مجلة العلوم الاقتصادية والإدارية والقانونية
العدد الثالث عشر ــ المجلد الثاني
أكتوبر 2018م
ISSN: 2522- 3372

المجلة العربية للعلوم و نشر الأبحاث
Arab Journal of Sciences & Research Publishing
AJSRP

إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقًا للتشريع الإماراتي

سعيد سالم المزروعي عزمان عبد الرحمن
جامعة العلوم الإسلامية الماليزية

الملخص: هدفت هذه الدراسة إلى استقصاء إجراءات التحقيق في جرائم تقنية المعلومات وفقًا للتشريع الإماراتي، وذلك من خلال استعراض إجراءات رجال الشرطة (مأموري الضبط القضائي) خلال مرحلة جمع الاستدلالات وإجراءات التحقيق الابتدائي التي تجريها النيابة العامة لمكافحة جرائم تقنية المعلومات، وقد تمثلت مشكلة الدراسة في إبراز المشاكل القانونية والفنية والتحديات التي تواجه التحقيق في مثل هذه الجرائم، وبيان مدى ملاءمة وسائل التحقيق الجنائي التقليدية في مجال جرائم تقنية المعلومات، وقد اعتمدت الدراسة على منهج الوصف التحليلي للنصوص القوانين ذات العلاقة والأحكام القضائية الصادر عن المحاكم العليا في دولة الإمارات العربية المتحدة، وانتهت الدراسة إلى مجموعة من النتائج أبرزها أن جرائم تقنية المعلومات تتطلب من مأموري الضبط القضائي أن يكونوا على قدر معقول من الثقافة في مجال نظم تقنية المعلومات؛ ليتمكنوا من مباشرة إجراءات جمع الاستدلالات، وأن قانون الإجراءات الجزائية الإماراتي لم يتطرق إلى قواعد الضبط في جرائم تقنية المعلومات مكتفي بالقواعد العامة للضبط في الجرائم، كما توصلت الدراسة إلى مجموعة من التوصيات أهمها؛ ضرورة إخضاع جهات التحقيق المسؤولة عن مكافحة جرائم المعلومات لتدريب متخصص يمكنهم من فهم مضامين البلاغات المرتبطة في جرائم تقنية المعلومات واستيعاب معطيات مسرح الجريمة، والتعامل مع الأدلة المتحصلة من الوسائل الإلكترونية.

الكلمات المفتاحية: جرائم تقنية المعلومات، المجرم الإلكتروني، الأدلة الرقمية، الأمن الإلكتروني.

المقدمة:

بالرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة، وفي شتّى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة، والانحراف عن الأغراض المتوخاة منها، تبدّت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي ظاهرة جرائم تقنية المعلومات أو ما يسمى الجرائم الإلكترونية، ليس هذا فحسب، بل سهّلت هذه التقنية ارتكاب بعض الجرائم التقليدية.

ولم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك من يُطلق عليها تسمية جرائم المعلوماتية، في حين يذهب أخرون إلى تسميتها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، ويسميها أخرون جرائم الكومبيوتر والأنترنت، وهناك من يطلق عليها الجرائم المستحدثة. وعرفت الجرائم الإلكترونية على أنها " سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات ونقل البيانات، أو هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة، وإساءة استخدام المخرجات إضافة إلى أفعال أخري تشكل جرائم أكثر تعقيدًا من الناحية التقنية مثل تعديل الكمبيوتر"[1]

ومن المؤكد أن إجراءات التحقيق الجنائي في جرائم تقنية المعلومات؛ لا يختلف عن إجراءات التحقيق في الجرائم التقليدية، بل هناك تشابه كبير بينهما، فالتحقيق في كليهما يحتاج إلى إجراءات تتشابه في عمومها من حيث

(1) أحد التعريفات التي وضعها مكتب المحاسبة العامة في الولايات المتحدة الأمريكية GOA:
www.goa.com

المعاينة والتفتيش والتحريات والاستجواب، بالإضافة إلى جمع الأدلة، كما أن التعامل مع مسرح الجريمة بشقيه الإلكتروني والتقليدي يتطلب الحرص الشديد، كما يتطلب مجموعة من الإجراءات التي تهدف بالأساس إلى حماية الدليل الموجود على مسرح الجريمة، والعمل على إبراز قيمته الاستدلالية.

ومن هذا المنطلق تم اختيار الموضوع لتسليط الضوء على إجراءات التحقيق الجنائي في تقنية المعلومات، وإبراز المشاكل القانونية الجديدة التي أفرزها ظهور المعلوماتية وتطبيقاتها المتعددة في نطاق القانون الجنائي الإماراتي، وكيفية التحقيق الجنائي في جرائم تقنية المعلومات، والتغلب على كافة الصعوبات التي تواجه مثل هذا التحقيق.

مشكلة البحث

تبرز إشكالية البحث في وجود مشاكل قانونية ومعيقات تواجه إجراءات التحقيق في جرائم تقنية المعلومات، وغموض في بيان مدى ملاءمة وسائل التحقيق الجنائي التقليدية في مواجهتها، حيث فرضت جرائم تقنية المعلومات على جهات مرحلة الاستدلالات والتحقيق الابتدائي تحديات كبيرة لم يسبق لها مثيل، بسبب ما تتميز به هذه الجرائم من السهولة والسرعة الفائقة في تنفيذ الجريمة، وانعدام الآثار المادية للجريمة، وغياب الدليل المادي، وصعوبة الوصول إلى الدليل بالوسائل الفنية التقليدية، وكذلك سهولة اتلاف الدليل المادي وتدميره في زمن قياسي، فضلًا عن صعوبة اكتشافها وإثباتها؛ نظرًا للحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها، وهذا يؤدي بدوره إلى تزايد الصعوبات التي تعترض رجال العدالة الجنائية والشرطة في كشف غموضها وفي إجراء التفتيش ومعاينة مسرح الجريمة الإلكتروني والضبط والتحقيق؛ لأن هذه النوعية من الجرائم تعتمد على قمة الذكاء والمهارة في ارتكابها. وعليه تبرز إشكالية البحث في بيان الإجراءات الجزائية المقرر لمواجهة جرائم تقنية المعلومات خلال مرحلة جمع الاستدلالات والتحقيق الابتدائي.

أسئلة البحث:

1- كيف يتم تلقي البلاغ وإجراء البحث والتحري في جرائم تقنية المعلومات؟
2- ما هو المقصود في الانتقال والمعاينة في جرائم تقنية المعلومات؟
3- ما المقصود بالتفتيش في جرائم تقنية المعلومات؟
4- كيف يتم ضبط الأشياء في جرائم تقنية المعلومات؟
5- كيف يتم ندب الخبراء والاستجواب في جرائم تقنية المعلومات؟

أهداف البحث:

1- بيان كيفية تلقي البلاغ في جرائم تقنية المعلومات وإجراء التحريات بشأنها.
2- الوقوف على آلية الانتقال والمعاينة في جرائم تقنية المعلومات.
3- بيان المقصود بالتفتيش في جرائم تقنية المعلومات وبيان إجراءاته.
4- بيان كيفية ضبط الأشياء في جرائم تقنية المعلومات.
5- بيان أهمية ندب الخبراء في جرائم تقنية المعلومات وكيفية الاستجواب.

أهمية البحث:

تبرز أهمية البحث من خلال المحاور الآتية:

- **الأهمية النظرية:** تنبع أهمية البحث النظرية في اكتسابه بعدًا شرطيًّا؛ لكونه وثيقَ الصلة بجهاز الشرطة الذي يعد أول الأجهزة المكلفة بمكافحة جرائم تقنية المعلومات في جميع صورها وأشكالها، إضافة إلى أنه المسؤول عن حفظ الأمن والنظام في دولة الإمارات، وتحقيق الأمان لأفراد المجتمع بها، حيث أن موضوع جرائم تقنية المعلومات والتحقيق الجنائي فيها يعد من الموضوعات الأمنية التي باتت الحاجة إلى دراستها دراسة متأنية من قبل الباحثين ودارسي القانون، وباتت من الأمور الضرورية الملحة في الوقت الراهن، وهذا ما دفع الباحث إلى إجراء هذه الدراسة في هذا المجال الخصب.
- **الأهمية العملية:** وتبرز أهمية البحث العملية كونه يتناول الجانب الإجرائي لمكافحة جرائم تقنية المعلومات، ويسلط الضوء على وسائل التحقيق خلال مرحلة جمع الاستدلالات المنوطة بمأموري الضبط القضائي، ومرحلة التحقيق الابتدائي المنوطة بالنيابة العامة.

منهج البحث:

استخدمت الباحث المنهج الوصفي التحليلي، لتوصيف الإجراءات الجزائية المقرر لمواجهة جرائم تقنية المعلومات خلال مرحلة جمع الاستدلالات والتحقيق الابتدائي، من خلال دراسة وتحليل التشريعات النافذة في دولة الإمارات العربية المتحدة ذات العلاقة، والاطلاع على الأحكام القضائية في مجال الإجراءات الجزائية المتعلقة بجرائم تقنية المعلومات، والاستعانة بالكتب والمراجع العامة والمتخصصة والرسائل الجامعية والأبحاث المنشورة في المجلات والدوريات المحكمة المتاحة والمتعلقة بمكافحة جرائم تقنية المعلومات.

حدود البحث:

- **الحدود الموضوعية:** يتناول البحث الإطار القانوني لإجراءات التحقيق في جرائم تقنية المعلومات في ضوء التشريع الإماراتي متمثلاً بقانون الإجراءات الجزائية الاتحادي رقم (35) لسنة 1992م وتعديلاته، والمرسوم بقانون اتحادي لدولة الإمارات العربية المتحدة رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات والقانون العقوبات الاتحادي رقم (3) لسنة 1987م، والأحكام القضائية الصادرة عن المحاكم العليا في دولة الإمارات.
- **الحدود المكانية:** سوف يتم تناول الموضوع في حدود دولة الإمارات العربية والمتحدة.
- **الحدود الزمانية:** سيقوم الباحث بدراسة الموضوع في إطار زمني يتوافق مع صدور التشريعات محل الدراسة.

الخطة وهيكل البحث

المبحث الأول: إجراءات التحقيق خلال مرحلة جمع الاستدلالات في جرائم تقنية المعلومات.

المطلب الأول: البلاغ والبحث والتحري في جرائم تقنية المعلومات.

المطلب الثاني: الانتقال والمعاينة في جرائم تقنية المعلومات.

المبحث الثاني: إجراءات التحقيق الابتدائي في جرائم تقنية المعلومات.

المطلب الأول: التفتيش في جرائم تقنية المعلومات وجمع الأدلة وضبطها.

المطلب الثاني: ندب الخبراء والاستجواب في جرائم تقنية المعلومات.

المبحث الأول: إجراءات التحقيق خلال مرحلة جمع الاستدلالات في جرائم تقنية المعلومات

يعرف الاستدلال على أنه مجموعة من الإجراءات التمهيدية السابقة على تحريك الدعوى الجنائية، والتي تهدف إلى جمع المعلومات في شأن جريمة ارتكبت، وإثبات الآثار التي نتجت عنها، حتى تتخذ سلطات التحقيق بناء عليها القرار بشأن تحريك الدعوى الجنائية عنها [2].

وتعد الاستدلالات مرحلة ممهدة للدعوى الجزائية، بالإضافة إلى اتصالها المباشر والوثيق بحرية الفرد وحقه في الحياة في أمان بعيدًا عن أي اعتداءات من السلطات، كما تعد هذه المرحلة من أهم إجراءات العدالة الجنائية، وأكثرها حساسية باعتبارها بداية الطريق إلى ساحة العدالة الجنائية وكفالة الحقوق، والسبيل إلى مواجهة الجرائم منعًا وكشفًا، كما أنها تعد- بحق- معيارًا لقياس كفاءة الأجهزة الشرطية والأمنية وقدرتها على تحقيق الأمن بمنع وقوع الجرائم والحد منها، والكشف عنها، وضبط مرتكبيها عند وقوعها، وتقديمهم للمحاكمة العادلة، [3]. وعليه يمكن بيان إجراءات جمع الاستدلالات لمواجهة جرائم تقنية المعلومات من خلال تقسيم المبحث إلى مطلبين، **المطلب الأول:** البلاغ والبحث والتحري في جرائم تقنية المعلومات، **والمطلب الثاني:** الانتقال والمعاينة في جرائم تقنية المعلومات.

المطلب الأول: البلاغ والبحث والتحري في جرائم تقنية المعلومات

يجب على مأمور الضبط القضائي تلقي البلاغات التي ترد إليه بشأن الجرائم، كما يجب عليه قبول الشكاوى التي ترد إليه بشأن الجرائم التي تطلب فيها المشرع تقديم شكوى من المجني عليه، وأن يثبتها في محضر الاستدلال، ثم يرسلها إلى النيابة العامة، وكذلك إجراء التحريات اللازمة لجمع كافة القرائن والأدلة التي تفيد في التوصل إلى الحقيقة إثباتًا أو نفيًا لوقوع الجريمة ونسبتها إلى فاعلها [4]، وعليه سنتناول في هذا المطلب تلقي البلاغات والشكاوى وإجراءات البحث والتحري في جرائم تقنية المعلومات على النحو الآتي:

الفرع الأول: تلقي البلاغات والشكاوى في جرائم تقنية المعلومات

يقصد بالبلاغ إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع، أو أن هناك اتفاقًا جنائيًا أو أدلة أو قرائن أو عزمًا على ارتكابها، أو وجود شك أو خوف من أنها أُرتكبت [5]، ويعرف بأنه" إبلاغ السلطات المختصة بوقوع جريمة ينص عليها القانون الجنائي"[6].

وفي ذلك نصت المادة (35) من قانون الإجراءات الجزائية الاتحادي الإماراتي رقم (35) لسنة 1992م [7] على أنه "يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم في شأن الجرائم، ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على الإيضاحات وإجراء المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلمون بها بأية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة"، كما

---

(2) سالم، نبيل مدحت (2009)، شرح قانون الاجراءات الجنائية، الجزء الثاني، دار النهضة العربية، القاهرة، مصر، ص 733.

(3) محمد، نصر محمد (2012)، التحقيق الجنائي بين الواقع والقانون، دراسة تطبيقية على أنواع البصمات وحجيتها، الفكر الشرطي، مركز بحوث شرطة الشارقة، القيادة العامة لشرطة الشارقة، الشارقة، المجلد (21) العدد (83)، شهر أكتوبر، ص113- 114.

(4) سرور، أحمد فتحي (2012)، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ص552.

(5) هروال، نبيلة هبة (2013)، الجوانب الإجرائية لجرائم الإنترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ص177.

(6) عمر، راشد خالد (2013)، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، ص85.

(7) منشور في الجريدة الرسمية، دولة الإمارات العربية المتحدة، العدد مائتان وتسعة وثلاثون، 29 يونيو 1992م.

نصت المادة (37) من القانون ذاته على أن "على كل من علم بوقوع جريمة مما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي عنها". كما تناولت المادة (38) من القانون ذاته على أنه "يجب على كل من علم من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأدية عمله أو بسبب تأديته بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ عنها فورًا النيابة العامة أو أقرب مأموري الضبط القضائي".

فقد نصت هذه المواد على ضرورة الإبلاغ عن الجرائم للسلطات العامة المختصة، سواء من أفراد المجتمع أم من الموظف العام والمكلف بخدمة عامة، وهذا يقتضي توافر العلم بالجريمة أولاً من المبلغ، ولا يشترط لذلك علم تام بالجريمة وظروفها ووقائعها، بل يكفي بأن يكون هناك جريمة ما تم ارتكابها، ثم يتدرج بعد ذلك مستوى العلم، وكلما أحاط المبلغ بمعلومات وتفصيلات عن الجريمة كان أفضل، وترتب عليه واجب ملزم بالإفصاح عنها دون أن يكتم شيئًا [8].

ولقد رتب المشرع الإماراتي المساءلة الجزائية عن كل من يمتنع على الإبلاغ عن الجرائم، فأفرد الفصل الرابع من الباب الثالث من قانون العقوبات الاتحادي رقم (3) لسنة 1987م[9]. لهذا الغرض، فقد جاء في المادة (272) منه على أن "يعاقب بالحبس أو بالغرامة كل موظف عام مكلف بالبحث عن الجرائم أو ضبطها أهمل أو أرجأ الإخبار عن جريمة اتصلت بعلمه".

ومن هذا المنطلق؛ فبمجرد تلقي مأمور الضبط القضائي أو جهة التحقيق المختصة بلاغًا يشير إلى ممارسة شخص أنشطة تندرج ضمن جرائم تقنية المعلومات في مكان أو أجهزة محددة، ووفق لغات برمجية معلومة؛ كتلقيه مثلًا بلاغًا فيه معلومات عن نشر فيروسات تخريبية عبر الشبكة الإلكترونية، فإنه حينئذ يبدأ في اتخاذ اختصاصاته.

وفي الأحوال جميعها؛ فإن أي بلاغ عن جريمة؛ سواء كان فاعلها مجهولاً أم معلومًا وتندرج تحت جرائم تقنية المعلومات؛ ينبغي أن يتضمن العناصر الآتية [10]:

1. **تحديد مكان وقوع الجريمة**: على المبلغ تحديد المكان الذي وقعت فيه الأفعال غير المشروعة، ووصفها بما يسمح بالدلالة عليها كوصف موقع الشركة أو عنوانها أو البنك أو المنزل الذي تعرض للاعتداء.
2. **تحديد نوع الجريمة:** لا يكفي أن يقوم المبلغ بتحديد مكان وقوع الجريمة؛ بل ينبغي عليه أن يبين نوع الجريمة المرتكبة؛ ما إذا كانت اعتداءً على مال أم تزوير بطاقة ائتمانية أو جرائم اختراق وتعطيل وإعاقة المواقع والاعتداء على البيانات والمعلومات الإلكترونية.
3. **تحديد محل الجريمة:** يجب على المبلغ أن يحدد لرجال الضبط القضائي المختصين الجهاز الذي وقعت عليه الجريمة، والموقع الذي استهدفه الاعتداء.

وعليه؛ تعد هذه العناصر مهمة وضرورة لمساعدة رجال الضبط القضائي في أي بلاغ متعلق بجرائم تقنية المعلومات، بحيث تمكنهم من تحديد معالم الجريمة، ووضع خطة للتعامل معها من الناحيتين الفنية والقانونية.

والبلاغ هنا قد يتم عن طريق الإنترنت أي ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق والتحري لإبلاغها عن وجود صفحات أو مواقعَ غير

---

(8) شحاته، محمد أحمد (2013)، شرح قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة، المكتب الجامعي الحديث، الإسكندرية، ص99- 100.

(9) منشور بالجريدة الرسمية، دولة الإمارات العربية المتحدة، العدد مائة واثنان وثمانون، 20 ديسمبر 1987م.

(10) إبراهيم، راشد بشير (2008)، التحقيق الجنائي في جرائم تقنية المعلومات، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة الأولى، العدد 131، أبو ظبي، ص48- 49.

مشروعة تمارس جرائم تقنية المعلومات إلى موقع القيادة العامة لشرطة دبي فرع إدارة مباحث الجرائم الإلكترونية بالإدارة العامة للتحريات والمباحث الجنائية في شرطة دبي [11]، أو موقع القيادة العامة لشرطة أبوظبي فرع الجريمة الإلكترونية بإدارة التحريات والمباحث الجنائية في شرطة أبو ظبي[12].

والمبلغ في جرائم تقنية المعلومات لابد وأن تكون لديه معرفة مقبولة بالجوانب الفنية للحاسوب الإلكتروني والشبكة الإلكترونية حتى يتمكن من تقديم معلوماتٍ تصف الحادث بشكل جيدٍ، ويمكن مأمور الضبط القضائي أو المحقق من الوقوف على طبيعة الجريمة وبشكل مقبول حتى يمكنه من مباشرة التحقيق فيها. وبالتالي يفترض أن يكون لدى من يتلقى البلاغ المعرفة الكافية بالجوانب الفنية للحاسوب الإلكتروني والشبكة الإلكترونية حتى يستطيع مناقشة المبلغ في الكثير من الجوانب المتعلقة بالجريمة محل البلاغ [13].

الفرع الثاني: البحث والتحري وكشف غموض جرائم تقنية المعلومات

يقصد بعملية التحري عبر الشبكة الإلكترونية: هو عمل أمني يقوم به رجل التحريات عبر شبكة الإنترنت بواسطة التكنولوجيا الإلكترونية الرقمية لتحقيق غرض محدد، وتخزين النتيجة في ملف رقمي أو إفراغها في وثيقة تفيد في إثبات حصول جريمة إلكترونية [14]، وإسنادها إلى شخص بعينه وهي أحد عناصر الإثبات الجنائي[15].

وحددت المادة (30) من قانون الإجراءات الجزائية الاتحادي الإماراتي اختصاصات مأموري الضبط القضائي في البحث والتحري حيث تنص على أن: "يقوم مأمورو الضبط القضائي بتقصي الجرائم والبحث عن مرتكبيها وجمع المعلومات والأدلة اللازمة للتحقيق والاتهام".

وعلى هذا الأساس؛ فإن التحري عبر الشبكة المعلوماتية [16] يعد عملًا أمنيًّا وقانونيًّا يقوم به رجل البحث الجنائي المختص عبر الشبكة بواسطة وسيلة تقنية المعلومات[17] للحصول على بيانات ومعلومات تعريفية أو

---

(11) القيادة العامة لشرطة دبي، التبليغ عن جريمة، وزارة الداخلية، دولة الإمارات العربية المتحدة:
http://www.dubaipolice.gov.ae/dp/jsps/content/flat_content.do?contentCode=88355

(12) القيادة العامة لشرطة أبو ظبي، نظام الشكاوى والآراء، وزارة الداخلية، دولة الإمارات العربية المتحدة:
https://www.fms.ae/

(13) الفيل، على عدنان (2012)، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ص11.

(14) موسى، مصطفى محمد (2005) دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، المحلة الكبرى، ص22.

(15) المليح، عبد الله محمد (2009) مدخل الإجراءات الشرطية في البلاغات الأمنية في دولة الإمارات العربية المتحدة، مركز بحوث الشرطة، شرطة الشارقة، الشارقة، ص91.

(16) عرفت المادة رقم (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات **الشبكة المعلوماتية** على انها "أي أداة الكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين".

(17) عرفت المادة رقم (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات **وسيلة تقنية المعلومات** على أنها "أي أداة الكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين".

توضيحية عن الأشخاص أو الأماكن أو الأشياء للحد من جرائم تقنية المعلومات، أو ضبطها؛ لتحقيق الأمن الإلكتروني، أو لأي غرض آخر [18].

ولمأمور الضبط القضائي – رجل البحث الجنائي- في هذا سلطة تقديرية واسعة في اختيار وسائل إجراءات التحري التي يراها مناسبة ولازمة لإتمام عمله بصورة إيجابية في جمع المعلومات التي سيستفيد منها لضبط الجرائم الإلكترونية أو الحد منها، وله في ذلك مصادر عدة، وأبرز ما يعنينا منها في موضوع دراستنا هو الإرشاد الجنائي والمراقبة الإلكترونية، ويمكن بيان ذلك على النحو الآتي:

1- الإرشاد الجنائي عبر الشبكة الإلكترونية:

يعد الإرشاد الجنائي عبر الشبكة الإلكترونية ضروريًّا ومهمًّا لرجل الضبط القضائي حيث يعتمد عليه في تحرياته وجمع المعلومات، وهو يلعب دورًا كبيرًا في التقصي والكشف عن جرائم تقنية المعلومات؛ إذ نجد العديد من المؤسسات الضبطية حول العالم تقوم باستخدامه، وذلك عن طريق تجنيد مصادرها أو الغير للدخول إلى العالم الافتراضي، وذلك بقصد البحث عن الجرائم الإلكترونية ومرتكبيها ثم تقديمهم إلى المحاكمة، ويمكن أن يقوم مأمور الضبط القضائي بالبحث والتحري بنفسه في العالم الافتراضي من خلال الحصول على إذن رسمي لمباشرة مهامه في البحث والتحري عن جرائم تقنية المعلومات ومرتكبيها، ويجب أن يتضمن ذلك الأخير رقم الحاسوب وصلاحيته للعمل، وخلوه من العوائق التكنولوجية واحتواءه على برمجيات أصلية وليست منسوخة، فضلاً عن ذكر أرقامها المسلسلة ورقم الترخيص بها وتاريخه وجهة إصدارها، ثم يجلس – بعد ذلك- أمام حاسوب متصل بالشبكة الإلكترونية؛ للقيام بعمله في البحث والتحري، وذلك بالدخول في نقاشات مع الغير باستخدام أسماء مستعارة لأشخاص أو لهيئات مختلفة عبر قاعات الدردشة وحلقات النقاش [19].

وبمجرد الحصول على المعلومة التي تفيد مأمور الضبط القضائي في ارتكاب المشروع الإجرامي من قبل المجرم الإلكتروني؛ كسؤال الهاكر مثلًا عن كيفية اختراق المواقع أو النظام المعلوماتي عن طريق الشبكة الإلكترونية، والتحقق من دخوله موقع إلكتروني أو نظام معلومات الكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة، يقوم باستدراجه حتى يتم التعرف عليه، وبالتالي إلقاء القبض عليه.

ومن أمثلة ذلك متابعة إدارة المباحث الإلكترونية بشرطة دبي إحدى القضايا الخاصة بتسريب امتحانات تابعة لإحدى المدارس في إمارة دبي؛ فقد تم- بعد البحث والتحري- تحديد الطالب المخترق المسؤول عن عملية تسريب الامتحانات، ومن خلال التحقيق معه فقد اعترف المتهم بالتهم المنسوبة إليه، وقدم شرحًا عن كيفية قيامه بالعملية عن طريق اختراق الشبكة الإلكترونية الخاصة بالمدرسة، ثم زرع ملفات تجسس في جهاز الحاسوب الآلي الخاص بالمعلمة، ثم سحب الامتحانات الموجودة في جهازها. وقد أثبت تقرير المختبر الجنائي الواقعة التي تم تحويلها إلى مركز شرطة "بر دبي" لاتخاذ اللازم [20].

---

(18) موسى، مصطفى محمد، دليل التحري عبر شبكة الإنترنت، مرجع سابق، ص22.

(19) هروال، نبيلة هبة، مرجع سابق، ص195- 196.

(20) ولد راحة، الراشد سالم عبيد سالمين (2010)، عرض التجارب والخبرات الأمنية المختلفة في التعامل مع جرائم تقنية المعلومات والاتصالات الخاصة بالأطفال، الطبعة الأولى، مركز بحوث الشرطة، أكاديمية شرطة دبي، دبي، ص69.

2- المراقبة الإلكترونية للشبكة عبر الإنترنت:

يقصد بالمراقبة الإلكترونية: العمل الذي يقوم به المراقب- باستخدام التقنية الإلكترونية- لجمع بيانات ومعلومات عن المشتبه فيه سواء أكان شخصًا أم مكانًا، أم شيئًا حسب طبيعته مرتبطًا بالزمن والتاريخ والوقت لتحقيق غرض أمني أو لأي غرض آخر [21].

وتعتبر المراقبة الإلكترونية من أهم مصادر البحث والتحري التي تتم باستخدام تقنية المعلومات، لجمع البيانات عن المشتبه فيهم في جرائم تقنية المعلومات، ومع ذلك فإن المراقبة تعد من الإجراءات التي تعتدي على حق الخصوصية (كمراقبة البريد الإلكتروني الخاص بالمشتبه فيهم) التي كفلها الدستور والقانون بالحماية، ومن ثم فهي تتطلب- قبل البدء بها – حصول مأمور الضبط القضائي على الإذن بها من السلطات القضائية المختصة [22].

ومن هذا المنطلق؛ فإن المراقبة الإلكترونية هي وسيلة من وسائل جمع البيانات والمعلومات عن جرائم تقنية المعلومات، ويقوم بها مراقبٌ إلكترونيٌّ يتمثل في مأمور الضبط القضائي الذي يتمتع بكفاءٍ تقنية عالية تتماشى مع نوعية جرائم تقنية المعلومات التي يتعامل معها، مستخدمًا في ذلك التقنية الإلكترونية وعبر الشبكة الإلكترونية؛ كأن يراقب أحد الهكرة ممن قام باختراق الحاسوب الآلي الخاص بالمجني عليه وبريده الإلكتروني، أو اختراقه للمواقع.

ويسمح القانون الاتحادي لدولة الإمارات العربية المتحدة رقم (3) لسنة 2003م في شأن تنظيم قطاع الاتصالات في المادة (75) من القانون بأنه: "يجوز للمرخص له بعد الحصول على إذن مسبق من الهيئة أن يضع تحت المراقبة أي جهاز أو خلافه إذا توافرت لديه أسباب معقولة للاعتقاد بأنه يستغل في أي مخالفة منصوص عليها في المادة 72 من هذا القانون".

فعندما يقوم الموظفون لدى مقدمي خدمة الاتصال بمراقبة الاتصالات لحماية حقوق مزودي الخدمة فيكتشفون الاختراقات التي ترتكب من المجرم الإلكتروني، ويكشفونها للسلطة؛ فلا يوجد حينئذ انتهاك للقانون؛ فمزودو الخدمة الذين يحققون في الاستخدامات غير المشروعة لنظم المعلومات لديهم سلطة موسعة للمراقبة، ولديهم الحق في الكشف عن دليل الاستخدام غير المشروع [23].

وعلى هذا الأساس؛ فإن ما يثير الإشكالية هنا هو أن القيام بالمراقبة السرية الإلكترونية في جرائم تقنية المعلومات التي تحدث عبر الشبكة الإلكترونية ووسائلها ليس بالأمر السهل؛ إذ ينبغي أن تتوافر لدى جهات الضبط القضائي القائمة بها المؤهلات العلمية والتقنية اللازمة لأداء هذه المهمة على أحسن وجه، وذلك لا يمكن إنجازه إلا من خلال إسناد مثل هذه المهمة بجهات ضبط قضائي خاصة مؤسسة ومعدة خصيصًا لهذا الغرض ضمن جهاز شرطي مختص بمكافحة جرائم تقنية المعلومات والتحري عنها، كما أن أفراد هذه الجهات لا بد أن يكونوا على إلمام ودراية بالبيانات الإلكترونية التي ترتبط بمفهوم الحياة الخاصة للأفراد التي لا تجوز مراقبتها إلا بإذن قضائي، وتحقيق مثل هذا الإلمام بدوره يقتضي- من جهة- تنظيم المشرع لإجراءات المراقبة التي تعد من الإجراءات

(21) موسى، مصطفى محمد (2003)، المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، القاهرة، ص192.

(22) موسى، مصطفى محمد، مرجع سابق، ص192.

(23) الحمودي، محمد علي (2009)، دور مأمور الضبط القضائي في مواجهة جرائم المعلومات، الطبعة الأولى، الناشر المؤلف، بلد النشر (بدون)، ص145- 155.

التحقيقية، كما يقتضي- من جهة أخرى- إمداد أفراد تلك الجهات بالثقافة القانونية اللازمة لهذا الغرض عبر تنظيم دورات خاصة لهم[24]. وفي سبيل تحديد شخصية المجرم الإلكتروني ورصد تحركاته، يمكن الاستعانة في العناصر الآتية [25]:

أ- **مزود الخدمة**: الذي يمكنه رصد هذه التحركات من خلال اكتشاف العناوين التي تم الدخول إليها.

ب- **الرسائل المرسلة والملفات** التي تم تنزيلها من الشبكة.

ج- **بروتوكول الانترنت:** وهو البروتوكول الخاص بالاتصال بالإنترنت الذي يمكن- من خلاله- تحديد الشخص المستخدم للإنترنت، وتحديد موقعه.

د- **نظام الـ PROXY:** وهو حاسوب يقوم بدور الوكيل، وذلك لاختصار الوقت اللازم للوصول إلى موضع معين على شبكة الإنترنت عند تكرار الدخول إلى الموقع نفسه.

هـ- **مراقبة عمل الموظفين على الشبكة:** ويعتبر من قبيل الرقابة الإدارية لمصلحة أصحاب العمل، للتأكد عن أن العمال لا يبددون أوقات العمل لمصالحهم الشخصية، أو أنهم يعملون لمصلحة الغير.

و- **التحري الإلكتروني:** تقوم بعض الدول بتخصيص مأموري ضبط قضائي لإجراء التحريات عن جرائم تقنية المعلومات، وتتوافر لديهم الخبرة الفنية في التحقيق الجنائي، ومعالجة البيانات الإلكترونية.

المطلب الثاني: الانتقال والمعاينة في جرائم تقنية المعلومات

الانتقال والمعاينة من أهم إجراءات مرحلة جمع الاستدلالات التي يقوم بها مأموري الضبط القضائي، وعصب التحقيق الجنائي ودعامته وعماده؛ فهي تعبر عن الوقائع والحقائق تعبيرًا صادقًا، لا تكذب ولا تحابي ولا تخدع؛ فتعطي رجل الشرطة صورة صحيحة واقعية لمكان الجريمة وما يتصل بها من ماديات وآثار، كما أنها تكشف غموض الجريمة التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها [26].

الفرع الأول: المقصود بالانتقال والمعاينة في مسرح جرائم تقنية المعلومات

يقصد بالانتقال: توجه المحقق إلى محل الواقعة أو إلى أي مكان آخر توجد به آثار أو أشياء تفيد في الكشف عن الجريمة، ويكون ذلك في أسرع وقت ممكن قبل أن تزول آثارها، وبغرض جمع الآثار المتعلقة بها، وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة [27].

ولم يحدد المشرع الإماراتي المقصود بالمعاينة، ولذلك فقد عرفها الفقه الجنائي بأنها: "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته، وضبط كل ما يلزم لكشف الحقيقة" [28].

---

(24) عمر، راشد خالد (2013)، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، ص75.

(25) المعيني، سرحان حسن (2011)، التحقيق الجنائي التطبيقي، الطبعة الأولى، أكاديمية العلوم الشرطية، الشارقة، ص85- 86.

(26) إبراهيم، خالد ممدوح (2010)، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ص152- 154.

(27) جهاد، جوده حسين (2009)، الإجراءات الجزائية الدعاوى الناشئة عن الجريمة والإجراءات التحضيرية للدعوى الجزائية، الطبعة الأولى، أكاديمية شرطة دبي، دبي، ص383.

(28) حجازي، عبد الفتاح بيومي (2009)، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، منشأة المعارف، الإسكندرية، ص208.

ومعاينة مسرح الجريمة الإلكتروني يقصد به: معاينة الآثار التي يتركها مستخدم الشبكة الإلكترونية أو الإنترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها، وكل الاتصالات التي تمت من خلال الحاسوب الآلي والشبكة الإلكترونية [29].

والانتقال فورًا نحو مسرح الجريمة وإجراء المعاينة يهدف إلى ضمان عدم الشك في الدليل المستفاد منها، وذلك لأن انقضاء فترة ما بين وقوع الجريمة وإجراء المعاينة يمكن أن يسمح بأن يتمكن الجاني من أزاله العناصر المادية التي تفيد في كشف الحقيقة [30].

فبعد تلقي البلاغ تأتي الخطوة التالية، وهي الانتقال لمعاينة مسرح الجريمة والتي غالبًا ما يقوم بها رجال الضبط القضائي للكشف على مكان وقوع الجريمة وفحصه والتحفظ على أي آثار أو مخلفات أو متعلقات مادية تمت بصلة إلى الجريمة ومرتكبيها، وكذلك تصوير الموقع ووضع السيناريوهات المقترحة لكيفية حدوثها وزمن ارتكابها والملابسات المحيطة بها وإثباتها على مرتكبها [31].

وقد قضت المحكمة الاتحادية العليا في دولة الإمارات العربية المتحدة بأنه "لما كانت المواد 35- 36- 40 من قانون الإجراءات الجزائية الاتحادي 1992/35 توجب على مأموري الضبط القضائي ومرؤوسيهم أن يحصلوا على الإيضاحات، وإجراء المعاينة اللازمة لتسهيل الوقائع التي تبلغ إليهم أو التي يعملون بها بأية كيفية كانت وأن يثبتوا الإجراءات التي يقومون بها في محاضر موقع عليها منهم؛ يبين بها وقت اتخاذ الإجراءات ومكان حصولها" [32].

الفرع الثاني: ضوابط المعاينة في جرائم تقنية المعلومات

الأصل أن للمعاينة ضوابط إجرائية يجب على مأمور الضبط القضائي التقيد بها، حيث يجب عليه الالتزام بقواعد المحافظة على مسرح الجريمة، ومنع الأشخاص من الدخول إليه؛ مع عدم السماح لنفسه أو من برفقته بلمس أو تحريك الأشياء قبل وصول الخبراء المختصين، وعليه أن يحترس في كل خطوة يخطوها داخله حتى لا يضيف أو يزيل أثرًا ماديًا، أما المعاينة في مسرح الجرائم الإلكترونية تتم على النحو الآتي:

1- **مسرح الجريمة التقليدي**: ويقع خارج بيئة الحاسوب، ويتكون- بشكل رئيسي- من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، وقد يترك فيها الجاني آثار عدة كالبصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه [33]. وفي هذه الحالة ليست هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات للمعاينة من قبل مأمور الضبط القضائي، والتحفظ على الأشياء التي تعد أدلة مادية علي ارتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة، والتحفظ عليها، مع إخطار النيابة العامة بذلك، والسبب في

(29) إبراهيم، خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص165.

(30) الشواربي، عبد الحميد، (بدون سنة نشر)، البطلان الجنائي، دار النهضة العربية، القاهرة، ص148.

(31) عبد الفتاح مراد، مرجع سابق، ص247.

(32) الطعن رقم 133 لسنة 17 ق جزائي، جلسة 27 / 01 / 1996، مكتب فني 18، رقم الجزء 1، ص 2 اتحادية عليا.

(33) السرحاني، محمد بن نصير محمد (2004)، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ص77.

سهولة المعاينة في هذه الحالة أنها تتم علي عناصر مادية ملموسة كانت محلًّا للجريمة، أو تخلفت عنها عكس المعاينة التي تتم عقب وقوع الجريمة بواسطة مكونات غير مادية [34].

2- **مسرح الجريمة الافتراضي**: ويقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد وتتنقل داخل بيئة الحاسوب وشبكة الانترنت، وفي ذاكرته وفي الأقراص الصلبة الموجودة بداخله. والتعامل مع الأدلة الموجودة في هذا المسرح يجب ألا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع [35].

وفي هذه الجرائم تظهر صعوبات تحول دون فاعلية المعاينة أو فائدتها، ويمكن تلخيصها في الآتي:

أ- الصعوبة الأولى تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلوماتية بصفة عامة، وبرامج الحاسوب الآلي وبياناته بصفة خاصة.

ب- الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبًا ما تكون طويلة نسبيًّا، ما بين وقوع الجريمة والكشف عنها، الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها، وهو ما يلقي ظلالًا من الشك علي الدليل المستمد من المعاينة [36].

وبخلاف ذلك فمن الممكن أن تكون الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الحاسوب الآلي ثرية جدًّا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة والبريد الإلكتروني والفيديو الرقمي والصوت الرقمي وغرف الدردشة والمحادثة، والملفات المخزنة في الحاسوب الآلي الشخصي، والصورة المرئية، والدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمات [37].

ولذلك؛ فإنه يجب عند معاينة مسرح جرائم تقنية المعلومات مراعاة القواعد والإرشادات الفنية الآتية [38]:

1- القيام بتصوير الحاسوب الآلي، وما قد يتصل به من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد به بصفة عامة، مع العناية بتصوير أجزائه الخلفية، وملحقاته الأخرى على أن يراعى تسجيل تاريخ المكان الذي تم التقاط الصورة فيه وزمانه.

2- ملاحظة طريقة إعداد نظام الحاسوب بعناية بالغة.

3- إثبات الحالة التي تكون عليها كابلات الحاسوب وتوصيلاته بمكونات النظام؛ حتى يسهل عليه القيام بعملية المقارنة والتحليل لها عند عرض الموضوع على المحكمة المختصة.

4- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة قبل إجراء الاختبارات اللازمة؛ للتيقن عن عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة بسبب تداخل المجالات المغناطيسية مع بعضها البعض.

5- حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة، وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها علاقة بالجريمة المرتكبة؛ لأن دليل الجهة قد يكمن في مكافحة هذه القصاصات.

6- حفظ المستندات الخاصة بالإدخال، وكذلك مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع البصمات التي قد تكون موجودة عليها ومضاهاتها.

---

(34) حجازي، عبد الفتاح بيومي، مرجع سابق، ص211.

(35) السرحاني، محمد بن نصير محمد، مرجع سابق، ص77.

(36) حجازي، عبد الفتاح بيومي، مرجع سابق، ص212.

(37) إبراهيم، خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص165.

(38) حجازي، عبد الفتاح بيومي، مرجع سابق، ص212- 214.

7- يجب قصر عملية المعاينة على مأموري الضبط القضائي سواء أكانوا من الباحثين أم المحققين الذين تلقوا التدريب الكافي والذين تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات، ومواجهة هذه النوعية من الجرائم، والتعامل مع أدلتها التي قد تتخلف عنها على مسرح الجريمة التقليدي.

ويبين مما تقدم أن جهاز الشرطة المتمثل في مأموري الضبط القضائي يعملون من خلال البحث والتحري عن الاستدلالات التي تدين المجرم الإلكتروني؛ فحين تلقيهم البلاغات والشكاوى المرتبطة بجرائم تقنية المعلومات عبر الشبكة الإلكترونية؛ يقومون بالبحث والتحري عن مرتكب تلك الجريمة، وكشف غموضها بواسطة الإرشاد الجنائي والمراقبة الإلكترونية للشبكة عبر الإنترنت، وذلك من خلال التقنية الإلكترونية للحصول على بيانات ومعلومات تفيد في التعرف على مرتكب جرائم تقنية المعلومات، للحد منها وضبطها؛ لتحقيق الأمن الإلكتروني.

وعلى هذا الأساس يجب على القائمين بعملية البحث والتحري ومعاينة مسرح الجرائم الإلكترونية أن يكونوا على درجة عالية من التأهيل والتدريب الفني الكافي لمواجهة هذه النوعية من الجرائم، وأن تعطى هذه الاختصاصات في البحث والتحري والمعاينة في العالم الافتراضي إلى سلطة مختصة في الجرائم الإلكترونية، وتكون تابعة لإدارة التحريات والمباحث الجنائية بدولة الإمارات العربية المتحدة مثل المباحث الإلكترونية بشرطة دبي، وفرع الجرائم الإلكترونية بأبوظبي؛ لكون مرتكبي هذه الجرائم على درجة عالية من الذكاء والتخصص في اختراق المواقع أو النظام المعلوماتي.

المبحث الثاني: إجراءات التحقيق الابتدائي في جرائم تقنية المعلومات

إن التحقيق الابتدائي اختصاص أصيل وهام تباشره النيابة العامة بإجراءات متعددة تتسم بالحيدة التامة، وأعضاؤها هم الذين يضطلعون به أصلًا بأنفسهم توصلًا إلى مدى توافر أركان الجريمة، ومدى ثبوتها أو عدم ثبوتها في حق متهم معين.

وفي ذلك أسند المشرع الإماراتي سلطة التحقيق والاتهام إلى النيابة العامة دون سواها، فقد نص القانون رقم (3) لسنة 1983م في شأن السلطة القضائية الاتحادية في المادة (57) من الفقرة الثانية منه على أن "النيابة العامة لا تتجزأ بوصفها سلطة تحقيق أو سلطة اتهام"، بما مفاده أن المشرع جعل السلطتين في يد النيابة العامة كقاعدة عامة، كما نص قانون الإجراءات الجزائية الاتحادي الإماراتي رقم (35) لسنة 1992 في المادة (5) منه على أن "النيابة العامة جزء من السلطة القضائية وتباشر التحقيق والاتهام في الجرائم وفقًا لأحكام هذا القانون".

وعلى ذلك فإذ يباشر أعضاء النيابة التحقيق لا يقصدون من ورائه سوى التوصل إلى كشف الحقيقة؛ سعيًا إلى تطبيق موجبات القانون وتحقيق العدالة التي هي أسمى رسالة في الوجود. وللنيابة العامة أن تكلف أحد مأموري الضبط القضائي للقيام بعمل معين أو أكثر من أعمال التحقيق مثل التفتيش والضبط والانتقال والمعاينة فيما عدا استجواب المتهم [39]. وعليه سيتم تقسيم المبحث إلى مطلبين، **المطلب الأول:** التفتيش في جرائم تقنية المعلومات وجمع الأدلة وضبطها، و**المطلب الثاني:** ندب الخبراء والاستجواب في جرائم تقنية المعلومات.

المطلب الأول: التفتيش في جرائم تقنية المعلومات وجمع الأدلة وضبطها

من الناحية القانونية لم يعرف المشرع الإماراتي "التفتيش" في قانون الإجراءات الجزائية؛ لذلك تكفل الفقه بتعريف التفتيش؛ وهو إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، ويستهدف البحث عن الأدلة المادية لجريمة تحقق وقوعها في مكان معين، أو محل خاص، أو في أي مستودع للسر يتمتع بالحرمة؛ بغض النظر عن

(39) جهاد، جوده حسين، مرجع سابق، ص363

إرادة صاحبه. وينطوي التفتيش على إذن للمساس بحرية الشخص في حماية أسراره، ويستهدف البحث عن أدلة الجريمة أو ضبط الأشياء التي تفيد في كشف الحقيقة [40].

الفرع الأول: التفتيش في جرائم تقنية المعلومات

إن التفتيش إجراء من إجراءات التحقيق، ويستهدف البحث عن الحقيقة مستودع السر؛ لذلك يعد من أهم إجراءات التحقيق في كشف الحقيقة؛ لأنه غالبًا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم، والتفتيش ليس غاية في حد ذاته؛ وإنما وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في بيان الحقيقة وظهورها، ونتيجة لذلك يعد تفتيش نظام الحاسوب والإنترنت من أخطر المراحل حال اتخاذ الإجراءات الجنائية ضد مرتكب جرائم تقنية المعلومات؛ لكون محل التفتيش هنا وهو الحاسوب والشبكات [41].

أولاً: السلطة المختصة بالتفتيش في جرائم تقنية المعلومات

والتفتيش لا تملكه- بحسب الأصل- إلا سلطة التحقيق وهي النيابة العامة، ويخضع للخصائص العامة التي تخضع لها كل إجراءات التحقيق الابتدائي، وإذا كان القانون قد سمح لمأموري الضبط القضائي من غير أعضاء النيابة العامة بالقبض على المتهمين وتفتيشهم وتفتيش مساكنهم في حالات معينة في المواد (45، 51، 53، 54) من قانون الإجراءات الجزائية الاتحادي الإماراتي؛ فهذا استثناء من القاعدة العامة، حيث أن النيابة غير مطالبة بإجراء التفتيش بنفسها؛ فربما لا يتسع وقت وكيل النيابة لتنفيذه، لا سيما إذا تعددت الأماكن أو الأشخاص أو الحاسبات المراد تفتيشها، لذا فقد جرى العمل- في غالب الأحيان- على ندب أحد مأموري الضبط القضائي لإجرائه بإعطائه ما يسمى "بإذن أو بأمر التفتيش" الذي ينبغي أن تراعى في إصداره وتحريره جميع القيود الخاصة بالندب[42]، فقد نصت المادة (72) من قانون الإجراءات الجزائية الإماراتي على أنه " لعضو النيابة العامة تفتيش منزل المتهم بناء على تهمة موجهة إليه بارتكاب جريمة أو باشتراكه في ارتكابها، وله أن يفتش أي مكان ويضبط فيه أية أوراق أو أسلحة وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج منها أو وقعت عليه وكذلك كل ما يفيد في كشف الحقيقة"، وكذلك نصت المادة (75) من القانون آنف البيان على أنه " لعضو النيابة العامة أن يفتش المتهم ولا يجوز له تفتيش غير المتهم أو منزل غير منزله إلا إذا اتضح من إمارات قوية أنه حائز لأشياء تتعلق بالجريمة. ويجوز له بموافقة النائب العام أن يضبط لدى مكاتب البريد جميع المكاتبات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق جميع البرقيات، وأن يراقب ويسجل المحادثات بما في ذلك السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك".

وعليه فالتفتيش الإلكتروني إجراء من إجراءات التحقيق يهدف إلى البحث في داخل نظام الحاسوب الآلي أو الإنترنت المعين بإذن قضائي مسبق سواء أكان هذا النظام مكونًا من حاسوب واحد أو عدة حواسيب مرتبطة فيما بينها بشبكة في محل له حرمة منحه إياها القانون، والغرض استخراج أدلة معلوماتية متمثلة في المعلومات أو البيانات التي تساعد على كشف الحقيقة في جريمة من نوع جناية أو جنحة وقعت، والتحقيق فيها جار"[43].

---

(40) الجندي، حسنى (بدون سنة نشر)، قانون الإجراءات الجزائية في دولة الإمارات العربية المتحدة معلقا عليه بالفقه وأحكام القضاء، الطبعة الأولى، الجزء الأول الاسكندرية، ص 494.

(41) مصطفى، عائشة بن قارة (2010)، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ص87- 88.

(42) جهاد، جوده حسين، مرجع سابق، ص389.

(43) حسين، سامي جلال فقي (2011)، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، المحلة الكبرى، ص55.

ثانيًا: محل التفتيش في جرائم تقنية المعلومات

محل التفتيش في الجرائم التقليدية قد يكون الشخص، وقد يكون مسكنه وقد يكون كلاهما محلًا للتفتيش وكل الأشياء التي تفيد في كشف الحقيقة، بينما محل التفتيش في جرائم تقنية المعلومات تتمثل في البرامج أو الكيانات المنطقية والبيانات المسجلة في ذاكرة الحاسوب الآلي أو في مخرجاته، والسجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات ودفتر يومية التشغيل وسجل المعاملات، والسجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، وما يتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة[44]، ويمكننا أن نرصد خضوع الحاسوب الآلي والشبكة المعلوماتية للتفتيش، وذلك على النحو الآتي:

1- **الاحتمال الأول**: أن يكون حاسوب المتهم متصلاً بحاسب أو نهاية طرفية موجودة في مكان آخر داخل الدولة.
2- **الاحتمال الثاني:** هو اتصال حاسوب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة. ومن المشكلات التي تواجه القائمون على جمع الأدلة والتحقيقات حالة امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي لدولة أخرى وهو ما يسمى بالولوج أو التفتيش عبر الحدود، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية.
3- **الاحتمال الثالث:** التنصت والمراقبة الإلكترونية لشبكات الحاسوب الآلي.

من جماع ما تقدم يبين بجلاء أن جرائم تقنية المعلومات قد تقع في صورة كيانات مادية يسهل تفتيشها واكتشاف أمرها وضبطها، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبالضمانات نفسها والإجراءات المقررة قانونًا. أما الجرائم التي تقع على الكيان المعنوي فإنه يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات، أما إذا تحولت هذه الكيانات إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها[45].

وتجدر الإشارة إلى خلو قانون الإجراءات الجزائية الإماراتي من إجراءات التفتيش التي تتمثل في اتصال حاسوب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة. كما خلا أيضا القانون الاتحادي رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات من إجراءات التفتيش.

الفرع الثاني: جمع الأدلة الإلكترونية وضبطها

إن الغرض من التفتيش هو ضبط الأدلة أو الأشياء التي تفيد في ظهور الحقيقة في الجريمة التي وقعت، فالضبط في معظم الأحوال هو غرض التفتيش، وإن لم يكن هو السبب الوحيد، فقد يتم الضبط استنادًا لأسباب أخرى غير التفتيش من ذلك المعاينة وما قدمه المتهم والشهود لمأموري الضبط القضائي[46].

يقصد بالضبط في قانون الإجراءات الجزائية وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق[47].

فالغاية من التفتيش هي ضبط كل ما يفيد في كشف الحقيقة سواء تعلق ذلك بأشخاص أو أماكن أو أشياء طالما كان لها اتصال بالجريمة، وقد قضت المحكمة الاتحادية العليا بأنه "عدم الالتزام بمبدأ تخصيص التفتيش

---

(44) على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، مرجع سابق، ص40.

(45) إبراهيم، خالد ممدوح، مرجع سابق، ص195- 200.

(46) حجازي، عبد الفتاح بيومي، مرجع سابق، ص260.

(47) الديربي، عبد العال، وإسماعيل محمد صادق (2012)، الجرائم الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ص321

بجريمة معينة وهى التي يجرى في شأنها الاستدلال أو التحقيق إذ ينحصر اتجاه المشرع فيما يفيد في كشف الحقيقية في شأن هذه الجريمة فإذا استهدف الضابط البحث عن أشياء تتعلق بجريمة مختلفة فعثر عليها، ثم ضبطها كان ضبطها باطلاً ويتصل بذلك أنه إذا حقق أمر القبض أو التفتيش غرضه فليس على الضابط الاستمرار بعد ذلك للعثور على ما يعد جريمة لضبطه، إذ أن ضبطه يقع باطلاً مثال صدور إذن النيابة العامة لضبط المتهم المطلوب لتهمة الاعتداء ومحاولة اللواط والخطف فإن أخذ العينة من بول الطاعن وتحليلها لتهيئة الدليل لجريمة تعاطى المخدرات يكون متجاوزًا لإذن النيابة الصادر بشأن القبض عليه بسبب قضايا أخرى ليس من شأن التفتيش بمناسبتها اتخاذ هذا الإجراء باعتبار أن أمر القبض قد حقق غرضه بمجرد إلقاء القبض على المتهم وكان التزيد بأخذ العينة مستهدفا البحث عن دليل يتعلق بجريمة أخرى غير تلك التي وردت بإذن النيابة ولم نتناولها وبالتالي خلق جريمة أخرى لم تكن فيها إرادة الشخص حرة" [(48)].

وبناءً عليه، فإن الأشياء التي ينبغي إخضاعها لأجراء الضبط في جرائم تقنية المعلومات والتي تعد كيانات ذات قيمة يمكن الاستفادة منها في إثبات الجريمة أو نسبتها إلى الجاني هي:

1- **ضبط المستندات والكيانات الورقية** التي وقعت عليها العمليات الإلكترونية والتي يعتقد أن لها صلة بالجريمة أو مرتكبيها، وقد تكون محررات مزورة داخل نظام الحاسب الآلي أو في أي مكان خارجه، ويمكن أن تكون في سلة المهملات.
2- **وحدة المدخلات** المكونة من مفردات لوحة المفاتيح والشاشة والفارة والخادم مجمع المعلومات الماسحة الضوئية وكذلك برنامج معالجة النصوص وبرنامج عرض الشرائح
3- **ضبط المراسلات الإلكترونية** التي تستخدم البريد الإلكتروني عبر شبكة الأنترنت والتي يتم من خلالها نقل الرسائل ومحتوى المستندات الورقية حيث تتمتع هذه الوسيلة بنظام حماية تتكون من رموز وشفرات لا يمكن الاطلاع عليها إلا إذا عرفت عليها الجهة المستقبلية، وهي تحتفظ بنسخ عن المواد المرسلة منها وإليها يمكن استرجاعها والاطلاع عليها وضبطها.
4- **الشرائط المغنطة** وهي جميع الشرائط ووسائط النقل والتخزين التي يعتقد أنها تحتوي على مواد تفيد في كشف الحقيقية أو مرتكبيها.
5- **ضبط الطابعات وأجهزة التصوير بكافة أنواعها**، ولا سيما أن الأجهزة الحديثة يمكنها تخزين المستندات والمواد المطبوعة أو المنسوخة، حيث يمكن إعادة استخراجها والتعرف على محتوياتها.
6- **ضبط وحدة الذاكرة الرئيسية**، ووحدة التحكم، والمودم (وهي الوسيلة التي تتمكن من خلالها أجهزة الحاسوب من الاتصال فيها بينها بواسطة خطوط الهاتف).

المطلب الثاني: ندب الخبراء والاستجواب في جرائم تقنية المعلومات

الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلاً مستقلاً عن الدليل القولي أو الدليل المادي، وإنما هي تقييم فني لهذا الدليل، والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة والشهادة والتفتيش، وهو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها

(48) الطعن رقم 138 لسنة 2008 جزائي جلسة 29 / 12 / 2009 اتحادية عليا.

التدليلية في الإثبات، حيث تفيد الخبرة في إثبات وقوع الجريمة أو نسبتها إلى المتهم أو في تحديد ملامح شخصيته الإجرامية [49].

أما الاستجواب فيعد من أهم إجراءات التحقيق المستخدمة في كشف الحقيقة، حيث يمكن الاستجواب السلطة المناط بها التحقيق من طرح الأسئلة الدقيقة والولوج في موضوع الدعوى، والتعرف إلى أدق التفصيلات فيما يتعلق بالجريمة، ويعرف الاستجواب بأنه "إجراء من إجراءات التحقيق تتم فيه مناقشة المتهم فيما هو منسوب إليه من جرم، ويُطلب منه الرد على الأدلة القائمة ضده إما بتنفيذها أو التسليم بها"[50].

الفرع الأول: ندب الخبراء في جرائم تقنية المعلومات

لقد أباح قانون الإجراءات الجزائية الإماراتي للمحقق متى استلزم إثبات الحالة الاستعانة بالخبراء، فنصت المادة (96) منه على أنه: "إذا اقتضى التحقيق الاستعانة بطبيب أو غيره من الخبراء لإثبات حالة من الحالات كان لعضو النيابة العامة أن يصدر أمرًا بندبه ليقدم تقريرًا عن المهمة التي يكلف بها. ولعضو النيابة العامة أن يحضر وقت مباشرة الخبير مهمته، ويجوز للخبير أن يؤدي مهمته بغير حضور الخصوم".

ومن هذا المنطلق؛ فإنه من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع جرائم تقنية المعلومات، ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات وتشغيل الحاسوب الآلي وعلومه، وأن نجاح جمع الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنًا بكفاءة وتخصص هؤلاء الخبراء.

ويجب على المحقق الجنائي أن يحدد للخبير المعلوماتي دوره في المسألة المنتدب فيها على وجه الدقة، وهذا يعود بنا إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق الابتدائي في الجرائم المعلوماتية لنجاح تحقيق مثل هذه الجرائم، ودرءاً لما ينادي به البعض من أنه يمكن للخبير نفسه أن يحدد إطار مهمته، إذ أن ذلك سوف يقوض دور المحقق والقاضي في الدعوى الجنائية المتعلقة بجرائم تقنية المعلومات [51].

والنيابة العامة تمتلك سلطة تقديرية في ندب الخبراء من عدمه، وذلك تحت رقابة محكمة الموضوع.

وتجدر الإشارة إلى أنه يمكن القول بأن الاستعانة بالخبراء في مجال الجرائم التي تقع على تقنية المعلومات ضرورية، وخاصة عندما يعجز المحقق- أثناء التحقيق في جريمة ما- عن فهم الجوانب التقنية أو العلمية التي تحتاج إلى قدر متقدم من التخصص لكشف غموضها أو فهم طبيعتها، وقد أجاز له القانون الاستعانة بأشخاص أو جهات فنية أو مخبرية أو مهنية متخصصة في المسألة موضوع الخبرة.

وتعد الاستعانة بالخبراء جزءًا من عملية التحقيق، وذلك للمساعدة في كشف غموض الجريمة وإثبات أدلتها في مواجهة الجناة أو المشتبه فيهم أو نفيها عنهم [52].

---

(49) المهيري، خالد محمد كدفور (بدون سنة نشر)، التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، الطبعة الثانية، معهد القانون الدولي، دبي، ص489.

(50) إبراهيم، خالد ممدوح، مرجع سابق، ص241.

(51) حجازي، عبد الفتاح بيومي، مرجع سابق، ص601.

(52) إبراهيم، راشد بشير (2008) التحقيق الجنائي في جرائم تقنية المعلومات، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، العدد 131، ص67.

الفرع الثاني: الاستجواب في الجرائم تقنية المعلومات

إن مباشرة الاستجواب في جرائم تقنية المعلومات تتم بواسطة سلطة التحقيق، حيث نصت المادة (99) من قانون الإجراءات الجزائية الاتحادي على أنه: "يجب على عضو النيابة العامة عند حضور المتهم لأول مرة في التحقيق أن يدون جميع البيانات الخاصة بإثبات شخصيته، ويحيطه علمًا بالتهمة المنسوبة إليه، ويثبت في المحضر ما قد يبديه في شأنها من أقوال".

والاستجواب بهذا المعنى يحقق وظيفتين: أولاهما، إثبات شخصية المتهم ومناقشته تفصيلاً في الاتهام الموجه إليه، وثانيتهما تحقيق دفاع المتهم، ذلك أن مناقشة المتهم في أدلة الاتهام قد تؤدي إلى اعترافه بارتكاب الجريمة، كما أنها في الوقت ذاته تفسح السبيل أمامه إذا كان بريئًا، وذلك لتقنين الأدلة القائمة ضده فتجنبه رفع الدعوى عليه، ومغبة الوقوف موقف الاتهام، علاوة على أنه قد تساعد العدالة على معرفة الحقيقة وكشف الفاعل الحقيقي[53].

والتشريع الإماراتي يوجب استجواب المتهم أثناء التحقيق الابتدائي في أحوال معينة أظهرها حالات القبض على المتهم وحبسه احتياطيًا؛ فعلى النيابة العامة أن تستجوبه خلال أربع وعشرين ساعة ثم تأمر بالقبض عليه أو إطلاق سراحه [54]، ويجوز لعضو النيابة بعد استجواب المتهم أن يصدر أمرًا بحبس احتياطيًا إذا كانت الدلائل كافية وكانت الواقعة جناية أو جنحة معاقب عليها بغير الغرامة [55].

على أن الاستجواب لا يخلو من خطورة؛ لأنه ينطوي بذاته على رغبة تضييق الخناق على المتهم، وقد يدفعه تعدد الأسئلة التي توجه إليه في استدراجه إلى أن يقول صدقًا أم كذبًا، أو ما ليس في صالحه، أو إلى اعتراف غير مطابق للواقع ومضلل للعدالة [56].

وعليه؛ يجب إلمام المحقق في مرحلة الاستجواب بجرائم تقنية المعلومات وطرق ارتكابها، وبمبادئ الحاسوب والإنترنت والمصطلحات المتعلقة بها، ومبادئ وأسس أمن المعلومات بالشكل الذي يمكنه من التواصل الجيد مع الشهود والمتهمين من جهة ومع خبير الحاسوب في فريق التحقيق من جهة أخرى، وربما كان الأسلوب الأمثل في عملية الاستجواب هو الذي يقوم على ضرورة حضور خبير الحاسوب لعملية الاستجواب، وتمكينه من الاشتراك فيها بتوجيه الأسئلة الفرعية للشاهد أو المتهم، وربما قام بكتابة السؤال على قطعة من الورق ووضعها أمام المحقق ليقوم الأخير بتخَّين الفرصة المناسبة لإلقاء السؤال بما يتناسب والأصول الفنية للاستجواب.

الخاتمة

تناول البحث موضوع الإطار القانوني لإجراءات التحقيق في جرائم تقنية المعلومات في ضوء التشريع الإماراتي، من خلال بيان إجراءات التحقيق المتعلقة بمرحلة الاستدلالات التي يقوم بها مأموري الضبط القضائي من رجال الشرطة أو الخبراء المختصين الذين منحوا هذه الصفة، وكذلك الإجراءات المتخذة خلال مرحلة التحقيق الابتدائي التي تقوم بها النيابة العامة. وفي خاتمة البحث، فقد توصل الباحثان إلى مجموعة من النتائج والتوصيات، وهي على النحو الآتي:

---

(53) المهيري، خالد محمد كدفور، مرجع سابق، ص574.

(54) المادة رقم (47) من قانون الإجراءات الجزائية الاتحادي رقم (35) لسنة 1992م وتعديلاته.

(55) المادة رقم (106) من قانون الإجراءات الجزائية الاتحادي رقم (35) لسنة 1992م وتعديلاته.

(56) المادة رقم (1/165) من قانون الإجراءات الجزائية الاتحادي رقم (35) لسنة 1992م وتعديلاته.

أولاً: النتائج الرئيسية

خلصت هذه الدراسة إلى مجموعة من النتائج تتمثل في الآتي:

1- تعد أجهزة الشرطة (مأموري الضبط القضائي) خلال مرحلة جمع الاستدلالات والنيابة العامة خلال مرحلة التحقيق الابتدائي الجهات المختصة في مواجهة جرائم تقنية المعلومات.

2- أن مأموري الضبط القضائي حين تلقيهم البلاغات والشكاوى المرتبطة بجرائم تقنية المعلومات عبر الشبكة الإلكترونية؛ يقومون بالبحث والتحري عن مرتكب تلك الجريمة، وكشف غموضها بواسطة الإرشاد الجنائي والمراقبة الإلكترونية للشبكة عبر الإنترنت، وذلك من خلال التقنية الإلكترونية للحصول على بيانات ومعلومات تفيد في التعرف على مرتكب جرائم تقنية المعلومات، للحد منها وضبطها؛ لتحقيق الأمن الإلكتروني.

3- أن القائمين على عملية البحث والتحري ومعاينة مسرح الجرائم الإلكترونية يجب أن يكونوا على درجة عالية من التأهيل والتدريب الفني الكافي لمواجهة هذه النوعية من الجرائم.

4- خلو قانون الإجراءات الجزائية الإماراتي من إجراءات التفتيش التي تتمثل في اتصال حاسوب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة، كما خلا أيضا القانون الاتحادي رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات من إجراءات التفتيش.

5- لم يتطرق قانون الإجراءات الجزائية الإماراتي إلى قواعد الضبط في جرائم تقنية المعلومات مكتفي بالقواعد العامة للضبط في الجرائم.

6- صعوبة إثبات جرائم تقنية المعلومات؛ بسبب صعوبة الاحتفاظ الفني بآثارها إن وُجدت، والحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها، وهذا ما يعرقل عمل رجال التحقيق الذين تعودوا على التعامل مع الجرائم التقليدية.

ثانيًا: التوصيات والمقترحات

1- ضرورة صدور قانون ينظم إجراءات الضبط والتفتيش للكيانات المعنوية للحاسب الآلي، ونظم تقنية المعلومات، يأخذ في الاعتبار خصائص جرائم تقنية المعلومات من حيث سرعة إخفاء الدليل وتدميره وعدم ترك آثار مادية.

2- ضرورة إخضاع مأموري الضبط القضائي على تدريب متخصص يمكنهم من فهم مضامين البلاغات المرتبطة في جرائم تقنية المعلومات واستيعاب معطيات مسرح الجريمة، والتعامل مع الأدلة المتحصلة من الوسائل الإلكترونية.

3- ضرورة خضوع اتصالات الشبكة الإلكترونية في دولة الإمارات العربية المتحدة إلى الشرطة، حيث لا يوجد نص في القانون الاتحادي رقم (3) لسنة 2003م في شأن تنظيم قطاع الاتصالات في هذا الشأن.

4- ضرورة أن يتضمن قانون الإجراءات الجزائية الاتحادي بدولة الإمارات قواعد لتنظيم إجراءات الضبط في جرائم تقنية المعلومات، يعطي مأموري الضبط القضائي سلطة استخدام كافة الوسائل الممكنة للضبط المشروع عن طريق الشبكة الإلكترونية.

5- إعطاء اختصاص البحث والتحري والمعاينة في العالم الافتراضي إلى سلطة مختصة في جرائم تقنية المعلومات، ويمكننا تحديد المهارات الفنية الواجب توافرها بالتدريب والتأهيل لدى ضباط الشرطة والتحقيق في جرائم تقنية المعلومات.

قائمة المراجع

أولاً: المراجع الفقهية

1- إبراهيم، خالد ممدوح (2010): فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية.

2- إبراهيم، راشد بشير (2008): التحقيق الجنائي في جرائم تقنية المعلومات، مركز الإمارات للدراسات والبحوث الاستراتيجية، الطبعة الأولى، العدد 131، أبو ظبي.

3- الجندي، حسنى (بدون سنة نشر): قانون الإجراءات الجزائية في دولة الإمارات العربية المتحدة معلقا عليه بالفقه وأحكام القضاء، الطبعة الأولى، الجزء الأول الإسكندرية.

4- جهاد، جوده حسين (2009): الإجراءات الجزائية الدعاوى الناشئة عن الجريمة والإجراءات التحضيرية للدعوى الجزائية، الطبعة الأولى، أكاديمية شرطة دبي، دبي.

5- حجازي، عبد الفتاح بيومي (2009): الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، منشأة المعارف، الإسكندرية.

6- حسين، سامي جلال فقي (2011): التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، المحلة الكبرى.

7- الحمودي، محمد علي (2009): دور مأمور الضبط القضائي في مواجهة جرائم المعلومات، الطبعة الأولى، الناشر المؤلف، بلد النشر (بدون).

8- الديربي، عبد العال، وإسماعيل، محمد صادق (2012): الجرائم الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة.

9- سالم، نبيل مدحت (2009): شرح قانون الاجراءات الجنائية، الجزء الثاني، دار النهضة العربية، القاهرة، مصر.

10- السرحاني، محمد بن نصير محمد (2004): مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض.

11- سرور، أحمد فتحي (2012): الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة.

12- شحاته، محمد أحمد (2013): شرح قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة، المكتب الجامعي الحديث، الإسكندرية.

13- الشواربي، عبد الحميد، (بدون سنة نشر): البطلان الجنائي، دار النهضة العربية، القاهرة.

14- عمر، راشد خالد (2013): المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية.

15- الفيل، على عدنان (2012): إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية.

16- محمد، نصر محمد (2012): التحقيق الجنائي بين الواقع والقانون، دراسة تطبيقية على أنواع البصمات وحجيتها، الفكر الشرطي، مركز بحوث شرطة الشارقة، القيادة العامة لشرطة الشارقة، الشارقة، المجلد (21) العدد (83)، شهر أكتوبر.

17- مصري، عبد الصبور عبد القوي على (2012): المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض.

18- مصطفى، عائشة بن قارة (2010): حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية.
19- المعيني، سرحان حسن (2011): التحقيق الجنائي التطبيقي، الطبعة الأولى، أكاديمية العلوم الشرطية، الشارقة.
20- المليح، عبد الله محمد (2009): مدخل الإجراءات الشرطية في البلاغات الأمنية في دولة الإمارات العربية المتحدة، مركز بحوث الشرطة، شرطة الشارقة، الشارقة.
21- المهيري، خالد محمد كدفور (دون سنة نشر): التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، الطبعة الثانية، معهد القانون الدولي، دبي،
22- موسى، مصطفى محمد (2003): المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، القاهرة.
23- موسى، مصطفى محمد (2005): دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، المحلة الكبرى.
24- هروال، نبيلة هبة (2013): الجوانب الإجرائية لجرائم الإنترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية.
25- ولد راحة، الراشد سالم عبيد سالمين (2010): عرض التجارب والخبرات الأمنية المختلفة في التعامل مع جرائم تقنية المعلومات والاتصالات الخاصة بالأطفال، الطبعة الأولى، مركز بحوث الشرطة، أكاديمية شرطة دبي، دبي.
26- اليماحي، عبد الله راشد سعيد (2014): إجراءات تفتيش نظم الحاسب الآلي والإنترنت، دراسات قانونية، سلسة الرسائل العلمية، أكاديمية شرطة دبي، كلية الدراسات العليا، دبي.

ثانيًا: التشريعات في دولة الإمارات العربية المتحدة

1- المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.
2- قانون الإجراءات الجزائية الاتحادي رقم (35) لسنة 1992م وتعديلاته.
3- قانون العقوبات الاتحادي رقم (3) لسنة 1987م.
4- قانون السلطة القضائية الاتحادي رقم (3) لسنة 1983.
5- قانون تنظيم قطاع الاتصالات الاتحادي رقم (3) لسنة 2003م.
6- قانون السلطة القضائية الاتحادية رقم (3) لسنة 1983م.

ثالثًا: الاجتهادات القضائية

1- مجموعة أحكام النقض الصادرة عن المحكمة الاتحادية العليا لدولة الإمارات.
2- المبادئ القانونية المقررة من محاكم تمييز دبي.

Criminal Investigation Procedures in IT Crimes In accordance with UAE legislation

ABSTRACT: This study dealt with the subject of the legal framework for the procedures of investigating the crimes of information technology in accordance with UAE legislation by reviewing the procedures of the police officers during the period of gathering the inferences and the preliminary investigation procedures conducted by the Public Prosecution to combat IT crimes. The legal problems and challenges facing the investigation of such crimes, and to determine the appropriateness of traditional criminal investigation methods in the field of information technology crimes. The study relied on the analytical description of the relevant laws and laws The study concluded with a series of results, the most prominent of which is that IT crimes require judicial officers to have a reasonable degree of culture in the field of IT systems so that they can initiate the procedures for collecting inferences, UAE Code of Criminal Procedure to the rules of control in the crimes of information technology is satisfied with the general rules for the control of crimes. The study also reached a number of recommendations, the most important of which is the need to subject the investigation bodies responsible for combating information crimes to specialized training that enables them to understand the contents of the communications related to the crimes of information technology and to assimilate crime scene data and to deal with the evidence obtained from the electronic means.

Keywords: IT crimes, cybercriminals, digital evidence, electronic security.