الفصل الرابع

إشكاليات التحقيق في الجرائم المعلوماتية

٤,١ مقدمة

الجرائم المعلوماتية نمطا جديدا من الإجرام لم تكن موجودة في السابق وفي العديد من الحالات نجد ان القصور في التشريع العقابي، حيث هنالك نقص بين في التشريعات العقابية في هذا المجال حيث ترك المشرع في كثير من الأحيان أمر معالجتها للنصوص العقابية التقليدية والقواعد العامة الأمر الذي اوجد فراغا تشريعيا اتضح من خلاله قصور النصوص وعدم كفايتها لتغطية الإشكاليات المتنوعة للجرائم المعلوماتية، وأهم الإشكاليات القانونية التي تعترض مواجهة مثل هذا النوع من الجرائم تتمثل في مشكلات فنية ومشكلات قانونية سيتم تناولها في هذا الفصل بالتقسيم التالي:

المبحث الأول: المشكلات الفنية للتحقيق في الجرائم المعلوماتية

المبحث الثاني: المشكلات القانونية للتحقيق في الجرائم المعلوماتية

٤,٢ المبحث الأول: المشكلات الفنية للتحقيق في الجرائم المعلوماتية

يواجه التحقيق في الجرائم المعلوماتية عدد من المشكلات الفنية تتمثل في المشكلات المتعلقة بالدليل المعلوماتي ومشكلات متعلقة بسلطات الاستدلال والتحقيق، وسيتم تخصيص هذا المبحث لتناول ذلك من خلال مطلبين.

٤,٢,١ المطلب الأول: المشكلات المتعلقة بالدليل المعلوماتي

إذا كان وجود الأدلة بنوعيها المادية والمعنوية او القولية في إطار الجرائم التقليدية هو الذي يرجح كفة الإدانة على البراءة واثبات الجرم إلى مرتكبه، نجد ان ذلك محل أشكال في الجرائم الإلكترونية حيث تتعامل الأجهزة الجنائية الإجرائية مع أشكال غير محسوسة من الادلة، وهو ما يلقي بظلاله على أساليب كشف الجرائم الإلكترونية، وعمليات البحث والتحقيق ومنظومة التدريب التخصصي اللازم لاكتساب المهارات الحقيقية المتطلبة للتعامل مع هذه النوعية من الجرائم، حيث أنه يتعذر اتخاذ اجراءات التفتيش لضبط هذه الجرائم عندما تكون الأجهزة الإلكترونية متصلة بأجهزة خارج الدولة، ويكون تفتيشها ضروري لإماطة اللثام عما تشتمله من جرائم[١٢٣].

كما أن هنالك صعوبات تعترض سبل اكتشاف الجرائم الإلكترونية، خاصة إذا ما وضعنا في الاعتبار قدرة الجاني على تدمير الادلة في مقابل نقص الخبرات عند رجال التحقيق والإمكانات الفنية التي تمكنهم من اكتشاف الجريمة، كما ان الاساليب التي يتعامل معها في خصوص تلك الجرائم لا تسمح لسلطات التحقيق على وجه الخصوص في التعامل معها كما هو الحال في تعاملها مع الجرائم التقليدية [١٢٤].

كما ان إثبات الجرائم الإلكترونية يحيط بها الكثير من الصعاب نظرا لطابعها الخاص والتعقيد في إجراءات تحقيقها في ظل غياب الدليل المرئي الممكن بالقراءة فهمه وإعاقة الوصول إليه بوسائل الحماية الفنية كما يواجه رجال التحقيق ضخامة بالغة في كم البيانات المتعين فحصها كما ان مرتكبي هذه الجرائم يتميزون بأنهم إفراد ذو تدريب عالي جدا تقنيا وملمين بمهارات ومعارف فنية في المجال التقني ومتخصصين فيه.

---

١٢٣. هروال، نبيلة هبة. ٢٠١٣. *الجوانب الإجرائية لجرائم الانترنت*. ص. ٢٣٢.

١٢٤. العريان، محمد علي. ٢٠١٨. *الجرائم المعلوماتية*. ص. ٩٨.

أكثر الاثار التقليدية هو إعاقة الوصول إلى الدليل، وذلك لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول اليها او ترميزها او تشفيرها لإعاقة المحاولات الرامية إلى الوصول اليها والاطلاع عليها او استنساخها، فالبحث والتحقيق ينصب على الكشف عن الجريمة وعن أدلتها التي تثبت صلة شخص ما بها صلة مادية ونفسية، صلة السبب بالمسبب، كما يتم البحث عن الادلة التي تنفي الصلة[١٢٥]، وهنا نجد ان من المعوقات المتعلقة بالجريمة الإلكترونية سهولة محو الدليل او تدميره في زمن قصير جدا، فالجاني يمكنه ان يمحي الادلة التي تكون قائمة ضده او تدميرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فانه يستهدف بالمحو السريع عدم استطاعت هذه السلطات اقامة الدليل ضده، وبالتالي تنصله بمسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي او الشبكة او في الأجهزة [١٢٦] كما يواجه التفتيش عقبات فما هو إلا وسيلة للإثبات المادي، ذلك لأنه اجراء يستهدف ضبط اشياء مادية تتعلق بالجريمة او تفيد في كشف الحقيقة، وغايته دوما هي الحصول على الدليل المادي، وهذا مايتنافر مع الطبيعة غير المادية لبرامج وبينات الحاسب الآلية وكذا شبكة الشبكات، فهي مجرد برامج وبينات الكترونية ليس لها اي مظهر مادي محسوس في العالم الخارجي، وعلى ذلك فلا سبيل لان يرد عليها تفتيش او ضبط، ومن الاجدر إخضاعها لأحكام مستقلة تتلاءم وطبيعتها الخاصة [١٢٧].

وطبيعة التكنولوجيا الرقمية قد عقدت التحدي أيضاً امام اعمال التفتيش والضبط، وذلك بسبب امتداد الأدلة الإلكترونية عبر شبكات الحاسوب في اماكن بعيدة عبر الموقع المادي للتفتيش [١٢٨]، وإن كان

---

١٢٥. موسى، مصطفي محمد. ٢٠٢٠. *التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي*. القاهرة: دار الفكر العربي. ص. ٣٠٦.

١٢٦. عياد، سامي علي. ٢٠٢٠. *الجريمة المعلوماتية وأجرام الانترنت*. ص٧٥.

١٢٧. هروال، نبيلة هبة. ٢٠١٣. *الجوانب الإجرائية لجرائم الانترنت*. ٢٢٦.

١٢٨. مصطفى، عائشة بن قارة. ٢٠٠٦. *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن*. الإسكندرية: دار الجامعة الجديدة. ٩٨.

من الممكن الوصول اليها من خلال الحاسوب المأذون بتفتيشه، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي اخر او حتى في بلد آخر، فهل يمتد تفتيش حاسوب معين إلى الاجهزة المرتبطة به سواء كانت موجودة داخل البلاد او خارجه؟ وبالتالي يثار التساؤل حول تفتيش الانظمة المتصلة بالنظام المأذون تفتيشه إذا تواجدت في دوائر اختصاص مختلفة.

٤,٢,٢ المطلب الثاني: المشكلات المتعلقة بسلطات الاستدلال والتحقيق

هنالك العديد من المشكلات المتعلقة بسلطات لاستدلال والتحقيق سيتم تناولها في هذا المطلب على النحو التالي:

التحري في الجرائم المعلوماتية لابد أن يكون عمل امني متخصص [١٢٩] وهنا تكمن الصعوبة وتتعدد المعوقات، أهمها ما يرجع إلى شخصية المحقق مثل التهيب من استخدام الحاسب الآلي والتهيب من استخدام شبكة الإنترنت بالإضافة إلى عدم الإهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية والبعض الأخر يتعلق بالنواحي الفنية، كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم، ونقص المهارة في استخدام الحاسب الآلي والإنترنت، وعدم توفر المعرفة بأساليب ارتكاب جرائم الحاسب الآلي والإنترنت، وقلة الخبرة في مجال التحقيق في جرائم الحاسب الآلي والإنترنت والمعرفة باللغة الإنجليزية، سيما وأن للعاملين في مجال الحاسب الآلي مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم [١٣٠].

١٢٩. موسى، مصطفي محمد. ٢٠٢٠. *التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي*. ص. ٢٩٨.

١٣٠. الغافري، حسين بن سعيد. ٢٠٢٠. *السياسة الجنائية في مواجهة جرائم الانترنت*. ص. ٤٩١.

والمعلومة ان متطلبات العدالة الجنائية وإحقاق الحق تفرض على الأجهزة الحكومية بشكل عام والأجهزة المسئولة عن تتبع الجرائم وضبطها والتحقيق فيها بشكل خاص، وأن تتحمل مسؤولياتها نحو اكتشاف المجرمين وضبطهم ومحاكمتهم ومثل هذا الأمر يقتضي توفير الامكانات التقنية الأزمة سواء في عملية التحقيق او الكشف والاستدلال على الجرائم، لا سيما بعد ان تطورت ليس فقط أساليب الكشف عن الجرائم، إنما أيضا تطورت أساليب ارتكاب الجرائم وظهور أنماط جديدة من الجرائم ما كانت التشريعات لتعرفها من قبل إلا أن بعد أن ظهرت وسائل متطورة تمكن المجرمين إرتكاب جرائمهم بأساليب وطرق غير معهودة لرجال السلطة العامة، لذا وبما أن الجرائم المعلوماتية تتميز بخصائص فنية سواء بالنسبة لأشخاص مرتكبيها فنجد الإمكانات التقنية في التحقيق او الاستدلال عن هذه الجرائم سيكون اكثر حاجة فيها من غيرها من الجرائم[١٣١].

ويبنى على ذلك في توفير هذه الوسائل والإمكانيات، ما من شانه أن يؤدي إلى صعوبة في اكتشاف هذه الجرائم ان لم يكن عدم ضبطها لعدم اكتشافها اذن ما يزيد من صعوبة اكتشافها هو قلة خبرة سلطات التحقيق، بل والغالب انعدام تلك الخبرة لدي القائمين بالبحث عن الجرائم، إلى جانب انعدام أو قلة الوسائل والإمكانيات لدي تلك الجهات أن توفر الكادر الفني، سواء في البحث عن هذه الجرائم وضبطها او في التحقيق فيها أن تم ضبطها، لذلك هناك وفي سبيل تذليل هذه الصعوبة من يقترح ضرورة استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال للاستعانة به في تحقيق هذه الجرائم، وضرورة الاستعانة بالنخبة المتخصصة في الحاسب الآلي لضبط هذه الجرائم واكتشافها، وتقديم ادلة الإدانة فيها، وتولي شرح هذه الأدلة وأبعادها أمام المحاكم[١٣٢].

---

١٣١. موسى، مصطفي محمد. ٢٠٢٠. *التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي*. ص. ٣٠٢.

١٣٢. عياد، سامي علي. ٢٠٢٠. *الجريمة المعلوماتية وأجرام الانترنت*. ص. ٥٦.

قد يترتب على اختلاف الطبيعة القانونية للمال المعلوماتي اختلافا في النتائج المترتبة على تطبيق بعض نصوص القانون الجنائي التقليدي، ولذلك ظهرت هذه الخلافات الفقهية وتبعها في ذلك عدم استقرار الأحكام القضائية، فالإعتداء على برامج ومعلومات الحاسب الآلي يجعلنا أمام مشكلة قانونية ذات طبيعة خاصة، يتطلب فيه البحث في تطبيق الجزاء الجنائي الواجب في حالة الاعتداء على المال المعلوماتي المعنوي أي المحتوى الداخلي للشريط الممغنط أو الاسطوانة الممغنطة، ومن خلال تحديد الطبيعة القانونية للمال المعلوماتي المعتدى عليه، يمكن تحديد الطبيعة القانونية للجريمة الإلكترونية والوضع القانوني للبرامج والمعلومات، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت.

٤,٣ المبحث الثاني: المشكلات القانونية للتحقيق في الجرائم المعلوماتية

الجرائم الإلكترونية نمطا جديدا من الإجرام لم تكن موجودة في السابق وفي العديد من الحالات نجد ان القصور في التشريع العقابي، حيث هنالك نقص بين في التشريعات العقابية في هذا المجال حيث ترك المشرع في كثير من الأحيان أمر معالجتها للنصوص العقابية التقليدية والقواعد العامة الأمر الذي اوجد فراغا تشريعيا إتضح من خلاله قصور النصوص وعدم كفايتها لتغطية الإشكاليات المتنوعة للجرائم الإلكترونية، وأهم الإشكاليات القانونية التي تعترض مواجهة مثل هذا النوع من الجرائم تتمثل في الاختصاص القضائي بالتحقيق في دعاوي الجرائم المعلوماتية والمشكلات المتعلقة بالإجراءات الحديثة لجمع الأدلة

٤,٣,١ المطلب الأول: الاختصاص القضائي بالتحقيق في دعاوي الجرائم المعلوماتية

تبرز الإشكالية فيما يتعلق بموضوع تطبيق القانون الجنائي على الجرائم المعلوماتية في مدى أخذنا في الاعتبار موضوع العالم الافتراضي الذي خلقته التكنولوجيا ووضعته في خدمة الإنسان، وفيما إذا كان هذا العالم الافتراضي يشكل عالم أخر غير عالمنا تقع فيه الجريمة وتتكامل أثارها أم أنه جزء من عالمنا، وبالتالي ما يرتكب من جرائم عبره إنما يخضع لسلطان امتداد القانون الجنائي.

ولقد سارع المشرع المقارن ليفرض تحديثاً في تشريعه لكي يتناسب مع التطورات في هذا الإطار، وفي هذا المقام نجد أن المشرع الإماراتي أدرك وشعر بهذه المشكلة وعالجها من خلال إصدار قانون جرائم تقنية المعلومات الاتحادي الذي حدد الأفعال المجرمة في هذا الشأن وسد النقص الموجود، الأمر الذي فتح المجال أمام سلطات التحقيق وأجهزة العدالة الجنائية لمواجهة هذه الجرائم [١٣٣].

إن اختصاص القضاء بنظر الجرائم المعلوماتية والقانون الواجب التطبيق يشوبه نوع من الغموض وعدم الوضوح والدقة، أما حقيقة ان أغلبية هذه الجرائم ترتكب من قبل أشخاص خارج حدود الدولة او أنها تمر عبر أنظمة معلومات خارج الحدود الإقليمية، الأمر الذي يبرز أهمية ملائمة قواعد الاختصاص والقانون الواجب التطبيق، وما إذا كانت القواعد والنظريات التي تنظم هذه الجزئية صالحة للتطبيق في مجال الجرائم المعلوماتية.

أم أن الآمر يتطلب أفراد قواعد خاصة تتلاءم مع خصوصية هذا النوع من الجرائم وفي هذا الخصوص نصت المادة (٤٧) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٨ في شان مكافحة جرائم تقنية المعلومات 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 نظام

---

١٣٣. موسى، مصطفي محمد. ٢٠٢٠. *التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي*. ص. ٥٢٠.

معلوماتي الكتروني او شبكة معلوماتية او موقع الكتروني أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة أو إحدى الهيئات او المؤسسات العامة المملوكة لأي منهما.

٤,٣,٢ المطلب الثاني: المشكلات المتعلقة بالإجراءات الحديثة لجمع الأدلة

هنالك العديد المشكلات المتعلقة بالإجراءات الحديثة لجمع الأدلة في إطار التحقيق في الجرائم المعلوماتية تتمثل في الاتي:

إخفاء الجريمة وغياب الدليل المرئي، وافتقاد أكثر الآثار التقليدية وإعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية، كاستخدام كلمات السر حول مواقعهم تمنع الوصول اليها او ترميزها او تشفيرها لإعاقة المحاولات الرامية إلى الوصول اليها والاطلاع عليها او استنساخها، فالبحث والتحقيق ينصب على الكشف عن الجريمة وعن أدلتها التي تثبت صلة شخص ما بها صلة مادية ونفسية، صلة السبب بالمسبب، كما يتم البحث عن الادلة التي تنفي الصلة[١٣٤]، وهنا نجد أن من المعوقات المتعلقة بالجريمة المعلوماتية سهولة محو الدليل او تدميره في زمن قصير جدا، فالجاني يمكنه ان يمحي الادلة التي تكون قائمة ضده او تدميرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعت هذه السلطات اقامة الدليل ضده، وبالتالي تنصله بمسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي او الشبكة او في الأجهزة [١٣٥] كما يواجه التفتيش عقبات، فما هو إلا وسيلة للإثبات المادي، ذلك لأنه إجراء يستهدف ضبط اشياء مادية تتعلق بالجريمة او تفيد في كشف الحقيقة، وغايته دوما هي الحصول على الدليل المادي، وهذا ما

١٣٤. موسى، مصطفي محمد. ٢٠٢٠. *التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي*. ص. ٣٠٦.

١٣٥. عياد، سامي علي. ٢٠٢٠. *الجريمة المعلوماتية وأجرام الانترنت*. ص. ٧٥.

يتنافر مع الطبيعة غير المادية لبرامج وبينات الحاسب الآلية وكذا شبكة الشبكات، فهي مجرد برامج وبينات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي، وعلى ذلك فلا سبيل لان يرد عليها تفتيش أو ضبط، ومن الاجدر إخضاعها لأحكام مستقلة تتلاءم وطبيعتها الخاصة [١٣٦].

وطبيعة التكنولوجيا الرقمية قد عقدت من التحدي امام اعمال التفتيش والضبط، وذلك بسبب إمتداد الادلة المعلوماتية عبر شبكات الحاسوب في اماكن بعيدة عبر الموقع المادي للتفتيش[١٣٧]، وإن كان من الممكن الوصول اليها من خلال الحاسوب المأذون بتفتيشه، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر او حتى في بلد آخر، فهل يمتد تفتيش حاسوب معين إلى الاجهزة المرتبطة به سواء كانت موجودة داخل البلاد او خارجه؟ وبالتالي يثار التساؤل حول تفتيش الانظمة المتصلة بالنظام المأذون تفتيشه إذا تواجدت في دوائر اختصاص مختلفة.[١٣٨]

تثير الشكوى الخاصة في مجال تحريك الدعوى الجزائية في الجرائم الإلكترونية العديد من الإشكالات، وذلك كالآتي:

٤,٣,٢,١ الشكوى الخاصة وأثرها السلبي على التحقيق في الجرائم الإلكترونية

يعتبر تعليق تحريك الدعوى الجزائية في جرائم الشكوى على تقديم الشكوى الخاصة من المجني عليه أو ممثله القانوني واحداً من العوائق التي تتعرض سبيل التحقيق في الجرائم الإلكترونية، فهو وإن كان لا يمنع سلطات الاستدلال من اتخاذ اجراءات الاستدلال التي لا تمس شخص المتهم من مثل معاينة موقع الجريمة

---

١٣٦. هروال، نبيلة هبة. ٢٠١٣. *الجوانب الإجرائية لجرائم الانترنت*. ص. ٢٢٦.

١٣٧. مصطفى، عائشة بن قارة. ٢٠٠٦. *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن*. ص. ١٢٢.

[138] Curtis, G. (2011). The law of cybercrimes and their investigations. CRC Press.

وسماع الشهود، إلا أنه يمنع سلطات التحقيق من إتخاذ أية إجراءات تحقيق بصدد الجريمة الواقعة فيما إذا كانت ماسة بشخص المتهم إلا بعد تقديم الشكوى الخاصة [١٣٩].

وهذا يعني أنه في حال وقوع جريمة معلوماتية في صورة جريمة من جرائم الشكوى، مثل نشر الجاني لألفاظ بذيئة عن غيره عبر شبكة الإنترنت، فإنه لا يجوز اللجوء إلى التفتيش في مثل هذه الجرائم إلا بعد تقديم الشكوى الخاصة، بالرغم من أهميته وضرورة الإسراع في إجرائه، خصوصاً وأن أغلب آثار وأدلة هذه الجرائم، كما أسلفنا سابقاً هي من البيانات الإلكترونية القابلة للمحو والتعديل سواء عن قرب أو عن بعد، وبسهولة وسرعة فائقتين، وما يزيد الطين بلة هو أن المجني عليه الذي يختص هو وممثله القانوني بتقديم الشكوى الخاصة غالباً لا يكون بإمكانه ممارسة حقه هذا في مجال الجرائم الإلكترونية، بالنظر لصعوبة إمكانية اكتشافه لهذه الجرائم، فهو في الغالب يجعل وقوعه ضحية لجريمة معلوماتية، ومن ثم فلا يكون بمقدوره التعبير عن إرادته بخصوصها،[١٤٠] وهذا بدوره يؤدي إلى انتفاء العلة الرئيسية من تقرير هذا الحق التي تتمثل بمنح المجني عليه المجال للتفكير والتثبت من مدى تحقق مصلحته من عدمها في تقديم الشكوى بصدد الجريمة الواقعة عليه باعتباره هو الأدرى والأقدر من غيره في تقدير ذلك [١٤١].

كما وأن هذه الجرائم غالباً ما تقع عبر شبكة الإنترنت، مما يعني إمكانية وصول الجريمة إلى علم الملايين من مستخدمي هذه الشبكة، بالرغم من جهل المجني عليه نفسه بوقوعها، وهذا بدوره يؤدي إلى انتفاء علة رئيسة أخرى لتقرير هذا الحق، ألا وهي عدم فضح علاقات وأسرار كانت تنبغي أن تبقى مستورة [١٤٢].

---

١٣٩. عمر، رشاد خالد. ٢٠١٨م. *المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية*. ص. ٨١.

[140] Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. Journal of Scandinavian Studies in Criminology and Crime Prevention, 18(2), 157-175.

١٤١. الفقي، أحمد عبد اللطيف. ٢٠٠٣. *النيابة العامة وحقوق ضحايا الجريمة*. القاهرة: دار الفجر. ص. ٢٢-٢٣.

١٤٢. عبد الله، سعيد حسب الله. ٢٠١٧. *شرح قانون اصول محاكمات الجزائية*. لندن: نور للنشر. ص. ٥٣.

ومعالجة هذه المشكلة تكمن في ضرورة إنشاء جهاز متخصص بمكافحة الجرائم الإلكترونية، بحيث يكون اكتشاف الجرائم الإلكترونية عموماً واحدة من مهامه حتى ولو كانت الجريمة من جرائم الشكوى، على أن يقوم الجهاز في الحالة الأخيرة بإخطار المجني عليه بالجريمة الواقعة عليه (فيما إذا كان شخصاً معلوماً أو كان من الممكن معرفته من خلال معالم الجريمة) ليمارس حقه في تحريك الدعوى الجزائية من عدمه بصدد الجريمة الواقعة عليه، فهذه المعالجة تساعد من جهة المجني عليه في العلم بالجريمة الواقعة عليه وممارسة حقه في تقديم الشكوى الخاصة بصددها من عدمه، وهي من جهة أخرى تساعد في تحريك الدعوى الجزائية بأكبر قدر ممكن من السرعة وبالتالي تزيد من إمكانية إجراء التفتيش وغيرها من الإجراءات الماسة بشخص المتهم بالسرعة اللازمة لمواجهة هذه الجرائم[١٤٣].

٤,٣,٢,٢ مدى جواز تقديم الشكوى الخاصة بصورة إلكترونية

بالرجوع إلى قانون الإجراءات الجزائية، نلاحظ ان المشرع الإماراتي لم يشترط تقديم الشكوى الخاصة بصورة أو بشكل محدد بالذات، وإنما أشترط فقط تقديمها من المجني عليه أو من يمثله قانوناً، مما يعني جواز تقديمها بصورة تحريرية أو شفوية شأنها في ذلك شأن الشكوى العامة أو الإخبار، وهذا يعني أيضاً إمكانية تقديمها بصورة إلكترونية، مادام أن المشرع لم يحدد أية صورة لتقديمها.[١٤٤]

ولكن إذا كان تقديم الشكوى الخاصة بصورة إلكترونية جائزاً بمقتضى النصوص القانونية يرى الباحث عدم تأييد هذه الإجازة، ذلك لأن المشرع عندما خص المجني عليه أو ممثله القانوني بتقديم هذه الشكوى دون غيرهما، فإنه أوجب بالتالي ضرورة التثبت من شخصية المتقدم بالشكوى الخاصة لمعرفة ما إذا كان هو

---

١٤٣. عمر، رشاد خالد. ٢٠١٨م. *المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية*. ص. ٨٤.

[144] Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1), 1-22.

المجني عليه أو ممثله القانوني قبل قبول شكواه، لأنه وبمجرد قبول الشكوى ستحرك الدعوى الجزائية مباشرة وسيكون بالإمكان إتخاذ إجراءات ماسة بشخص المتهم وحريته.

ويرى الباحث من الصعوبة بمكان التثبت من هوية وشخصية المتقدم بالشكوى الخاصة بصورة إلكترونية، فإننا نرى وعلى فرض وجود مسبق لجهة مختصة بقبول مثل هذه الشكاوى، بضرورة قبول تلك الشكاوى إبتداءً على أنها مجرد إخبار عن الجريمة الإلكترونية الواقعة، ومن ثم فإذا تقدم المشتكي شخصياً أو من يمثله قانوناً فيما بعد لتقديم شكواه بصورة تحريرية أو شفوية فعندها وبعد التثبت من شخصيته يمكن اعتبار الشكوى المقدمة من عنده على أنها شكوى خاصة، وهذا الأمر له أهمية قصوى من حيث إنه يمنع من إتخاذ الإجراءات الماسة بشخص المتهم قبل التثبت من شخصية مقدم الشكوى الخاصة، كما انه يمكن سلطات الاستدلال من إتخاذ الإجراءات التي تكفل الكشف عن الجريمة.

٤,٤ ملخص الفصل الرابع

استعرض الفصل الرابع اشكاليات التحقيق في الجرائم المعلوماتية، حيث استعرض الفصل المشكلات الفنية المتعلقة بالتحقيق في الجرائم المعلوماتية، وكذلك استعرض الفصل الرابع المشكلات القانونية المتعلقة بالجرائم المعلوماتية، كما تطرق الفصل الرابع إلى المشكلات الحديثة التي تتعلق بإجراءات التحقيق في الجرائم المعلوماتية.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA