم تكن وليدة إرادته وحده، وإنما كانت نتاج تعاون بين أشخاص عديدين لكل منهم دوره المادي وإرادته الإجرامية[٤٥].

والمساهمة الجنائية في الإجرام المعلوماتي تتخذ في الواقع اتحاد مجموعة حواسب لها طابع المشاركة فيما بينها، ومن ثم يتحدد مظهر المساهمة الجنائية بالمعنى الواسع لها – أي اشتمالها على المساهمة والاشتراك الضروري والتوافق – وذلك في

(٤٢) وهي المقابلة لنص المادة الثانية فقرة (١) من القانون الإماراتي رقم ٥ لسنة ٢٠١٢.
(٤٣) انظر: نص م(٢) فقرة ثانية من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي، والمادة (٢/٢) من مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ الإماراتي.
(٤٤) د. محمود نجيب حسني، المرجع السابق، ص٦٦٤.
(٤٥) د. محمود نجيب حسني، المرجع السابق، ص٣٩٧.

ضوء قيام مجموعة حواسيب بالعمل الإجرامي، يقود كل حاسب فيها شخص بذاته، على أن يكون كل حاسب متصلاً بالضرورة بالإنترنت، ومع ذلك يظل الاختلاف فيما بين المظاهر الجماعية الثلاثة متعلقاً ببحث وحدة الركن المعنوي فيما بين مستخدمي هذه الجوانب المشار إليها(٤٦).

فقد تقوم المساهمة الجنائية في الجرائم المعلوماتية عبر اتفاق مجموعة أفراد على ارتكاب جريمة من جرائم تكنولوجيا المعلومات، كما لو قام شخصان فأكثر باختراق نظام أمني أو نظام اتصالات أو القرصنة، ففي مثل هذه الحالة يتشكل التعدد الشخصي والرابطة المعنوية الجماعية في ارتكاب الجريمة، ويشترط هنا أن يكون كل منهم قد قام بمحاولات تساعد الفاعلين الآخرين معه في القيام بالمشروع الإجرامي، فيقوم أحدهم مثلاً بعملية انتهاك الخادم المضيف، وإعلام الغير من المجموعة بذلك وبطريقة الانتهاك، ومنحهم برمجة محددة يتم بها الانتهاك، ويقوم الآخر – أو أكثر من ضمن هذه المجموعة – بالقيام بمسح رقمي لكيفية اختراق الحاسب الآلي، ويكون دور المساهم الثالث القيام بتحصين هوية كل مساهم في الجريمة حتى لا يتم كشفها، ففي هذه الحالات تقوم المساهمة الجنائية فيما بين مجموعة الأفراد المشاركين في مشروع إجرامي واحد، وبينهم رابطة معنوية جماعية مضمونها ارتكاب جريمة محددة، فكل منهم فاعل مع غيره في هذه الجريمة أو شريك في ارتكابها بحسب الأحوال(٤٧).

ويلزم لوصف كل من هؤلاء بوصف الفاعل أو الفاعل مع غيره، أن يضع كل منهم يده رقمياً على المحل الرقمي (المحل المادي) للجريمة، ففي جريمة الاختراق وهي الدخول غير المشروع، يلزم أن يقوم كل منهم بالاختراق فعلاً إلى الخادم أو الموقع المراد اختراقه، وفي جريمة العدوان على الحق في الخصوصية فإنه يلزم قيام كل من الفاعلين في المشروع الإجرامي – لكي يمكن وصفهم جميعاً بصفة الفاعلين الأصليين – بالمساهمة في انتهاك الخصوصية والاطلاع على محتويات الخصوصية هذه(٤٨).

وفيما يتعلق بالتمييز بين الفاعل والشريك، فالقانون يحدد صوراً ثلاث للاشتراك هي الاتفاق والمساعدة والتحريض، وهذه الصور الثلاث يمكن أن يكون لها وجود في

(٤٦) د. علاء محمود يسن حراز، رسالة دكتوراه، المرجع السابق، ص٢٨١.
(٤٧) د. علاء محمود يسن حراز، رسالة دكتوراه، المرجع السابق، ص٢٨٢.
(٤٨) د. عمر يونس، المرجع السابق، ص٢٨٤.
انظر: نص المادة ٢ من القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات الكويتي، وكذا المادة ٢ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ الإماراتي.

المشروع الإجرامي، بشرط وحدة الجريمة ووجود رابطة معنوية، إلا أن الشريك لا يضع يده على المحل الرقمي (المحل المادي) للجريمة، في الوقت الذي ينتهك المحل أو الموضوع القانوني للجريمة(٤٩)، كما لو كان أحد أفراد المجموعة الإجرامية له دور استطلاعي رقابي أثناء عملية المسح بحيث يحدد الأبواب التي يمكن الدخول عبرها، ويقوم بإعلام الآخرين بالأبواب المفتوحة المشار إليها، إلا أنه لا يقوم بالدخول معهم إلى الحاسب الآلي المقصود بالانتهاك أو الاختراق (الدخول غير المشروع) ففي هذه الحالة يصنف بكونه شريكاً بالمساعدة، كما يعد شريكاً من يقوم بتحريض غيره(٥٠) على الدخول بعد أن يكشف الأبواب المفتوحة بشرط أن يكون هناك مظهر لمشروع إجرامي جماعي سابق مع عناصر بشرية محددة، وتبرز هذه الصورة في مرحلة قيام أحد عناصر المجموعة الإجرامية بالعدول الاختياري عن ارتكاب الجريمة، فيقوم أحدهم أو بعضهم من ذات المجموعة بتحريضه على القيام بالدخول غير المشروع حال كونهم قد كشفوا الأبواب المفتوحة، فيدخل هو ولا يدخلون هم إلى الخادم أو الحاسب الآلي المراد اختراقه.

وتظهر صورة الاتفاق كمظهر من مظاهر الاشتراك القانونية عند قيام أحدهم مثلاً بالاتفاق على أن يكون دوره في جريمة دعارة أطفال إلكترونية، بإعداد صفحة الدعارة وإعداد الصور رقمياً والقيام بتحميل هذه الصور على موقع عبر الإنترنت دون أن يكون له علاقة بحركة هذا الموقع من حيث استقبال الاتصال وتوزيع الطلبات، كما تبرز صورة الاتفاق هنا في قيام أحدهم بتحميل ما يطلب منه تحميله من معلومات ومراسلات، حول كيفية التعامل بالمواد المخدرة وكيفية تعاطيها وزراعتها وتحديد الجرعات ونوعية المخدر، فهنا يظل الشخص شريكاً، إلا أنه إذا تحول إلى الرد على المطالبات من الغير واستقبال الرسائل والاستفسارات وطلب جرعات وتحديد نوعيتها والاتصال بالمصارف والبنوك لمعرفة المدفوعات من حركة التداول وتحديد المشتري فكل ذلك يجعله فاعلاً في الجريمة(٥١).

ومن المتصور عند تمييز الشريك أن يكون الشخص ذا اتصال بالعالم المادي،

(٤٩) د. فوزية عبد الستار، المساهمة الأصلية في الجريمة، من دون ناشر، ١٩٦٧م، ص٣٦ وما بعدها.

(٥٠) د. عبد الفتاح الصيفي، الاشتراك بالتحريض وموضعه من النظرية العامة للمساهمة الجنائية، ١٩٨٥م، ص٢٩.

(٥١) د. محمود نجيب حسني، المرجع السابق، ص٤٥٢.

فمن يقوم بالاتفاق مع امرأة بقصد إعداد فيلم تصويري سينمائي لها بقصد تحميله على الإنترنت، فإنه يكون شريكاً بالاتفاق، في حين تعد المرأة المذكورة فاعلاً أصلياً لكونها هي التي تم بث صور متحركة خلاعية لها، شريطة أن تكون المرأة المذكورة هي التي تتولى أو تشرف على الصفحة أو الموقع، من حيث استقبال وإرسال طلبات الدعارة المختلفة، أما إذا كان الشخص هو من يقوم بذلك دون إشراف من المرأة المذكورة، بل يخضع تحريك الموقع أو الصفحة لتقديره هو، فإنه يعد فاعلاً وليس شريكاً حيث يتحول الاتفاق بين الرجل وبين المرأة المذكورة إلى اتفاق جنائي بالمعنى الواسع (فاعل) وليس المعنى الضيق (شريك بالاتفاق). وفي فرضية قيام أحد الفاعلين في هذه الجريمة بارتكاب جريمة عرضية أثناء تنفيذه لدوره في المشروع الإجرامي الجماعي، كما لو قام أحد القراصنة أثناء تنفيذ هذه المجموعة لمشروع إجرامي، بأن يملأ خادم مضيف برسائل تافهة، فإن مثل هذه الجريمة العرضية تنسب إلى فاعلها ولا يعد الفاعلون الآخرون في المشروع فاعلين أو شركاء في ارتكابها(٥٢)، هذا ما لم تكن الجريمة العرضية التي وقعت بالفعل نتيجة محتملة لحظة تنفيذ الجريمة الأصلية التي أريد ارتكابها أصلاً، فهنا يسأل الفاعلون جميعاً عن الجريمة التي وقعت ولو كانت غير الجريمة التي قصدوا المساهمة فيها.

(٥٢) د. عمر يونس، المرجع السابق، ص٢٨٥-٢٨٦.

المبحث الثاني
أهم الأحكام الإجرائية لجرائم تقنية المعلومات عبر شبكة الإنترنت

تمهيد وتقسيم:

نظراً للطبيعة الخاصة والمستجدة لجرائم تقنية المعلومات عبر شبكة الإنترنت وما فرضته ثورة تكنولوجيا المعلومات من تحديات كبيرة، أدت لازدياد مخاطر الجرائم التقليدية فضلاً عن الجرائم المستحدثة التي برزت وتطورت بتطور تكنولوجيا تقنية المعلومات، مما أوجب على الجهات المعنية والمختصة اكتشاف تلك الجرائم، وعلى جهات التحقيق مواكبة ذلك التطور الإجرامي إذ إن جرائم تقنية المعلومات تتميز بخصوصية سواء في كيفية ومكان ارتكابها، فضلاً عن طبيعة الجاني، وهو ما يلقي بظلاله على الأحكام الإجرائية الحاكمة للضبط والتحقيق؛ لذا سنقوم بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: مرحلة ما قبل المحاكمة

المطلب الثاني: مرحلة المحاكمة

المطلب الأول
مرحلة ما قبل المحاكمة

تمهيد وتقسيم:

يتضمن هذا المطلب الإجراءات الجنائية في مراحلها الأولى وصولاً لمدى ملاءمتها، وجرائم تقنية المعلومات عبر شبكة الإنترنت في مراحلها الأولى، وذلك خلال مرحلة جمع الاستدلالات ومرحلة التحقيق بشأن هذه الجرائم.

أولاً – مرحلة جمع الاستدلالات بشأن جرائم تقنية المعلومات عبر شبكة الإنترنت:

تعد مرحلة جمع الاستدلالات من المراحل الهامة في مجال الدعوى الجنائية، فهي أولى مراحل المواجهة الجنائية للجريمة واكتشافها، بل ومحاولة منع وقوعها أو الانتقال للحيلولة دون ضياع الأدلة(٥٣).

(٥٣) د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ج١، ط/١٩٩٣م، ص٢٦٧.

حيث تنص المادة (١٥) من القانون رقم ٦٣ لسنة ٢٠١٥ على أنه: "للموظفين الذين يصدر بتحديدهم قرار من الوزير المختص، ضبط الجرائم التي تقع بالمخالفة لأحكام هذا القانون وتحرير المخالفات عنها وإحالتها إلى النيابة العامة، وعلى جميع الجهات ذات الصلة تقديم التسهيلات اللازمة لهؤلاء الموظفين"، فقد منح المشرع الكويتي للموظفين الذين يصدر بتحديدهم قرار بذلك من وزير العدل – الوزير المختص سابقاً[٥٤] – (قرار بمنحهم صفة الضبط القضائي)، أي مأموري الضبط القضائي، ومن ثم يكون لهم جمع الأدلة والمعلومات عن الجرائم التي ترتكب بصدد القانون رقم ٦٣ لسنة ٢٠١٥، وذلك في مرحلة جمع الاستدلالات وهي مرحلة سابقة على مرحلة التحقيق التي تختص بها النيابة العامة؛ وذلك لتيسير عمل النيابة العامة، لأن أعضاء النيابة العامة ليس بمقدورهم القيام بمهمة جمع الاستدلالات نظراً لما يقع عليهم من أعباء جسام بخصوص إجراءات التحقيق وهي من أخص خصوصيات النيابة العامة[٥٥].

وتعد عملية الضبط القضائي هي بداية جمع الاستدلالات، وقد اتفق الفقه على أن أعمال الضبط القضائي لا تقع تحت حصر[٥٦]، وقد أوردها المشرع بشكل فضفاض كقيام رجال الضبط القضائي بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق وكذلك قبول الشكاوى التي ترد إليهم تمهيداً لإرسالها فوراً للنيابة العامة.

وتفعيلاً للقانون رقم ٦٣ لسنة ٢٠١٥ فقد تم إنشاء إدارة تسمى إدارة مكافحة الجرائم الإلكترونية – التابعة للإدارة العامة للمباحث الجنائية – في وزارة الداخلية، حيث تقوم بإصدار نشرات توعية للجمهور المستخدمين للإنترنت لتعريفهم بما يدور

(٥٤) بعد قرار مجلس الوزراء رقم ٥٥١ لسنة ٢٠١٧ بتحديد الوزير المختص بتطبيق القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، أصبح الآن الوزير المختص بتطبيق القانون وإصدار القرارات اللازمة لتنفيذ أحكامه هو نائب رئيس مجلس الوزراء ووزير الداخلية.

(٥٥) انظر في ذلك: نص المادة ٤٩ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الإماراتي، وهي المقابلة للمادة ١٥ من القانون ٦٣ لسنة ٢٠١٥ الكويتي والتي تنص على: "يكون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل صفة مأموري الضبط القضائي في إثبات الأفعال التي تتم بالمخالفة لأحكام هذا المرسوم بقانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكنهم من القيام بعملهم.

(٥٦) د. عبد المهيمن بكر سالم، الإجراءات الجنائية، ج١، ط/١٩٩٧م، ص٣٧.

في هذا العالم الافتراضي من سلبيات وإيجابيات حتى يأخذ الفرد حذره عند استعماله لشبكة الإنترنت، هذا من جانب، ومن جانب آخر فإن هذه الإدارة تقوم بتلقي الشكاوى من المواطنين للتحري عنها وعرضها على النيابة العامة، وهذا يعد تطوراً كبيراً بالنسبة لهذه الأنواع من الجرائم المستحدثة والتي تتطور يوماً بعد يوم، ومن ثم يجب تطور هذه الإدارة بالسرعة ذاتها وبالتقنية نفسها التي تحدث في ارتكاب هذه الجرائم(٥٧).

ويجب أن يكون مأمور الضبط القضائي متخصصاً في جرائم تقنية المعلومات عبر شبكة الإنترنت، وأن يكون مدركاً لكيفية التعامل الصحيح مع تلك الجرائم المستحدثة بما ينطوي على لزوم وتوقيت تدخله، وكيفية ذلك سواء لمنع الجريمة أو ضبطها ومرتكبها، مع القدرة على جمع الأدلة والتحفظ عليها، وبما يتوافق مع القواعد الإجرائية الحاكمة لذلك الأمر، ودون تجاوز لها، ومن ثم مشروعية الضبط على وجه العموم، وحيث إن الحياة الافتراضية عبر الشبكة المعلوماتية، إنما تتجاوز عنصري الزمان والمكان، وهو ما نتج عنه أن ارتكاب الجريمة والكشف عن مرتكبها وضبطه والأدلة الجنائية قبله، يجب أن يتم بطريقة تواكب ذات سمات مجال ارتكاب الجريمة، ولما كانت الطرق التقليدية في منح الإذن القضائي تتعارض وطبيعتها، ومن ثم فالأمر هنا يتطلب تدخلاً تشريعياً بشأن الحصول على الإذن القضائي لهذه الجرائم المستحدثة(٥٨).

وحيث إن الانتقال المكاني عبر شبكة الإنترنت، إنما هو انتقال رقمي وليس مادياً، فلا يوجد هناك ما يمنع من السماح لرجل الضبط القضائي بالتنقل عبر العالم الافتراضي للتعاون مع جهات الضبط الدولية، فالأمر مختلف عن العالم المادي، وهذا يجب تقريره بنص تشريعي صريح، ومن ثم فالمسألة الإجرائية تتطلب تدخلاً تشريعياً

(٥٧) ويمكن لضحايا الجرائم الإلكترونية في دولة الإمارات العربية المتحدة الإبلاغ لدى أقرب مركز شرطة عن الجرائم الإلكترونية، بالإضافة إلى بعض المواقع المحددة على شبكة الإنترنت.
ونظراً لما يجب أن يكون عليه مأمور الضبط القضائي من درجة عالية من التخصص في جرائم تقنية المعلومات عبر شبكة الإنترنت، لذا نرى أنه من الأفضل أن تحذو دولة الإمارات حذو دولة الكويت في إنشاء إدارة مشابهة للإدارة التي أنشأتها وزارة الداخلية الكويتية وهي إدارة مكافحة الجرائم الإلكترونية لما لها من صلاحيات وإمكانيات أكثر مما لمراكز وأقسام الشرطة في هذا الصدد.

(٥٨) د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، ط/ ٢٠١٢م، ص٧٨٥-٧٨٦.

يناسب سمات العالم الافتراضي والجرائم المرتكبة خلالها، وأيضاً طبيعة المجرم المعلوماتي وقدرته على التخفي السريع وذكاءه وخبراته التقنية(٥٩).

ومسألة تلقي البلاغات والتحقق منها وإجراء المعاينات عبر العالم الافتراضي لانتشار الجرائم المرتكبة به، أدى إلى نشاط الضبط القضائي عبر شبكة الإنترنت فهناك مواقع قد تخصصت في تلقي البلاغات والشكاوى عبر العالم الافتراضي(٦٠).

والتحري بالنسبة لجرائم تقنية المعلومات، لا يختلف من حيث مضمونه عنه في غيرها، فالأصل أنه مجرد وصول البلاغ لمأمور الضبط القضائي، يجري التحريات اللازمة وإجراءات الاستدلال كاملة وصولاً لتحديد المتهم والتحفظ على الأدلة وإرساله وإياها لجهة التحقيق خلال المدة المقررة قانوناً، ولعل من وسائل التحري، بل وأهمها هي المراقبة، ومن ثم ينبغي إلقاء الضوء حول ما يسمى بالمراقبة البرمجية عبر الإنترنت، وهي تأخذ صورة إرسال برمجية لخوادم مختلفة بقصد اكتشاف الجرائم والتوصل لمرتكبها عبر الإنترنت ومن ثم تؤدي دور المراقبة، والمرشد الجنائي في العالم المادي شريطة ألا يكون هناك تدخل وعدوان على الحق في الخصوصية وإلا لزم استصدار أمر قضائي بهذا الشأن(٦١).

وفي حالات التلبس يخول لمأمور الضبط ولغيره مطاردة مرتكب الجريمة المعلوماتية، والأصل أن صلاحية المطاردة تتوفر كون القبض والتفتيش صحيحين، ومن ثم فهي من الإجراءات التي تستلزم استصدار أمر قضائي بشأنها، إلا أنه في حالة التلبس بارتكاب الجريمة، تتم المطاردة دون إذن أو أمر قضائي، وتتم المطاردة من جانب جهات الضبط القضائي أو المجني عليه في العالم الافتراضي للجاني مرتكب جريمة ما بقصد تحديد هويته(٦٢).

---

(٥٩) د. مأمون سلامة، قانون الإجراءات الجنائية معلقاً عليه بالفقه وأحكام النقض، ط٢، ٢٠٠٥م، ص٦١٩ وما بعدها.

(٦٠) كما هو الحال في مواقع المباحث الفيدرالية الأمريكية، وإدارة العدل الأمريكية وموقع هيئة حماية البرمجيات الأوروبية وغيرها من المواقع التي تخصصت في ضبط نوعيات معينة من الجرائم كحماية المستهلك والتبليغ عن جرائم المخدرات والمؤثرات العقلية والإرهاب، ومن ثم فقد شملت جميع الجرائم المعلوماتية سواء المستحدثة أو التقليدية. انظر في ذلك: د. محمود عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص٢٦٤.

(٦١) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، وضمانات المتهم المعلوماتي، دراسة مقارنة، ط/٢٠٠٠م، ص٧٠ وما بعدها.

(٦٢) د. محمود عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص٢٧١.

ثانياً – مرحلة التحقيق بشأن جرائم تقنية المعلومات عبر شبكة الإنترنت:

تنص المادة (١٧) من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي على أنه: "تختص النيابة العامة وحدها دون غيرها بالتحقيق والتصرف والادعاء في جميع الجرائم المنصوص عليها في هذا القانون".

وبمطالعة المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات لم نصادف نصاً مشابهاً للنص السابق، ومن ثم نحيل في ذلك إلى قانون الإجراءات الجزائية الإماراتي رقم ٣٥ لسنة ١٩٩٢ في مادته رقم (٦٥)، حيث تنص على: "تباشر النيابة العامة التحقيق بنفسها في الجنايات وكذلك في الجنح إذا رأت ذلك".

من النصوص السابقة يتضح لنا أن إجراءات ومرحلة التحقيق بشأن جرائم تقنية المعلومات عبر شبكة الإنترنت تختص بها النيابة العامة، تحقيقاً وادعاء وتصرفاً، وللنيابة العامة تكليف أحد رجال الضبط القضائي بإجراء أو أكثر من إجراءات التحقيق عدا استجواب المتهم. وقد تم إنشاء نيابة شئون الإعلام والمعلومات والنشر للتحقيق والتصرف في جميع الجرائم التي تقع بالمخالفة لأحكام القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات الكويتي، وذلك تفعيلاً لهذا القانون سالف الذكر(٦٣).

وبالنسبة لدولة الإمارات فقد صدر القرار الوزاري رقم ٢٢٠ لسنة ٢٠١٧ بإنشاء النيابة الاتحادية لجرائم تقنية المعلومات والتي تختص بالتحقيق والتصرف ومباشرة الدعوى الجزائية في جرائم استعمال الإنترنت؛ وذلك لمواجهة الجرائم المستحدثة(٦٤).

وفي شأن جرائم تقنية المعلومات عبر شبكة الإنترنت يلزم الارتقاء بمعلومات المحقق ومهاراته الفنية بشأن أدوات ارتكاب الجريمة المعلوماتية حتى يتمكن من الوصول للحقيقة، فضلاً عن الاستعانة بالخبرة المتخصصة وصولاً لمواجهة المجرم المعلوماتي.

إن إجراءات جمع الأدلة بصفة عامة يمكن حصرها في الانتقال والمعاينة وسماع الشهود والتفتيش وضبط الأشياء ومراقبة المحادثات والاستجواب والمواجهة، وهي

---

(٦٣) http://www.aljarida.com/articles/1485796695790498900/

(٦٤) amp/s/www.emaratalyoum.com/ local - section/ other/ 2017-03-13-1.977733%3fot-to.amppage layout.

من الإجراءات التقليدية في جمع الأدلة، ولا تختلف بمكان سواء بالعالم المادي أو العالم الافتراضي، ومن ثم سنتناول بالبحث ما هو مستحدث متعلقاً بالعالم الافتراضي وأهمها الدليل الرقمي والخبرة التقنية والمراقبة الإلكترونية والتفتيش الإلكتروني، فالدليل الرقمي يعتمد بالأساس على لغة الحاسب الآلي والتي يتم استخدامها ومعالجتها آلياً لاسترجاعها في شكل بيانات ومعلومات، ومن ثم فهو المظهر التقني المعلوماتي، وتلك اللغة في العالم الافتراضي تعتمد على الطابع الرقمي، ومن هنا كان المسمى، فهي تعد أمراً غير محدد لأرقام ثنائية، وكل ما ينتج من جهاز الحاسب الآلي سواء من بيانات أو صور أو غير ذلك إنما يكون نتاج معالجة آلية لتلك الأرقام الثنائية، ومن ثم فإن الدليل الرقمي هو الدليل الأساسي في العالم الافتراضي والذي يثبت الجريمة ومرتكبها – فهو ذلك الذي يستعان فيه بتقنية المعلومات والتي لها دورها في تكوين اقتناع القاضي الجنائي بارتكاب شخص ما لجريمة ما(٦٥)، والأمر يدق خاصة وأن المجرم المعلوماتي من الذكاء بمكان حيث يستخدم برمجيات عالية التقنية يضحى معها من الصعوبة بمكان الوصول للعنوان الإلكتروني للمجرم المعلوماتي، فتمكنه من بث عنوان خاطئ للخوادم المضيفة أو إزالة ذلك الدليل كلياً عن بعد، وهو ما يصعب معه الوصول لمرتكب الفعل الإجرامي(٦٦).

ومن جانبنا نرى أن هذا ليس هو مثار الأخذ بالدليل من عدمه، وإنما يظل في نطاق العرض على القاضي الجنائي ومدى قناعته بسلامته من عدمه، شأنه شأن أي دليل آخر وفق ظروف وملابسات الواقعة المطروحة عليه. ويستلزم من بعد أن يكون القائمون على ضبط تلك الجرائم المعلوماتية من الذكاء والقدرات في مجال التكنولوجيا المعلوماتية ما يفوق ذكاء وقدرات المجرم المعلوماتي، فيظل الأمر صراعاً بين مرتكب الجريمة والقائم على ضبطها.

وأهم ما يميز الدليل الرقمي هو صعوبة التخلص منه، وهو ما يميزه عن الأدلة التقليدية والتي يمكن التخلص منها بإعدامها، أما إذا أمكن التوصل للدليل الرقمي فيصعب من بعد التخلص منه حتى لو حاول المستخدم إزالته من الحاسب أو الإنترنت بأي خاصية إلغاء، فلا يحول ذلك دون استرجاعه إذا ما توافرت البرمجيات التي تتيح ذلك الأمر(٦٧).

---

(٦٥) Amanda Hoey, Analysis of the Police and Criminal Evidence Act sec-69 Computer Generated Issues, UK. 1996, p.2.

(٦٦) د. محمد عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص٢٨٤.

(٦٧) د. محمد عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص٢٨٨.

ويتم الحصول على الدليل الرقمي من خلال فحص الاتصال بالإنترنت، فيتأتى ذلك من خلال نظام الاتصال بالعالم الافتراضي وذلك من خلال ما يطلق عليه متابعة لمسار الاتصال، وهو المسار الذي تتخذه البيانات والمعلومات حال إرسالها أو استدعائها(٦٨)، ويجب أن يكون الدليل الرقمي متوافقاً مع الأدلة التي تم التحصل عليها من العالم المادي.

وتتم المراقبة الإلكترونية أو التفتيش الإلكتروني من خلال تعقب شخص ما عبر الخادم والمضيف، وذلك باستخدام برمجيات معينة تسمح حال معرفة المضيف بالوصول لعنوان المستخدم، ومن بعد يتم بسهولة تعقبه في أي صفحات يدخلها والوصول للمحتوى المعلوماتي الذي يقوم بإرساله أو استقباله، ولكن هذا بطبيعة الحال يتطلب تدخلاً تشريعياً إجرائياً لتنظيم المراقبة الإلكترونية، والتفرقة بين التتبع والوصول للمحتوى المعلوماتي(٦٩)، لما يتضمنه من عدوان على الحرية الشخصية خصوصاً وأن المراقبة قد تتم من دون وقوع جريمة ما، وفي إطار منع وقوع الجريمة وهو ما يثير المخاوف نحو الحريات العامة، وينبغي من بعد التدخل الفوري لتنظيمه قانوناً، وأن يكون الدور الوقائي مقصوراً على الصفحات والمواقع المباحة للكافة فقط، وأن يتم الفصل بين التعقب فقط أو فحص المحتوى المعلوماتي، فتلك الصورة الأخيرة إنما تستلزم بالضرورة الحصول على الأمر القضائي بإجرائه من الجهة المختصة قانوناً حال توافر شرائطه(٧٠).

ونظراً للطبيعة المستحدثة لجرائم تقنية المعلومات عبر شبكة الإنترنت، فلها ما يميزها من عناصر فنية تتعلق بالإجراءات والتصرفات التي تتخذ بدءً من تلقي البلاغ مروراً بكافة مراحل التحقيق المختلفة ووصولاً للأدلة وحفاظاً عليها، وبما يجعلها تتميز بخصوصية شديدة في التعامل تتطلب فريق عمل لديه مهارة تقنية عالية، وهو ما يطلق عليه الخبرة التقنية، ولعل ذلك ما يضفي أهمية خاصة بشأن الخبرة التقنية في العالم الافتراضي فضلاً عن طبيعة ذلك العالم الافتراضي من الأساس وسمات

(٦٨) Vicent Gryabaum, Le droit de reproduction et l'heure de la société de l'information, à propos de la directive 2001/20/CE du Parlement Européen et du conseil du 22/mai/2001 sur l'harmonisation de certains aspects du droit voisins dans la société' de l'information, p.2.

(٦٩) د. هلالي عبد اللاه أحمد، المرجع السابق، ص٢١٧ وما بعدها.

(٧٠) د. عمر محمد يونس، الجرائم الناشئة عن استخدام الإنترنت الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤م، ص١٨٨.

المجرم المعلوماتي وصولاً لضبط الجريمة ومرتكبها وبما يستلزم توافر تلك الخبرة التقنية لدى الخبراء ومأموري الضبط وجهات التحقيق(٧١).

المطلب الثاني
مرحلة المحاكمة

تمهيد وتقسيم:

سنقصر دراستنا على المستجدات التي تثيرها جرائم تقنية المعلومات وسنعرض في هذه المرحلة لمسألة في غاية الأهمية في مجال دراستنا نظراً لطبيعة العالم الافتراضي وعدم الاعتراف بالحدود الإقليمية، وهي مسألة الاختصاص وما تثيره من مشكلات في مرحلة المحاكمة، وذلك بشأن المحاكم الجنائية، كما سنعرض لقيود المحاكمات بشأن الجرائم المرتكبة خارج الدولة، ثم لمظاهر التعاون الدولي بالنسبة للإجراءات الجنائية، وصولاً للمواجهة المثلى للجريمة المعلوماتية، وذلك من خلال الآتي:

أولاً – القواعد الحاكمة لاختصاص المحاكم الجنائية بجرائم تقنية المعلومات:

إن البحث في القواعد الحاكمة لاختصاص المحاكم بجرائم تقنية المعلومات يستوجب العرض لتطور تلك القواعد في كل من القانون الكويتي والقانون الإماراتي وصولاً للمبادئ الأساسية في هذا الصدد.

١ – في التشريع الكويتي:

لقد اتخذ المشرع العقابي الكويتي في القانون رقم ١٦ لسنة ١٩٦٠ بإصدار قانون الجزاء، أصلاً عاماً وهو أن التشريع الجزائي الكويتي هو الذي يطبق دون غيره على من يرتكب في إقليم الدولة فعلاً يعد جريمة حسب النصوص الجزائية الكويتية أياً كانت جنسية مرتكب الفعل استناداً لمنطق سيادة دولة الكويت، واعتباراً من تأمين الحقوق الجديرة بالحماية الجنائية، وأورد ذلك بالمادة رقم (١١) من قانون الجزاء الكويتي والتي جرى نصها على أنه: "تسري أحكام هذا القانون على كل شخص يرتكب في إقليم الكويت وتوابعها جريمة من الجرائم المنصوص عليها فيه. وتسري

(٧١) د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، طبعة نادي القضاة، ٢٠١٠م، ص١٣٤ وما بعدها.

على كل شخص يرتكب خارج إقليم الكويت فعلاً يجعله فاعلاً أصلياً أو شريكاً في جريمة وقعت كلها أو بعضها في إقليم الكويت". كما تنص المادة (١٢) على أنه: "تسري أحكام هذا القانون أيضاً على كل شخص كويتي الجنسية يرتكب خارج الكويت فعلاً معاقباً عليه طبقاً لأحكام هذا القانون وطبقاً لأحكام القانون الساري في المكان الذي ارتكب فيه هذا الفعل، وذلك إذا عاد إلى الكويت دون أن تكون المحاكم الأجنبية قد برأته مما أسند إليه".

وفي هذا الشأن لا لبس في أن الجريمة المرتكبة في دولة الكويت يطبق بشأنها قانون الجزاء الكويتي، ومن ثم ينعقد الاختصاص بها للقضاء الكويتي، وبشأن الجريمة المرتكبة خارج دولة الكويت فقد نص المشرع الكويتي في المادة (١٢) على انعقاد الاختصاص للقضاء الكويتي عند ارتكاب الكويتي في الخارج لفعل معاقب عليه طبقاً لأحكام القانون الكويتي ولأحكام القانون الساري في مكان ارتكاب الفعل المجرم، وذلك عند عودته إلى الكويت دون أن تكون المحاكم الأجنبية قد برأته.

كما نصت المادة (١٣) من قانون الجزاء الكويتي على أنه: "في جميع الأحوال لا تقام الدعوى الجزائية على مرتكب جريمة في الخارج إذا ثبت أن المحاكم الأجنبية حكمت عليه نهائياً واستوفى عقوبته".

وهذا يعد قيداً بشأن الجرائم المرتكبة خارج دولة الكويت، فلا تقام الدعوى الجزائية على مرتكب جريمة أو فعل في الخارج إذا ثبت أن المحاكم الأجنبية قد حكمت عليه نهائياً واستوفى عقوبته. وتثار هذه المسألة كثيراً في جرائم تقنية المعلومات لانعقاد الاختصاص للعديد من الدول في إطار سمات العالم الافتراضي، وقد تتم محاكمة الجاني في دول معينة، ومن ثم كان لزاماً الإشارة لمدى الاعتداد بتلك الأحكام وآثارها المعتبرة، وهو ما جرى عليه العرف الدولي وأخذت به تشريعات جنائية مختلفة.

وبمطالعة القانون الكويتي رقم ٦٣ لسنة ٢٠١٥ لم نصادف نصاً واحداً يتعرض للجرائم الإلكترونية المرتكبة خارج البلاد، وذلك خلافاً لما سار عليه المشرع الإماراتي والذي نص على ذلك في المادة ٤٧ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ على أنه: "مع عدم الإخلال بأحكام الفصل الثاني من الباب الثاني من الكتاب الأول من قانون العقوبات، تسري أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة، إذا كان محلها نظاماً معلوماتياً إلكترونياً أو شبكة معلوماتية أو موقعاً إلكترونياً أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة أو إحدى الهيئات أو المؤسسات العامة المملوكة لأي منهما".

ولذا نناشد المشرع الكويتي بأن يحذو حذو نظيره الإماراتي وينص على ذلك في أقرب تعديل تشريعي له، حتى يكون القانون رقم ٦٣ لسنة ٢٠١٥ قانوناً مكتملاً من هذه الزاوية.

٢ – في قانون العقوبات الاتحادي الإماراتي لسنة ١٩٨٧م:

تنص المادة (١٦) من القانون سالف الذكر على أنه: "تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة" وهذا يعني أن قانون العقوبات الاتحادي الإماراتي هو الذي يطبق دون غيره على كل من يرتكب جريمة على إقليم دولة الإمارات العربية المتحدة، أياً كانت جنسية مرتكب الجريمة، وذلك استناداً لمبدأ السيادة وحفاظاً على حدود الدولة.

كما تنص المادة (١٩) من القانون ذاته على أنه: "يسري هذا القانون على كل من ارتكب فعلاً خارج الدولة يجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها داخل الدولة".

كما تنص المادة (٢٠) على أنه: "يسري هذا القانون على كل من ارتكب فعلاً خارج الدولة يجعله فاعلاً أو شريكاً في جريمة من الجرائم الآتية:

١ – جريمة ماسة بأمن الدولة الخارجي أو الداخلي أو ضد نظامها الدستوري أو سنداتها المالية المأذون بإصدارها قانوناً أو طوابعها أو جريمة تزوير أو تقليد محرراتها أو أختامها الرسمية.

٢ – جريمة تزوير أو تقليد أو تزييف عملة الدولة أو ترويجها أو حيازتها بقصد ترويجها سواء تمت تلك الأفعال داخل الدولة أو خارجها.

٣ – جريمة تزوير أو تقليد أو تزييف عملة ورقية أو مسكوكات معدنية متداولة قانوناً في الدولة أو ترويج تلك العملات والمسكوكات فيها أو حيازتها بقصد ترويجها".

كما تنص المادة (٢١) على أنه: "يسري هذا القانون على كل من وجد في الدولة بعد أن ارتكب في الخارج بوصفه، فاعلاً أو شريكاً، جريمة تخريب أو تعطيل وسائل الاتصال الدولية أو جرائم الاتجار بالمخدرات أو في النساء أو الصغار أو الرقيق أو جرائم القرصنة والإرهاب الدولي".

كما تنص المادة (٢٢) من القانون ذاته على أنه: "كل مواطن ارتكب وهو خارج الدولة فعلاً يعد جريمة بمقتضى أحكام هذا القانون سواء بوصفه فاعلاً أو شريكاً، يعاقب طبقاً لأحكامه إذا عاد إلى البلاد وكان ذلك الفعل معاقباً عليه بمقتضى قانون البلد الذي وقع فيه. ويسري هذا الحكم على من يكتسب جنسية الدولة بعد ارتكاب الفعل".

كما تنص المادة (٢٣) على أنه: "لا تقام الدعوى الجنائية على مرتكب جريمة في الخارج إلا من النائب العام ولا يجوز إقامتها على من يثبت أن المحاكم الأجنبية أصدرت حكماً نهائياً ببراءته أو إدانته واستوفى العقوبة، أو كانت الدعوى الجنائية أو العقوبة المحكوم بها سقطت عنه قانوناً أو حفظت السلطات المختصة بتلك الدولة التحقيق. ويرجع في تقدير نهائية الحكم وسقوط الدعوى أو العقوبة أو حفظ التحقيق إلى قانون البلد الذي صدر فيه الحكم.

فإذا كانت العقوبة المحكوم بها لم تنفذ كاملة وجب استيفاء مدتها، أما إذا كان الحكم بالبراءة صادراً في جريمة مما نص عليه في المادتين (٢٠)، (٢١) وكان مبنياً على أن قانون ذلك البلد لا يعاقب عليها، جازت إقامة الدعوى الجنائية عليه أمام محاكم الدولة، وتكون المحكمة الكائنة بمقر عاصمة الاتحاد هي المختصة بنظر الدعوى".

وطبقاً للنصوص السابقة فإن المشرع الإماراتي قد جعل تطبيق هذا القانون على كل من يرتكب فعلاً خارج الدولة، ويكون فاعلاً أو شريكاً في جريمة وقعت كاملة داخل الدولة أو وقع جزء منها في الدولة وجزء آخر خارجها، كما أن هناك بعض الجرائم ذات الخطورة بمكان والتي تقع خارج الدولة وتمس أمن الدولة السياسي والاقتصادي وقد نصت عليها المادة (٢٠) من القانون ذاته، كما يطبق هذا القانون على بعض الجرائم الدولية ذات الأهمية والتي تعد على درجة كبيرة من الخطورة الدولية لجرائم الاتجار في الرقيق والنساء والأطفال والمخدرات والإرهاب الدولي والتي وقعت في الخارج ووجد مرتكبها في الدولة وذلك في المادة (٢١)، كما يطبق القانون كذلك على من يرتكب في الخارج فعلاً يعد جريمة بمقتضى أحكام القانون الإماراتي وكان معاقباً عليه في الدولة التي ارتكب الفعل فيها وعاد الجاني إلى البلاد.

كما أن هناك قيداً نص عليه المشرع الإماراتي في المادة (٢٣) منه، وهو عدم إقامة الدعوى الجنائية على مرتكب جريمة في الخارج إلا من النائب العام، ولا تقام على من برئ من الجريمة أو أدين واستوفى العقوبة أو سقطت العقوبة أو الدعوى الجنائية عنه قانوناً أو حفظت بمعرفة السلطات المختصة في الدولة.

والمشرع الإماراتي لم يكتف بنصوص قانون العقوبات الاتحادي الإماراتي لسنة ١٩٨٧، بل أفرد نصاً في المرسوم بقانون رقم ٥ لسنة ٢٠١٢ وهو نص المادة ٤٧ سالفة الذكر وذلك بالنسبة للجرائم المعلوماتية التي تتم خارج الدولة، وحسناً فعل ذلك حتى يكون التشريع الخاص بمكافحة جرائم تقنية المعلومات مكتملاً من هذا الجانب، وفي حالة وجود نقص يتم الرجوع إلى قانون العقوبات في هذا الصدد.

وتطبق كل هذه النصوص على الجرائم المستحدثة والتي تتم عن طريق شبكة الإنترنت.

ثانياً – مظاهر التعاون الدولي بالنسبة للإجراءات الجنائية:

بعد أن ناقشنا القواعد الحاكمة لاختصاص المحاكم الجنائية في جرائم تقنية المعلومات عبر شبكة الإنترنت، فيكون من الواجب مناقشة مظاهر التعاون الدولي في الإجراءات الجنائية، نظراً للطبيعة الخاصة بالعالم الافتراضي وبجرائم تقنية المعلومات حيث إن هذا العالم لا يعترف بحدود ما، فمستخدم الشبكة المعلوماتية يمكنه الانتقال بين أرجاء العالم دون أن يتحرك من مكانه، ومن ثم فإن أغلب الجرائم المرتكبة في هذا العالم الافتراضي تعد جرائم عابرة للحدود، وقد يساهم فيها أكثر من شخص في عدة دول، ويقع ضحيتها العديد من المجني عليهم في دول عديدة ومختلفة، كذلك ومن ثم كان للتعاون الدولي أهميته العظمى في مكافحة جرائم تقنية المعلومات، ولذا سنبحث أهم أوجه التعاون القضائي الدولي في المجال الجنائي كالمساعدات القضائية الدولية وتسليم المجرمين.

فالمساعدات القضائية الدولية هي كل إجراء قضائي تقوم به دولة ويكون من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم(٧٢). ولها عدة صور: الصورة الأولى: تبادل المعلومات القضائية مع دول أخرى بشأن أشخاص المتهمين في قضايا جنائية وبشرط المعاملة بالمثل(٧٣)، ويتم التخاطب بين السلطات القضائية المختصة في الدول المختلفة ويجوز أن يتم بالطرق الدبلوماسية. أما الصورة الثانية: فهي الإنابة القضائية وهي طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة المنيبة إلى الدولة المنابة للفصل في مسألة معروضة على السلطات القضائية في الدولة المنيبة ويتعذر عليها القيام به بنفسها(٧٤)، وهي بهذا الوصف تسهيل الإجراءات الجنائية وذلك بهدف كشف الحقيقة عن طريق سماع الشهود وإجراء المعاينات وكافة إجراءات التحقيق(٧٥).

---

(٧٢) د. جميل عبد الباقي الصغير، جرائم الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، ط/ ٢٠١٠م، ص٧٠.

(٧٣) د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ط/٢٠٠٣م، ص٨٥ وما بعدها.

(٧٤) د. عمر محمد سالم، الإنابة القضائية الدولية في المسائل الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، ط/٢٠١٠م، ص٥٦.

(٧٥) انظر في ذلك: اتفاق المساعدة القضائية بين مصر والكويت في ٣ يناير عام ٢٠١٧.

وبالنسبة لتسليم المتهمين، فإن مرتكب جرائم تقنية المعلومات عبر شبكة الإنترنت في العديد من الأحوال قد يكون في دولة أجنبية غير التي وقعت فيها الجريمة مما يؤدي إلى إفلاته من العقاب، فكان من الأهمية اللجوء إلى تسليم المتهمين ويتم عن طريق الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى جرائم الإنترنت، فإن كان قانون هذه الدولة يسمح بالمحاكمة وجب عليها ذلك وإلا قامت بتسليمه إلى الدولة المختصة بذلك(٧٦).

ثالثاً – كيفية إثبات الجريمة المعلوماتية جنائياً عبر شبكة الإنترنت:

تعد قواعد الإثبات من القواعد القانونية ذات الأهمية الخاصة، فالحق موضوع الدعوى لا تكون له أية قيمة إذا لم يقم الدليل على الواقعة التي يستند إليها، وهي القواعد التي تتعلق بالبحث عن الأدلة ووضعها أمام القضاء حتى يمكن تقدير هذه الأدلة، بمعنى أن الإثبات الجنائي ما هو إلا جميع الأدلة التي تؤكد وقوع الجريمة والتي تمنح القاضي اليقين لإدانة المتهم أو يراوده الشك فيها ومن ثم يحكم بالبراءة لأن الشك يفسر لصالح المتهم، وحتى نصل للدليل اللازم للإثبات فلابد من جمع عناصر التحقيق والدعوى وتقديمها إلى سلطة التحقيق الابتدائي، فإن أسفر التحقيق عن أدلة تدين المتهم، يتم تقديمه للمحاكمة، وتعد مرحلة المحاكمة أهم مراحل الدعوى الجنائية(٧٧)، وسوف نناقش إثبات الجريمة المعلوماتية بشهادة الشهود (الخبير)، الإقرار، الأدلة الرقمية، وكذلك القرائن، وذلك على النحو الآتي:

أ – إثبات جريمة تقنية المعلومات (الجريمة الإلكترونية) بالشهادة:

تتمثل الشهادة في تلك المعلومات التي يقدمها شخص أو أشخاص إلى سلطة التحقيق أو المحكمة(٧٨)، وللشهادة في الجرائم المعلوماتية دور هام، فهي تدل على الواقعة ذات الأهمية القانونية، حيث تدل على وقوع الجريمة ونسبتها للمتهم في الإطار الجنائي، والشهادة هي التي يدلي بها الشاهد وهو من الأشخاص الذين يكونون خارج نطاق الجريمة (ليس من أطراف الخصومة) وتكون عنده معلومات تفيد التحقيق

(٧٦) Ulrich Sieber, International Cooperation against Terrorist Use of the Internet,?d- ERES 2006/3 (Vol. 77).

(٧٧) د. عبد الناصر محمد فرغلي، د. محمد عيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٧م، ص١٦.

(٧٨) د. فتحي بن الطيب الخماسي، الفقه الجنائي الإسلامي، دمشق، سوريا، دار قتيبة، ص٩٧.

والمحكمة لكشف الحقيقة من حيث معرفة الأفعال التي ارتكبت وجسامتها ومن ثم نسبتها إلى الفاعل(٧٩)، والشهادة في الجريمة المعلوماتية لا تختلف من حيث ماهيتها عنها في الجريمة التقليدية، فالشاهد في الجريمة المعلوماتية هو الشخص الفني الذي يمتلك من الخبرة والتخصص في تقنية المعلومات ولديه معلومات هامة وجوهرية لازمة لدخوله في نظام المعالجة الآلية إذا كانت مصلحة التحقيق تقتضي البحث عن أدلة الجريمة وهو ما يسمى بالشاهد المعلوماتي وهو أحد الطوائف الآتية(٨٠): المحللون والمبرمجون ومشغلو الحاسب الآلي ومهندسو الصيانة والاتصالات ومديرو النظم.

وللشهادة كدليل إثبات في الجريمة المعلوماتية عدة شروط وهي:

١ – أن تكون الشهادة دليلاً يقينياً بمعنى أن تقترب الشهادة نحو الحقيقة الواقعية قدر الإمكان، وأن تكون بعيدة كل البعد عن الظنون والتخمينات(٨١).

٢ – يتعين مناقشة الشاهد كدليل على الجريمة الإلكترونية تطبيقاً لمبدأ شفوية المرافعة(٨٢).

٣ – مشروعية الدليل الجنائي بالنسبة للشهادة، فالأدلة في أي جريمة تبنى على دليل أخلاقي، ومن ثم يجب أن تكون هذه الأدلة مشروعة بمعنى أن تتفق إجراءات

---

(٧٩) د. فتحي بن الطيب الخماسي، المرجع السابق، ص١١٢.

(٨٠) د. هلالي عبد اللاه أحمد، التزام الشاهدة بالإعلام في الجرائم المعلوماتية، القاهرة، دار النهضة العربية، ٢٠٠٠م، ص٢٣-٢٤.
وحيث إن طوائف الشهود المذكورين في المتن يعدون من أهل الخبرة في مجال تقنية المعلومات، فيكون للمحكمة أن تستعين بهم لإبداء الرأي في مسألة فنية متعلقة بالقضية، حيث تنص على ذلك المادة ١٧٠ من القانون رقم ١٧ لسنة ١٩٦٠ في شأن الإجراءات والمحاكمات الجزائية الكويتي بقولها: "للمحكمة أن تستعين بخبير تندبه لإبداء الرأي في مسألة فنية متعلقة بالقضية، ويقدم الخبير تقريراً مكتوباً للمحكمة برأيه" وهي المقابلة للمادة ١٨٠ من قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة رقم ٣٥ لسنة ١٩٩٢.

(٨١) د. هند سليمان الخليفة، الحاسب الجنائي في الدول الغربية، دراسة استطلاعية، دراسة مقدمة لمؤتمر تقنية المعلومات والأمن الوطني المنعقد بالرياض في الفترة من ١-٤/١٢/٢٠٠٧، ص٦٢.

(٨٢) د. كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة من ٢٥-٢٨/١٠/١٩٩٣، القاهرة، ص٥٩.

الحصول على الشهادة كدليل إثبات للجريمة بما يتفق والقواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر(٨٣).

ب – إثبات جرائم تقنية المعلومات (الجريمة الإلكترونية) بالإقرار:

يقصد بالإقرار، إقرار المرء على نفسه فيما نسب إليه، وقد عرف بسيد الأدلة في المواد الجزائية(٨٤)، والإقرار من المتهم قد يكون شفهياً وقد يكون مكتوباً وأيهما كاف للإثبات، لكن الإقرار الشفوي يعتبر أقل قيمة في الإثبات من الإقرار المكتوب(٨٥).

وينقسم الإقرار إلى إقرار قضائي وهو الذي يصدر أمام المحكمة التي تنظر الدعوى الجزائية بالفعل، ويجيز هذا الإقرار للمحكمة الاكتفاء به والحكم على المتهم بغير سماع شهود(٨٦)، والإقرار غير القضائي وهو الذي يصدر خارج المحكمة التي تنظر الدعوى الجزائية وهو بهذا يعد اعترافاً غير قضائي، والقاضي الجزائي لما له من حرية في تكوين عقيدته، ومن ثم يملك الحرية في تقدير قيمة الاعتراف سواء أكان قضائياً أم غير قضائي(٨٧).

وقد تبنى المشرع الكويتي فكرة الإقرار في المادتين ١٥٦ و١٥٧ من القانون رقم ١٧ لسنة ١٩٦٠ بشأن الإجراءات والمحاكمات الجزائية، ففي الأولى ألزم المحكمة بأن تسمع أقوال المتهم تفصيلاً وتناقشه فيها، وإذا اطمأنت إلى أن الاعتراف صحيح، ورأت أنه لا حاجة إلى أدلة أخرى، فلها أن تستغني عن كل إجراءات التحقيق الأخرى أو بعضها، وأن يتقبل في القضية، ولها أن تتم التحقيق إذا وجدت لذلك داعياً، وفي الثانية اعتبرت أثر اعترافات المتهم الصريحة والقاطعة بارتكاب الجريمة قاصرة عليه دون سواه(٨٨).

---

(٨٣) د. عبد الكريم أبو الفتوح درويش، الإدارة الاستراتيجية لمكافحة الجرائم المستحدثة، الإمارات العربية المتحدة، شرطة دبي، ٢٠٠٣م، ص٥٢-٥٣.

(٨٤) د. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، القاهرة، دار النهضة العربية، القاهرة، ط١، ٢٠٠٦م، ص٦٦.

(٨٥) د. محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٤م، ص٧٥.

(٨٦) د. يونس عرب، جرائم الحاسب الآلي والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي المنعقد في الفترة من ١٠-٢٠٠٢/٢/١٢، أبو ظبي، المركز العربي للدراسات والبحوث الجنائية، ٢٠٠٢م، ص٣٠٤.

(٨٧) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٢م، ص٩٧.

(٨٨) والمادة ١٥٦ من القانون الكويتي هي المقابلة للمادة ١٦٥ من قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة (القانون الاتحادي رقم ٣٥ لسنة ١٩٩٢) وهي المعدلة بالقانون رقم ٢٩ لسنة ٢٠٠٥.

ج – إثبات جرائم تقنية المعلومات (الجريمة الإلكترونية) بالخبرة الفنية:

تعتبر الخبرة إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لاستخلاص الدليل الرقمي منه، أو تعتبر الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدات فنية أو إدارية لا تتوافر لدى النيابة العامة أو القضاء(٨٩).

وتكمن أهمية الخبرة في أنها تنير الطريق للقاضي الذي يهتدي به لتحقيق العدالة خاصة في المجال الجنائي، وتزداد هذه الأهمية وتصبح ضرورية وحتمية في إثبات الجرائم الإلكترونية، فالخبرة وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية، ومنذ ظهور الجريمة الإلكترونية تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي(٩٠).

وحيث إن عملية تجميع الأدلة الرقمية الجنائية في جرائم تقنية المعلومات من أصعب وأخطر الأمور التي تواجه عملية الإثبات الجنائي فكان من اللازم اللجوء إلى خبير قضائي معلوماتي يكون على دراية بهذه المسائل للحصول على الدليل العلمي والفني من الناحية الجنائية، كما أن عملية تجميع الأدلة الرقمية في جرائم تقنية المعلومات والتي تتم عبر الشبكة العالمية (شبكة الإنترنت) من خلال ثلاث مراحل(٩١): وهي مرحلة تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة، حيث تتبع الحاسبات، الخوادم التي دخل منها ومحاولة إيجاد أثر له، أما المرحلة الثانية فهي مرحلة المراقبة، وأخيراً مرحلة ضبط الأجهزة المشتبه فيها وفحصها.

ومن أهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم الإلكترونية هي:

---

(٨٩) د. مأمون سلامة، الإجراءات الجنائية في التشريع المصري، القاهرة، دار النهضة العربية، ٢٠٠١م، ص٦٤٥.

(٩٠) د. علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، محور القانون الجنائي في الفترة من ٢٦-٢٨/٤/٢٠٠٣، ص٢٨٥.

(٩١) د. محمد أمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والحاسب الآلي والإنترنت المنعقد في الفترة من ١-٣/٥/٢٠٠٠، الإمارات العربية المتحدة، العين كلية الشريعة والقانون، ص٢٤٣.

وصف الحاسبات المستخدمة في الجرائم(٩٢)، وكذلك بعض المعلومات والتقنيات المتعلقة بالحاسبات(٩٣).

وحيث إن للدليل الجنائي الرقمي أهمية كبرى ودوراً رئيسياً في معرفة كيفية حدوث الجريمة ومن ثم تباعاً أن يحتوي التحقيق الجنائي الرقمي على هذا الدليل، ويجب أن تكون المنشأة على استعداد وتأهب لمثل هذه الأمور غير التقليدية، كما يجب أن يكون الأشخاص المسؤولون عن التعامل مع هذه الأمور على فهم كبير واطلاع بالأمور التقنية وكيفية التعامل معها، كما أن الجريمة الإلكترونية والمعلوماتية تتم في بيئة أو إطار لا علاقة له بالأوراق أو المستندات، ومن ثم يمكن للجاني في لحظات أن يمحو المعلومات التي تم تدوينها قبل وصول الجهات المعنية إليها(٩٤).

ومما سبق يمكن توضيح القواعد الفنية التي تحكم عمل الخبير في مجال جرائم تقنية المعلومات وهي:

١ – الطرق الحديثة للوصول إلى الدليل الرقمي وتأثيرها على قوته في الإثبات الجنائي: فإذا كانت الوسائل التقليدية كافية لإثبات الجرائم التقليدية، إلا أنها ليست كذلك بالنسبة للجرائم المستحدثة وهي جرائم تقنية المعلومات، فأدلة الإثبات في الجرائم المستحدثة كجريمة التلاعب في الجانب المعنوي للحاسب الآلي يمكن إثباتها بأدلة تنتج عن وسائل إلكترونية(٩٥).

والطبيعة الفنية للكثير من الأدلة التي يمكن الحصول عليها من الوسائل الإلكترونية قد تكون محلاً لفحص معملي يقوم به أهل الخبرة الذين يتأثرون في عملهم بآراء شخصية لهم أو نتائج علمية قد تكون غير سليمة؛ مما يؤدي إلى البعد عن الوصول إلى الحقيقة، وبالتالي يقلل من درجة الاقتناع الذاتي للقضاة عندما تعرض عليهم هذه الأدلة بموجب تقارير الخبرة، مما يؤدي إلى فساد الحكم الذي ينتهي

(٩٢) د. عبد الناصر محمد فرغلي، د. المسماري محمد عبيد، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المرجع السابق، ص٢٧.

(٩٣) د. عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، القاهرة، دار النهضة العربية، ط٢، ٢٠٠٢م، ص٣٩.

(٩٤) د. عبد الفتاح بيومي حجازي، القانون الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مصر، دار الكتب القانونية، ٢٠٠٥م، ص٢٤.

(٩٥) د. كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال تقنية المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة من ٢٥-٢٨/١٠/ ١٩٩٣، القاهرة، ١٩٩٣م، ص٧٢-٧٣.

إليه القضاة، كما يؤثر في صحة الدليل الذي تم التوصل إليه من الوسائل الإلكترونية، تلك الإجراءات التي تتم بهدف الوصول إليه، فإن كانت وليدة إجراءات غير مشروعة فإنه يترتب عليها عدم مشروعيتها، ومن ثم بطلان الدليل المتحصل منها(٩٦).

٢ – تحديد مدى ارتباط الدليل المادي بالدليل الرقمي: فيتم في هذه المرحلة فحص كل من الدليل المادي المضبوط والدليل الرقمي المستخرج من جهاز الحاسب الآلي الموجود بملف النظام المضبوط، وبذلك يتم الربط بين الدليلين مما يجعل الدليل من الثقة واليقين اللذين يؤديان إلى قبوله أمام جهات التحقيق وجهات الحكم.

(٩٦) د. نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في العين بدولة الإمارات العربية المتحدة في الفترة من ١-٣/٥/٢٠٠٠، ص٧١.

المبحث الثالث
جريمة الدخول غير المشروع للنظام المعلوماتي كمثال على الجريمة المستحدثة

تفترض جريمة الدخول غير المشروع للنظام المعلوماتي كمثال على الجريمة المستحدثة عدم مشروعية الدخول لشبكة الإنترنت أو بمعنى آخر الدخول للشبكة عن طريق مستخدم غير شرعي(٩٧). ويتكون الركن المادي لهذه الجريمة من النشاط المادي ذي الطبيعة التقنية والمتمثل في الاستخدام غير الشرعي لكلمة المرور أو استخدام تقنية لإيهام المزود بأن المستخدم شرعي، وإدخال تلك الكلمة بالنظام المعلوماتي بهذا الشكل، مما يتأتى معه حدوث التعارف بينه وبين جهاز المستخدم ومن ثم الدخول لشبكة الإنترنت، وتتكامل بذلك عناصر الركن المادي للجريمة والتي نصت عليها المادة (٢) من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي، والتي تناولت هذه الجريمة من حيث الدخول غير المشروع إلى جهاز الحاسب الآلي أو إلى نظامه أو إلى نظام المعالجة الإلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت (وهو برنامج أو نظام إلكتروني لحاسب آلي تم إعداده ليتصرف أو يستجيب لتصرف بشكل مستقل كلياً أو جزئياً، دون تدخل أو إشراف أي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الاستجابة له)، أو إلى شبكة معلوماتية.

وقد تدرج المشرع الكويتي بالعقوبة في جريمة الدخول غير المشروع من عقوبة مخففة في حالة مجرد الدخول غير المشروع فقط، ثم ارتفع بهذه العقوبة حال الدخول غير المشروع عند إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، إلا أنه شدد العقوبة عن ذلك في حالة ما إذا كانت هذه البيانات أو المعلومات شخصية لأنها تعد اعتداء على الحق في الخصوصية، وانتهى المشرع في هذه المادة في فقرتها الأخيرة بتوقيع عقوبة أشد مما سبق لكل من ارتكب الدخول غير المشروع بالشكل المنصوص عليه في الفقرات (١، ٢، ٣) من هذه المادة، أو سهل ذلك للغير وذلك أثناء أو بسبب تأدية وظيفته، أما في دولة الإمارات العربية المتحدة، فقد نص القانون رقم ٥ لسنة ٢٠١٢ والمناظر للقانون الكويتي، على هذه الجريمة كذلك في المادة الثانية بفقراتها الثلاث، حيث وضع ظروفاً مشددة في

(٩٧) د. محمود عبد العزيز أبا زيد، رسالة دكتوراه، المرجع السابق، ص٣٣٢.

حالتين، حالة ما إذا ترتب على هذا الدخول غير المشروع إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات، وكذلك في حالة أخرى وهي حالة ما إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (٢) من هذه المادة شخصية لأنها تعد اعتداء على الحق في الخصوصية(٩٨).

كما أن المادة (٣) من القانون ذاته قد نصت على حالة ما إذا كانت هذه الجرائم المنصوص عليها في المادة (٢/١، ٢) قد ارتكبت بمناسبة أو بسبب تأدية الوظيفة(٩٩).

كما نص المشرع الكويتي في المادة (٣) منه على بعض حالات الدخول غير المشروع، ولكن بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون، وهذه تعد من أخطر حالات الدخول والاختراق غير المشروع؛ لأنها ترتكب في حق الجهات الحكومية بالنسبة للمعلومات والبيانات الخاصة والتي تحمل طابع السرية، وكذلك البيانات والمعلومات الخاصة بحسابات عملاء المنشآت المصرفية(١٠٠)، وقد قسمها المشرع من حيث العقوبة إلى عقوبة مخففة في حالة مجرد الدخول غير المشروع، وأخرى مشددة في حالة إذا ما ترتب على هذا الدخول إلغاء أو إتلاف أو تدمير أو نشر أو تعديل لهذه البيانات أو المعلومات(١٠١).

ولم تتطلب التشريعات التي جرمت فعل الدخول غير المشروع (فعل الاتصال الإلكتروني غير المشروع) أن يترتب ضرر على المجني عليه، فبمجرد إتيان النشاط المؤثم تقع الجريمة، فهي جريمة سلوك وليست جريمة ضرر، ومن ثم لا تفترض تحقق نتيجة، وذلك يرجع إلى المحافظة على السرية الذي يتحقق انتهاكها بمجرد القيام بالاتصال غير المشروع(١٠٢).

---

(٩٨) انظر: نص المادة (٢) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ وهي المناظرة للمادة (٢) من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي.

(٩٩) انظر: المادة (٣) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢.

(١٠٠) انظر: المادة (٣/١) من القانون رقم ٦٣ لسنة ٢٠١٥.

(١٠١) وقد نص المشرع الإماراتي على هذه الحالة من حالات الجرائم الناتجة عن الدخول غير المشروع. وذلك في المادة (٤) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢.

(١٠٢) د. أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، المدة من ٢٦-٢٨ أبريل ٢٠٠٣، منشور على: www.arablawinfor.com

وبعد أن بيَّنا الركن المادي في جريمة الدخول غير المشروع، فإن هذه الجريمة تعد من الجرائم التي يتطلب فيها توافر القصد الجنائي، فهي جريمة عمدية(١٠٣)، فيجب أن يعلم الجاني بأنه يدخل إلى نظام معلوماتي لا يجوز له الدخول فيه وأن تتجه إرادته إلى ذلك.

ويتطلب كل من المشرع الكويتي والإماراتي في تلك الجريمة القصد الجنائي العام وهو علم الجاني بأن دخوله إلى النظام المعلوماتي غير مشروع، وأن تتجه إرادته إلى ارتكاب هذا الفعل، ولا يشترط أن يكون لدى الجاني قصد خاص وهو نية الإضرار بالمجني عليه؛ نظراً لأن هذه الجريمة هي جريمة شكلية (جريمة سلوك)(١٠٤).

ومن حيث القصد الجنائي الخاص، فتظهر أهميته في تشديد العقاب على بعض صور السلوك الإجرامي والتي ترتبط مع جريمة الدخول غير المشروع للنظام المعلوماتي، فإن هناك جرائم أخرى ترتبط مع جريمة الدخول غير المشروع ولكنها تقيد تجريمها باستلزام توافر قصد جنائي خاص لدى المتهم بجانب القصد الجنائي العام(١٠٥)، وسنعالج بعضاً من صور القصد الجنائي الخاص حيث تشكل جرائم تتسم بقصد جنائي خاص وهي:

أولاً: الدخول بقصد العبث بالبيانات المبرمجة: قد يكون القصد من الدخول غير المشروع هو العبث بالبيانات داخل الحاسب الآلي، كأن يقوم بمحوها، أو تغييرها أو حذف البعض منها أو إعادة نشرها، حيث تعاقب المادة الثانية في فقرتها الثانية من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي هذه الصورة من صور الدخول غير المشروع بقولها: "فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين.

(١٠٣) د. أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص٢٩٢.

(١٠٤) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، ١٩٩٢م، ص١٢٤.

(١٠٥) وهو ما يتوافر طبقاً لنص المادة الثانية فقرة أولى من القانون رقم ٦٣ لسنة ٢٠١٥ (لا يحتاج قصد خاص)، وكذلك المادة الثانية فقرة أولى من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ (لا يحتاج قصد خاص)، أما توافر القصد الجنائي الخاص يتحقق في نص المادتين في فقرتهما الثانية.

فإذا كانت تلك البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين.

ويعاقب بالحبس مدة لا تجاوز خمس سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، كل من ارتكب أياً من الجرائم المنصوص عليها أعلاه أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته "(١٠٦).

ما أورده كل من المشرع الكويتي والمشرع الإماراتي بصدد جريمة الدخول غير المشروع بالعقاب بسبب إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها، فما ورد بهذه المادة بخصوص العقاب على البيانات جاء خاصاً بالشبكة المعلوماتية والبرامج أو البيانات الموجودة بها، أما إذا تعلق الأمر ببيانات لا توجد في شبكة معلوماتية، فإن النص يقف قاصراً عن العقاب عليه(١٠٧)، ومن ثم نناشد كلاً من المشرع الكويتي والمشرع الإماراتي بسد هذه الثغرة وتلافيها في أقرب تعديل تشريعي.

ثانياً: الدخول غير المشروع بقصد التهديد والابتزاز: حيث تعاقب على هذه الصورة المادة الثالثة في فقرتها الرابعة من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي والتي تنص على أنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من... ٤- استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه.

فإذا كان التهديد بارتكاب جناية أو بما يعد مساساً بكرامة الأشخاص أو خادشاً للشرف والاعتبار أو السمعة، كانت العقوبة الحبس مدة لا تجاوز خمس سنوات

(١٠٦) وهي المطابقة لنص المادة الثانية في فقرتيها الثانية والثالثة من القانون رقم ٥ لسنة ٢٠١٢ الإماراتي.

(١٠٧) فالشبكة المعلوماتية طبقاً لنص المادة الأولى من القانون رقم ٦٣ لسنة ٢٠١٥ هي: "ارتباط بين أكثر من منظومة اتصالات لتقنية المعلومات للحصول على المعلومات وتبادلها"، كما تنص على ذلك أيضاً المادة الأولى من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ على أنها "ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات".

والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين"[١٠٨].

والمشرع الإماراتي هنا يجرم استعمال الشبكة المعلوماتية أو أية وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه، فهنا لا يعاقب في هذا النص على التهديد أو الابتزاز بالفعل، بل يكفي اتجاه نيته على ذلك القصد حتى ولو لم يحدث، ويترك استخلاص تلك النية إلى المحكمة في ضوء ظروف وملابسات الدعوى، فإن قام بالتهديد والابتزاز فعلاً فهو بصدد جريمتين: الأولى الدخول غير المشروع، والثانية التهديد والابتزاز.

ثالثاً: الدخول غير المشروع بقصد العبث بالموقع: تنص المادة الرابعة الفقرة الثانية من القانون رقم ٦٣ لسنة ٢٠١٥ على أنه: "يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ... ٢- أدخل عمداً عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات ما من شأنه إيقافها عن العمل أو تعطيلها، أو دخل موقعاً في الشبكة المعلوماتية لتغيير التصاميم لهذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه أو إيقافه أو تعطيله"[١٠٩].

في هذه الصورة يعاقب المشرع الكويتي من يقوم بالدخول غير المشروع أو الدخول المشروع في النظام الإلكتروني إذا كان قصده أن يعتدي على الموقع بطريقة من الطرق التالية: إتلاف أو تعديل الموقع، شغل عنوان الموقع والمعروف أيضاً بجريمة شغل اسم موقع إلكتروني، فمن يقوم بالتداخل في عنوان الموقع حتى يحول دون استخدامه بشكل أو بآخر يسري عليه هذا التجريم[١١٠].

والتجريم يتوافر ومن ثم يحق توقيع عقوبة كاملة على الفاعل حتى ولو لم

---

(١٠٨) انظر: نص المادة (١٦) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ وهي المناظرة للمادة الثالثة فقرة أربعة من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي.

(١٠٩) انظر: نص المادة العاشرة من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ وهي المناظرة للمادة ٢/٤ من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي.

(١١٠) تنص المادة (١) من القانون رقم ٦٣ لسنة ٢٠١٥ على "الموقع: مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد"، كما تنص على ذلك المادة (١) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ على: "الموقع: مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات".

يتمكن من العبث بالموقع ما دام أن نيته من وراء الدخول غير المشروع هي الوصول إلى تحقيق هذه الغاية.

رابعاً: الدخول غير المشروع للحصول على بيانات تمس الأمن الوطني أو الاقتصاد الوطني: وفي هذه الصورة يكون قصد الجاني من الدخول هو أن يحصل على بيانات تمس الأمن الوطني أو الاقتصاد الوطني، حيث تنص على ذلك المادة ١/٣ من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي على أنه: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ١- ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون، فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، تكون العقوبة الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، ويسري هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية"(١١١).

كما تنص كذلك المادة (١٠) من القانون رقم ٦٣ لسنة ٢٠١٥ على أنه: "يعاقب بالحبس مدة لا تجاوز عشر سنوات وبغرامة لا تقل عن عشرين ألف دينار ولا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين، كل من أنشأ موقعاً لمنظمة إرهابية أو لشخص إرهابي أو نشر عن أيهما معلومات على الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات ولو تحت مسميات تمويهية لتسهيل الاتصالات بأحد قيادتها أو أعضائها، أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية"(١١٢).

ويتوافر التجريم وفقاً لصريح نص المادة ١/٣ من التشريع الكويتي حتى ولو لم يتمكن المتهم من الحصول على المعلومات أو البيانات الحكومية السرية، فمجرد الدخول بهذا القصد (الحصول على البيانات والمعلومات الحكومية السرية) يكفي للعقاب، كما أن مجرد إنشاء موقع لمنظمة إرهابية أو لشخص إرهابي يكفي كذلك

(١١١) انظر في ذلك: المادة (٤) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ وهي المناظرة للمادة ١/٣ كويتي.

(١١٢) انظر: نص المادة (٢٦) من المرسم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ وهي المناظرة للمادة ١٠ من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي.

للتجريم بحسب نص المادة العاشرة من التشريع الكويتي رقم ٦٣ لسنة ٢٠١٥، وهذا الأمر يتفق مع نص المادتين ٤، ٢٦ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢، إلا أن المشرع الإماراتي قد توسع في تجريم كل ما يتعلق بجرائم أمن الدولة سواء من الداخل أو الخارج، وذلك بنصه على هذه الجرائم في العديد من نصوصه(١١٣)، مما يعد تضييقاً على كل من تسول له نفسه ارتكاب مثل هذه الجرائم من قريب أو بعيد، ولذا نناشد المشرع الكويتي أن يحذو حذو نظيره الإماراتي وأن ينص على تجريم هذه الأفعال في أقرب تعديل تشريعي له، ولا نكتفي بما هو منصوص عليه في القانون رقم ٣ لسنة ٢٠٠٦ في شأن المطبوعات والنشر الكويتي؛ لأن النصوص الواردة فيه لا تكفي لسد الثغرات الموجودة في القانون رقم ٦٣ لسنة ٢٠١٥؛ لأنها تشير إلى الصحف ووسائل النشر التقليدية، ولم تشر من قريب أو بعيد إلى أي من جرائم تقنية المعلومات عبر شبكة الإنترنت(١١٤).

الخاتمة:

بعد أن انتهينا من دراسة موضوع البحث المعنون "الأحكام العامة للمواجهة الجنائية لظاهرة جرائم تقنية المعلومات: دراسة مقارنة بين قانوني مكافحة جرائم تقنية المعلومات الكويتي والإماراتي"، فقد توصلنا إلى بعض النتائج التي اهتدينا من خلالها إلى طرح بعض التوصيات وذلك على التفصيل الآتي:

١ – إنه من الصعوبة بمكان التوصل إلى اكتشاف الجريمة الإلكترونية؛ وذلك بسبب التقنية المتطورة والسريعة في هذا الصدد.

٢ – إن عملية إثبات الجريمة المعلوماتية وأمر اكتشافها للتوصل إلى مرتكبيها أمر صعب المنال.

٣ – نقص الخبرة الفنية والتقنية لدى رجال الضبط القضائي من رجال الشرطة ومن الموظفين المختصين بهذه الجرائم، ليس هذا فحسب بل إن ذلك ينصرف كذلك للنيابة العامة والقضاة، الأمر الذي يؤدي إلى صعوبة التوصل إلى إثبات هذا النوع من الجرائم.

(١١٣) انظر: المواد: ٢٤، ٢٨، ٢٩، ٣٠، ٣١، ٣٢، ٣٣، ٣٨ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢.

(١١٤) يمكن مراجعة المزيد عن هذه الجريمة وغيرها من جرائم تقنية المعلومات في الباب الأخير من مؤلف حديث للدكتور فتوح الشاذلي بعنوان جرائم التعزير المنظمة في المملكة العربية السعودية – الطبعة الرابعة – مكتبة الرشد ١٤٤١هـ– ٢٠٢٠م.

٤ – تتسم هذه الجرائم بأن أسلوب ارتكابها يعد أسلوباً حديثاً، كما أنها جرائم سريعة التنفيذ وسهلة الإخفاء لدليل ارتكابها وإمكانية محو آثارها، الأمر الذي يترتب عليه وجوبية أن تكون جهات التحقيق والمحاكمة (النيابة العامة والقضاء) على درجة كبيرة من المعرفة والفهم الدقيق بالأنظمة التكنولوجية.

٥ – تحتاج هذه الجرائم عند التحقيق مع مرتكبيها إلى أساليب مستحدثة وليست أساليب تقليدية.

٦ – تعد الشهادة كدليل إثبات بالنسبة للجريمة المعلوماتية في الشق الجزائي من الأهمية بمكان، حيث إنها ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها.

٧ – كذلك فإن الخبرة الفنية تعد من الوسائل المساعدة والهامة في إثبات الجريمة المعلوماتية؛ حيث إنها تبين وتكشف للقاضي الطريق للوصول إلى الجريمة ومرتكبيها.

٨ – من الصعوبة بمكان ظهور الدليل المادي لهذه الأنواع من الجرائم المعلوماتية.

وبعد أن عرضنا ما توصلنا إليه من نتائج فإننا نقترح بعض التوصيات اللازمة في هذا الصدد وهي:

١ – الاهتمام بتدريب الكوادر من العاملين في جهاز الشرطة ورجال القضاء والنيابة العامة، وكذلك الاستعانة بأهل الخبرة في هذا الصدد.

٢ – التحفظ على الأجهزة التي يشتبه في استخدامها في ارتكاب الجريمة المعلوماتية.

٣ – الاهتمام بتطوير دور الخبرة في مجال الجريمة المعلوماتية.

٤ – الاهتمام بإنشاء أقسام وإدارات في جهات الضبط القضائي والتحقيق تكون على درجة عالية من التخصص في مجال جرائم تقنية المعلومات، والعمل على تطويرها بصفة دائمة حسب المستجدات في عالم الإنترنت.

٥ – علاج أوجه القصور التي تم ذكرها في التشريعات المرتبطة بموضوع البحث، كما هو مبين في ثنايا البحث من خلال مناقشة هذا الموضوع؛ وذلك لمواكبة التطور المتلاحق في جرائم تقنية المعلومات.

٦ – حبذا أن تتم صياغة قانون خليجي أو عربي موحد لمكافحة جرائم تقنية المعلومات.

المراجع

أولاً – المراجع العربية:

- أحمد المجذوب، مشكلة تقنين القصد الجنائي، المجلة الجنائية القومية، العدد الأول، مجلد ١٣، ١٩٧٠م.
- أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٠م.
- أحمد فالح الخرابشة، الإشكالات الإجرائية للشهادة في المسائل الجزائية، دار الثقافة، الأردن، ط١، ٢٠٠٩م.
- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، ط٢، ٢٠١٢.
- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، القاهرة، دار النهضة العربية، القاهرة، ط١، ٢٠٠٦م.
- أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني دراسة مقارنة، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، المدة من ٢٦–٢٨/ ٤/ ٢٠٠٣م.
- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، ط/ نادي القضاه، ٢٠١٠م.
- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٢م.
- جميل عبد الباقي الصغير، جرائم الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، ط/ ٢٠١٠م.
- حسام الدين الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي، ط/ ١٩٩٤م.
- سليمان عبد المنعم، دروس في القانون الجنائي الدولي، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠م.
- شمس الدين إبراهيم أحمد، وسائل مواجهة الاعتداءات على الحياة الخاصة في مجال تقنية المعلومات، دار النهضة العربية، ط١، ٢٠٠٥م.
- طارق سرور، جرائم النشر والإعلام، دار النهضة العربية، القاهرة، ٢٠٠٨م.

- عبد الأحد جمال الدين، د. جميل الصغير، المبادئ الرئيسية في القانون الجنائي.
- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ط٣، ٢٠٠٣م.
- عبد الفتاح بيومي حجازي، القانون الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مصر، دار الكتب القانونية، ٢٠٠٥م.
- عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٢م.
- عبد الكريم أبو الفتوح درويش، الإدارة الاستراتيجية لمكافحة الجرائم المستحدثة، الإمارات العربية المتحدة، شرطة دبي، ٢٠٠٣م.
- هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، القاهرة، دار النهضة، القاهرة، ٢٠٠٠م.
- عبد الفتاح الصيفي، الاشتراك بالتحريض وموضعه من النظرية العامة للمساهمة الجنائية، ١٩٨٥م.
- عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، القاهرة، دار النهضة العربية، ط٢، ٢٠٠٢م.
- عبد المهيمن بكر سالم، الإجراءات الجنائية، ج١، ١٩٩٧م.
- عبد الناصر محمد فرغلي، د. محمد عيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٧م.
- علاء محمود يسن حراز، الحماية الجنائية للمعلومات المعالجة آلياً، دراسة مقارنة في القانون الوضعي والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.
- علي أحمد راشد، القانون الجنائي المدخل والنظرية العامة، ١٩٨٤م.
- علي القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، دار الجامعة الجديدة للنشر، ١٩٩٧.
- علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب

القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، محور القانون الجنائي في الفترة من ٢٦-٢٨/ ٤/ ٢٠٠٣م.

- عماد محمد ربيع، حجية الشهادة في الإثبات الجزائي، دراسة مقارنة، دار الثقافة للنشر والتوزيع، ط١، ٢٠١١م.
- عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، ١٩٨٦م.
- عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ج١، ١٩٩٣م.
- عمر محمد سالم، الإنابة القضائية الدولية في المسائل الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، ط١٠، ٢٠١٠م.
- عمر يونس، الجرائم الناشئة عن استخدام الإنترنت الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤م.
- عوض محمد عوض، شرح قانون العقوبات، القسم العام، دار المطبوعات الجامعية، ١٩٩١م.
- فوزية عبد الستار، المساهمة الأصلية في الجريمة، من دون ناشر، ١٩٦٧م.
- كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال تقنية المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة من ٢٥-٢٨/ ١٠/ ١٩٩٣، القاهرة.
- مارتن بور، المدخل إلى الإنترنت، ترجمة أ. عبد السلام رضوان، مجلة الثقافة العالمية، إصدار المجلس الوطني للثقافة والفنون والآداب، الكويت، العدد ٧٦، مايو ١٩٩٦م.
- مأمون سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، ٢٠٠١م.
- محمد أمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والحاسب الآلي والإنترنت المنعقد في الفترة من ١-٣/ ٥/ ٢٠٠٠، الإمارات العربية المتحدة، العين، كلية الشريعة والقانون.
- محمد عمر مصطفى، النتيجة وعناصر الجريمة، مجلة العلوم القانونية والاقتصادية، ع٢، س٧، يوليو ١٩٦٥م، كلية الحقوق، جامعة عين شمس.
- محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب

والإنترنت، رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٤م.

- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، ٢٠٠٣م.
- محمود عبد العزيز أبا زيد، الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.
- محمود كبيش، دروس في الجرائم المضرة بالمصلحة العامة، دار النهضة العربية، القاهرة، ٢٠٠٥م.
- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، ط/ جامعة القاهرة، ١٩٧٨م.
- مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٠م.
- مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ٢٠٠٠م.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م.
- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، وضمانات المتهم المعلوماتي، دراسة مقارنة، ط/ ٢٠٠٠م.
- هند سليمان الخليفة، الحاسب الجنائي في الدول الغربية، دراسة استطلاعية مقدمة لمؤتمر تقنية المعلومات والأمن الوطني المنعقد بالرياض في الفترة من ١-٢٠٠٧/١٢/٤م.
- القانون رقم ٦٣ لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات الكويتي.
- المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الإماراتي المعدل بالقانون ٢ لسنة ٢٠١٨.
- القانون رقم ١٧ لسنة ١٩٦٠ في شأن الإجراءات والمحاكمات الجزائية الكويتي.
- قانون الإجراءات الجزائية رقم ٣٥ لسنة ١٩٩٢ الإماراتي.
- القانون رقم ١٦ لسنة ١٩٦٠ بإصدار قانون الجزاء الكويتي.

- قانون العقوبات الإماراتي لسنة ١٩٨٧.

ثانياً – المراجع الأجنبية:

- Amanda Hoey, Analysis of the Police and Criminal Evidence Act sec-69 Computer Generated Issues, UK. 1996.
- Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, 1998 Wiley computer Publishing, United States of America.
- Janet Abbate, Inventing the Internet, Cambridge, Massachusetts: MIT Press, 1999.
- Jonathan Clough, Principles of Cybercrime, 2 ed - Cambridge University Press 2015, United Kingdom.
- Klaus Tiedeman, Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, Rev. D.P.C. 1984.
- Sebine Marcellin - Taupenas, Internet et le droit international, lamy droit d'l'informatique, No. 74, Octobre 1995.
- Tom Forester and Perry Morrison, Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, 2nd ed., Cambridge, Massachusetts: MIT Press, 1994.
- Ulrich Sieber, International Cooperation against Terrorist Use of the Internet,?d- ERES 2006/3 (Vol. 77).
- Vicent Gryabaum, Le droit de reproduction et l'heure de la société de l'information, à propos de la directive 2001/20/CE du Parlement Européen et du conseil du 22/mai/2001 sur l'harmonisation de certains aspects du droit voisins dans la société' de l'information.

The General Provisions for Criminal Confrontation of the Phenomenon of Information Technology Crimes

A Comparative Study between the Law of Combating Crimes of Information Technology in Kuwait and UAE

Dr. Bader Ahmad Al-Jaser Al-Rajhi

The crime itself is not a new phenomenon, but it is a phenomenon as old as history. However, this phenomenon in its traditional form is less serious and sophisticated than what exists for the new crime committed on the Internet progressively, quickly, and sophisticatedly, as a result of the emergence of information technology tools such as: computer, mobile phone, etc., which led to the emergence of so-called electronic or informatics crime (cybercrime), which posed a serious danger to the individual and his money. Not only that, but the impact of this type of crimes on the security, safety and stability of States, and thus highlighted in our study to combat these crimes through the Kuwaiti law 63 for the year 2015 in the matter of combating information technology crimes as well as the UAE Legislative Decree No. 5 of 2012 entitled: "The General Provisions for Criminal Confrontation of the Phenomenon of Information Technology Crimes: A Comparative Study between the Law of Combating Crimes of Information Technology in Kuwait and UAE".

A brief summary of the content of this research must be indicated, which we divided it into three main Sections preceded by an Introductory Research Section in which we dealt with the phenomenon of information technology crimes on the Internet, in terms of its concept, development and the interest protected. As for the First Section, we discussed the most important substantive provisions of information technology crimes via the Internet. We discussed the crime's elements - Actus reus and Mens rea - at first subsection, then we moved on to discuss the criminal contribution (accomplices) in the second subsection. As for the Second Section, we discussed the most important procedural provisions for the weakness dealt with through legislation. We also added an application to the crimes of information technology and how to combat them according to the provisions of the laws issued in this regard. We presented the crime of illegal access into the information system as an example of the new crime because of the importance of this new crime, in Section Three.