مجلة جامعة الشارقة للعلوم القانونية

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة

مجلة علمية محكمة

للعلوم القانونية

المجلد 21، العدد 3
ربيع الأول 1446هـ / سبتمبر 2024م

الترقيم الدولي المعياري للدوريات 2616-6526

https / /:doi.org /10.36394 /jls.v21.i3.2

الآليات الإجرائية لضبط الجريمة الإلكترونية "في التشريع الإماراتي ـ دراسة تحليلية"

محمـد إبراهيم العليلين[1]

حليمه خالد المدفع[2]

تاريخ الاستلام: 12-12-2022 **تاريخ القبول: 09-03-2023**

ملخص البحث:

يسـعى هـذا البحـث للتعـرف إلـى الآليـات الإجرائيـة لضبـط الجريمـة الإلكترونيـة فـي ظـل الخصائـص والطبيعـة القانونيـة الخاصـة المميـزة لهـا، والتعـرف إلـى الآليـات الإجرائيـة التقليديـة والمسـتحدثة لضبطهـا، وسـيدرس مـدى صلاحيـة أو كفايـة الآليـات الإجرائيـة التقليديـة الـواردة فـي قانـون الإجـراءات الجزائيـة لضبـط الجريمـة الإلكترونيـة، ومـدى احتـواء القوانيـن السـارية فـي دولـة الإمـارات بشـأن مكافحـة جرائـم تقنيـة المعلومـات علـى الآليـات الإجرائيـة المسـتحدثة لضبـط الجريمـة الإلكترونيـة. وقـد توصلـت الدراسـة إلـى أن القواعـد الإجرائيـة التقليديـة والمسـتحدثة الـواردة فـي القانـون الإماراتـي بشـأن ضبـط الجريمـة الإلكترونيـة غيـر كافيـة لتنظيـم ضبـط المكونـات المعنويـة أو الأدلـة الرقيمـة. وقـد أوصـت الدراسـة بدعـوة المشـرع الإماراتـي إلـى تضميـن قانـون الإجـراءات الجزائيـة الاتحـادي فصـل خـاص لضبـط الجرائـم الإلكترونيـة تتلاءم مـع الطبيعـة الخاصـة لهـذه الجرائـم، كبديـل شـامل ودقيـق بسـبب تفـرق هـذه القواعـد الإجرائيـة مـا بيـن عـدد مـن القوانيـن، التطويـر المسـتمر وزيـادة فعاليـة الوحـدات أو الإدارات أو الأقسـام المنـوط بهـا القيـام بإجـراءات التحـري والتحقيـق فـي الجرائـم الإلكترونيـة، وزيـادة وتكثيـف البرامـج التدريبيـة المتخصصـة لزيـادة وتحديـث المعـارف والمهـارات التقنيـة المعلوماتيـة لسـلطات الضبـط القضائـي والتحـري والتحقيـق فـي الجرائـم الإلكترونيـة، تخصيـص أعضـاء نيابـة وقضـاة تحقيـق وقضـاة محاكـم للتعامـل مـع الجرائـم الإلكترونيـة، والعمـل علـى تأهليهـم علميـاً وفنيـاً بكافـة المعـارف والمهـارات التـي تمكنهـم القيـام بأدوارهـم بكفـاءة وفعاليـة.

الكلمـات الدالـة: الجريمـة الإلكترونيـة، المعاينـة الرقميـة، التفتيـش المعلوماتـي، ضبـط الأدلـة الرقمية.

(1) كلية القانون – جامعة الشارقة (الشارقة – الإمارات العربية المتحدة)

alaleeli7@gmail.com

(2) كلية القانون – جامعة الشارقة (الشارقة – الإمارات العربية المتحدة)

المقدمة:

لقد أصبحت التقنيات الإلكترونية عنصرًا رئيسًا في مجالات عديدة للحياة اليومية، وقد وجد أصحاب الميول الإجرامية في هذه البيئة مجالاً خصباً لارتكاب صور عديدة ومتنوعة من الجرائم الالكترونية، منها ما يتعلق بالاعتداء على المعلومات واختراق الخصوصية، ومنها الاحتيال الإلكتروني، فضلاً عن الجرائم الإلكترونية ذات الطابع المالي، وأصبحت الجرائم الإلكترونية تشكل تحدياً قانونياً في شقها الموضوعي والإجرائي نظراً لصعوبة وصفها وإدراجها ضمن إطار التجريم في القوانين الجنائية لمعظم الدول، فضلاً عن صعوبة ملاحقتها والتصدي لها في ظل الأنظمة الإجرائية التقليدية المتعارف عليها، حيث يتطلب الأمر ضرورة تطوير التشريعات الجنائية الوطنية خاصة في شقها الإجرائي بما يتناسب مع طبيعة الجريمة الإلكترونية، أو من خلال سن قوانين للمواجهة الإجرائية تتضمن التحري والتحقيق وإثبات الجريمة الإلكترونية والحكم فيها من خلال أنظمة أو قواعد إجرائية مستحدثة

وقد دفع ذلك معظم الدول إلى تطوير قوانينها الإجرائية بإقرار وسائل وإجراءات تمثل قاسماً مشترك بين الجرائم الإلكترونية والجرائم التقليدية، وكذلك إقرار إجراءات خاصة تلائم الجرائم المستحدثة مثل الجرائم الإلكترونية وجرائم المعلومات، فضلاً عن ذلك قامت معظم الدول بإصدار قوانين خاصة لمكافحة الجرائم الإلكترونية أو جرائم تقنية المعلومات، والتي ضمنتها قواعد إجرائية خاصة تتفق والطبيعة الخاصة لهذه الجرائم.[1]

لم يعرف المشرع الإماراتي الجريمة الإلكترونية من خلال التشريعات المتتالية التي أصدرها بشأن الجريمة المعلوماتية، حتى في القانون رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، لكنه حدد الأفعال التي اعتبرها جرائم إلكترونية في المواد من (2 إلى 55) من نفس القانون، أما على الجانب الفقهي فقد تعددت وتباينت آراء الفقهاء حول تعريف الجريمة الإلكترونية وذلك وفقاً لزاوية النظر اليها (سلامة، 2016)، وخلاصة هذه التعريفات أن الجريمة الإلكترونية، هي " كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء المادي أو المعنوي على مصلحة يحميها القانون" (البشري، 2015)

توجد صور عديدة لارتكاب الجريمة الإلكترونية تختلف من مجتمع لآخر وفقاً لدرجة استخدام وسائل وشبكات الاتصالات والإنترنت، حيث تتزايد هذه الصور يوماً بعد يوم مع

(1) من هذه القوانين: قانون التجارة والمعاملات الإلكترونية التونسي لسنة 2000م، قانون المعاملات الإلكترونية الأردني عام 2001م، القانون الجزائري للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته لسنة 2009م.

تزايد الاعتماد على شبكات الاتصال والإنترنت في مجالات الحياة المختلفة، بوجه عام تقسم الجرائم الإلكترونية إلى قسمين، هما: الجرائم التي تستهدف العناصر غير المادية للنظام المعلوماتي، الجرائم التي ترتكب بواسطة النظام المعلوماتي مثل جرائم تستهدف الأشخاص، جرائم تستهدف الأموال، جرائم تستهدف أمن الدولة.

وقد منح ذلك الجريمة الإلكترونية مجموعة من الخصائص التي تميزها عن الجرائم التقليدية، هي: أنها جريمة مستحدثة، يتعدد الوصف القانوني لمحلها، ويتميز مرتكب الجريمة الإلكترونية بأنه عادة من ذوي الاختصاص والمعرفة في مجال المعلومات، وتتميز الجريمة الإلكترونية بأنها ذات بعد دولي، فضلاً عن صعوبة اكتشافها وإثباتها لأنها تتم من خلال نبضة إلكترونية خلال أقل من ثانية واحدة، يقوم الجاني بها بكل هدوء ودون ضجة، فضلاً عن أنها في الغالب لا تترك أثراً مادياً ظاهراً يمكن ضبطه، كما تقع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات في أية مرحلة من المراحل الاساسية لتشغيل نظام المعالجة الآلية للبيانات سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات، ولهذه الخاصية أثر كبير في تحديد قيام أو عدم قيام أركان الجريمة الإلكترونية، ففي حالة تخلف هذا الشرط تنتفي الجريمة الإلكترونية. (القطاوية، 2010)

مشكلة الدراسة:

تتمثل مشكلة هذه الدراسة فيما تتصف به الجريمة الإلكترونية من طبيعة وخصائص خاصة تتعلق بسهولة ارتكابها وتجاوزها حدود الزمان والمكان، وأنها تشكل تحدياً قانونياً خاصة في شقه الإجرائي لصعوبة ملاحقتها والتصدي لها في ظل الأنظمة الإجرائية التقليدية المتعارف عليها، وحاجتها إلى أنظمة وقواعد إجرائية مستحدثة للتحري والتحقيق الجريمة الإلكترونية، تتلاءم مع الخصائص والطبيعة الخاصة لهذه الجرائم، وبذلك يمكن صياغة مشكلة الدراسة في تساؤل رئيس، هو: **ما الآليات الإجرائية لضبط الجريمة الإلكترونية الواردة في قانون الإجراءات الجزائية الإماراتي والقوانين الأخرى السارية في دولة الإمارات بشأن مكافحة جرائم تقنية المعلومات؟**

ويتفرع عن هذا التساؤل الرئيسي عدة تساؤلات فرعية، هي:

1. ما الآليات الإجرائية التقليدية في التشريع الإماراتي ومدى كفايتها لضبط الجريمة الإلكترونية؟
2. ما أهم الآليات الإجرائية المستحدثة لضبط الجريمة الإلكترونية في التشريع الإماراتي؟

أهمية الدراسة:

تبدو أهمية هذه الدراسة من حداثة موضوعها في الجانب الإجرائي من القانون الجنائي، فلم يحظى هذا الموضوع بحظه من البحث والتحليل في إطار الفقه الجزائي، إذا أن أغلب الدراسات في مجال الجرائم الإلكترونية اقتصرت فقط على البحث في الجوانب الموضوعية لهذه الجرائم والتي تتضمن التجريم والعقوبة عليها، دون التصدي للجوانب الإجرائية في هذه الجرائم ذات الطبيعة الخاصة والتي تجعل من النظم الإجرائية التقليدية المتعارف عليها غير صالحة لضبط هذه الجرائم، ويمكن تقسيم أهمية هذه الدراسة وفقاً لما يلي:

الأهمية النظرية: وتتمثل في أنها تسلط الضوء على الآليات الإجرائية التقليدية المتعارف عليها لمواجهة الجرائم الإلكترونية، ومدى صلاحيتها لضبط والجريمة الإلكترونية، وكذلك الآليات الإجرائية المستحدثة لضبط الجريمة الإلكترونية

الأهمية العملية: فيما ستقدمه هذه الدراسة من نتائج تساهم في تقييم مدى فعالية النظام الإجرائي في التشريع الإماراتي لمواجهة الجريمة الإلكترونية، بالإضافة إلى تقديم مجموعة من التوصيات في ضوء ما سيتم التوصل إليه من نتائج

أهداف الدراسة:

تسعى هذه الدراسة إلى تحقيق الأهداف التالية:

1. التعرف على الآليات الإجرائية التقليدية لضبط الجريمة الإلكترونية.
2. التعرف على الآليات الإجرائية المستحدثة لضبط الجريمة الإلكترونية.
3. الوقوف على مدى صلاحية الآليات الإجرائية التقليدية والمستحدثة لضبط الجريمة الإلكترونية.

منهج الدراسة:

تعتمد هذه الدراسة على **المنهج الوصفي** كأصل من خلال الوقوف على الجوانب أو الآليات الإجرائية لضبط هذه الجرائم، بالاعتماد على المراجع والدراسات المتعلقة بموضوع الدراسة، فضلاً عن **المنهج التحليلي** من خلال تحليل المفاهيم والآراء الفقهية والقواعد القانونية في قوانين الإجراءات الجزائية والقوانين المتعلقة بمكافحة الجرائم الإلكترونية

تقسيم الدراسة:

سيتم عرض هذه الدراسة من خلال مبحثين، يتناول المبحث الأول إجراءات التحري والتحقيق التقليدية في الجريمة الإلكترونية، من خلال ثلاثة مطالب، هي: المعاينة الرقمية والخبرة، التفتيش المعلوماتي، ضبط الأدلة الرقمية، ويتناول المبحث الثاني إجراءات التحري والتحقيق المستحدثة في الجريمة الإلكترونية، من خلال مطلبين، هما: إجراءات تتعلق بالبيانات الإلكترونية المتحركة، إجراءات تتعلق بالبيانات الإلكترونية الساكنة

المبحث الأول: إجراءات التحري والتحقيق التقليدية في الجريمة الإلكترونية

تخضع الجريمة المعلوماتية لنفس خطوات سير الدعوي الجنائية وإجراءات وآليات البحث والتحري والتحقيق التي تمر بها الجرائم التقليدية، ومن أهم هذه الإجراءات المعاينة الرقمية والخبرة، والتفتيش المعلوماتي، وضبط الأدلة الرقمية (حجازي، 2012)، ونسعى من خلال هذا المبحث التعرف على مدى كفاية أو فعالية هذه القواعد الإجرائية في ضبط الجريمة المعلوماتية ملاحقة مرتكبيها من خلال ثلاث مطالب، هي: المعاينة الرقمية والخبرة، التفتيش المعلوماتي، ضبط الأدلة الرقمية

المطلب الأول: المعاينة الرقمية والخبرة

تعد المعاينة والخبرة من الإجراءات العامة التي كرسها المشرع والتي تمر بها أي جريمة، لكنهما يمثلان تحدياً كبيراً بصدد تطبيقهما لضبط الجريمة المعلوماتية، وهذا ما نسعى للوقوف عليه من خلال هذا المطلب وذلك وفقاً لما يلي:

الفرع الأول: المعاينة الرقمية:

المعاينة في مجال الإجراءات الجنائية هي إجراء من إجراءات التحقيق يقوم به المحقق بهدف الكشف عن غموض الجريمة من خلال الفحص المادي أو الحسي لجميع آثار الجريمة والتعرف على كيفية وقوعها (الشوابكة، 2013)، وتتضمن إثبات والتحفظ على الأشياء والأدوات والأشخاص الموجودة في مسرح الجريمة ورفع كافة الآثار التي خلفتها الجريمة من دماء وبصمات وحالة الأشخاص مثل المتهم والمجني عليه والشهود، وغير ذلك من الأمور التي تفيد التحقيق في الجريمة.[1]

أي أن المعاينة ذات أهمية كبيرة لكشف غموض غالبية الجرائم التقليدية من خلال مساهمتها في العثور على الاثار المادية للجريمة وإثباتها والتحفظ عليها، ومن ثم فحص

(1) تنص المادة (71) من قانون الإجراءات الجزائية الاتحادي الإماراتي على أن " ينتقل عضو النيابة العامة إلى أي مكان ليثبت حالة الأشخاص والأماكن والاشياء المتصلة بالجريمة وكل ما يلزم إثبات حالتها ... ".

مدى صلاحيتها كدليل للإثبات، لكن المعاينة بهذا المفهوم تواجه تحديات جوهرية عديدة في مجال الجرائم المعلوماتية، أهمها عدم وجود آثار مادية للجرائم المعلومات وذلك لإمكانية التلاعب في البيانات المتعلقة بالجريمة ومحوها من قبل الجناة، فضلاً عن تواجد أعداد كبيرة من الأشخاص في مسرح الجريمة أثناء ارتكابها إلى أن يتم الكشف عنها، الأمر الذي يجعل من المعاينة أمراً شديد الصعوبة ويضعف من أهميتها كدليل للإثبات. (مراد، 2018)

أولاً: مفهوم المعاينة الرقمية: ينصرف مفهوم المعاينة للجريمة المعلوماتية إلى معاينة الآثار المادية والبصمات الإلكترونية التي قد يتركها مستخدم شبكة المعلومات أو شبكة الإنترنت مثل الرسائل التي يرسلها أو التي يتلقها وكافة الاتصالات أو المحادثات التي قام بها أجرها من خلال الحاسب الآلي أو من خلال شبكات الاتصالات والمعلومات، لكن يجب مراعاة مبدأ الخصوصية المعلوماتية للأفراد وكذلك مبدأ الشرعية بحيث لا يتم البحث في المحتوى المعلوماتي إلا في حدود السلطات المخولة لجهات التحقيق. (العازمي، 2016)

ثانياً: آلية تنفيذ المعاينة الرقمية: تبدأ المعاينة للجرائم المعلوماتية من خلال المعاينة للمسرح المادي التقليدي من خلال انتقال المحقق إلى المكان الذي توجد به الأجهزة والمكونات المادية للحاسب الآلي ومستلزماته وملحقاته ووسائل الاتصال بالشبكة المعلوماتية وجميع الأشياء والمعدات والأدوات الأخرى التي تصلح أن تكون دليل إلكتروني مثل وسائط التخزين وغيرها، ويتطلب ذلك سرعة الانتقال إلى هذا المسرح المادي قبل أن يتمكن الجناة من التخلص منها بإخفائها أو التخلص منها, وبعد معاينة المسرح المادي للجريمة المعلوماتية يتم معاينة المسرح الإلكتروني الذي يتضمن برامج وبيانات الحاسب الآلي. (السعيد، 2019)

لكن التساؤل الذي يتبادر إلى الذهن في هذه الصدد هو، يتعلق بإمكانية معاينة الجريمة المعلوماتية وإثباتها وفقاً لما تقضي به القواعد الإجرائية العامة التي تحددها قوانين الإجراءات الجزائية التي سنت في الأساس لضبط الجريمة التي لها وجود مادي محسوس في العالم الخارجي حيث تقضي هذه القواعد على المحقق أن يجمع بالأشياء والأوراق والمعدات وغيرها من العناصر المادية التي يتم ضبطها في مسرح الجريمة ويحفظها في حرز مغلق

وبصدد المعاينة للجريمة المعلوماتية وفقاً للقواعد الإجرائية العامة الواردة في قوانين الإجراءات الجزائية، تبدو عقبة أساسية تتعلق بأن الجريمة المعلوماتية عادة ما يتم ارتكابها في بيئة افتراضية هي عبارة عن نبضات إلكترونية وبيانات ونظم معلومات تتسم بالخصوصية والحساسية الشديدة، أي أن الجريمة المعلوماتية وهي التي تقع على بيانات أو

برامج الحاسب الآلي أو بواسطتها تثير معاينتها وفقاً للقواعد الإجرائية التقليدية الكثير من التحديات تتمثل في قلة الآثار المادية التي تخلفها هذه الجرائم، فضلاً عن اتساع مسرح الجريمة وتواجد عدد كبير من الاشخاص على هذا المسرح خلال ارتكاب الجريمة ووجود فترة زمنية بين ارتكاب الجريمة واكتشافها الأمر الذي يمنح الفرصة للجناة في إخفاء أو إزالة الأثار المادية الظاهرة للجريمة المعلوماتية، الأمر الذي يتطلب أن يكون المحقق في الجرائم المعلوماتية ذو خبرة معلوماتية يستطيع من خلالها التعامل مع تعقيدات البيئة الرقمية، وما تتضمنه من أشياء أو عناصر يصعب ضبها وربطها في حرز مغلق، فضلاً عن أن المعاينة الرقمية لهذه الجرائم تتطلب إجراءات وضوابط خاصة سواء قبل وأثناء وبعد المعاينة.

الفرع الثاني: الخبرة في مجال ضبط الجريمة المعلوماتية:

أولاً: تعريف الخبرة وأهميتها: تعد الخبرة إجراء من إجراءات التحقيق يقوم بها اشخاص تتوافر لديهم معرفية فنية متخصصة في مجال معين بهدف استخلاص أدلة تعين القضاء على التوصل للحقيقة، فهي بمثابة استشارة فنية يلجأ إليها قاضي التحقيق في المسائل الفنية التي تتطلب معرفة فنية أو علمية لا تتوافر لديه (ابراهيم، 2017)، وللخبرة في مجال الدعوى الجنائية دور بالغ الأثر من خلال تقديم المعرفة الفنية المتخصصة لجهات الضبط والتحقيق والقضاء، لذلك فقد حرص المشرع الإماراتي على تنظيم عمل الخبرة في مجال الدعوى الجزائية من خلال المواد من المادة (96) إلى المادة (98) من قانون الإجراءات الجزائية الإماراتي، فقد نصت المادة (96) منه على أن " إذا اقتضى التحقيق الاستعانة بطبيب أو غيره من الخبراء لإثبات حالة من الحالات كان لعضو النيابة العامة أن يصدر أمراً بندبه ليقدم تقريراً عن المهمة التي يكلف بها..."

ويتبين من النص السابق أن الاستعانة بالخبير في الأمور الفنية البحتة هو من الأمور الهامة والتي تعين سلطات التحقيق والقضاء، وتبدو الضرورة القصوى للحبرة في مجال الجرائم المعلوماتية لما تتضمنه من مسائل فنية شديدة التخصص والتعقيد، يصعب على المحقق القيام بها، حيث يتطلب ذلك معرفة فنية وعلمية عميقة للكشف عن الأدلة الرقمية وتحليلها وتحديد خصائصها على اختلاف صورها سواء كانت مستندات رقمية أو برامج أو تطبيقات أو صور أو أصوات، فضلاً عما للخبرة دور هام في إصلاح هذه الأدلة الرقمية، وجمع كافة الآثار الرقمية والتأكد من مدى العبث بها أو تعديلها، كما يمتد دور الخبير في مجال الجرائم المعلوماتية إلى حماية وتامين الأنظمة المعلوماتية من استمرار تهديدها واستهدافها (ابراهيم، 2008)، ولم يضع المشرع الإماراتي نصوص قانونية خاصة لتنظيم أعمال الخبرة في مجال الجرائم المعلوماتية في القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم المعلوماتية، واكتفي فقط بالنصوص العامة لتنظيم الخبرة

والواردة في قانون الإجراءات الجرائية.[1]

ثانياً: ضوابط الخبرة: لأهمية الخبرة في إثبات الجريمة فقد اجتهد الفقه القانوني في تحديد أركانها الشكلية والموضوعية، ويتمثل ركنها الشكلي في التخصص والعلم الذي يجب توافره في الخبير حيث يجب أن يجمع الخبير بين العلم المتخصص والخبرة العملية في مجاله، أما الركن الموضوعي والذي يتعلق بالحرية العملية التي يجب توافرها للخبير والتي تمكنه من استخدام علمه وخبراته (موسى، 2015)، كما حرصت غالبية التشريعات تحديد ضوابطها وشروطها، ومن هذه الشروط ما يتعلق بالخبير نفسه فيشترط أن يتم اختياره من قائمة الخبراء المحدد أسمائهم في الجداول المعدة مسبقا، وفي حالة عدم تضمن الجدول الخبراء المتخصصين في مجال الخبرة المطلوبة، يجوز لجهات التحقيق استثنائياً اختيار خبراء غير مقيدين في الجدول، وقد نصت المادة (97) من قانون الإجراءات الجزائية الإماراتي على أن " إذا كان الخبير غير مقيد اسمه في الجدول وجب أن يحلف أمام عضو النيابة العامة يميناً بأن يؤدي عمله بالصدق والأمانة"

ونري في هذا الصدد أن المشرع الإماراتي قد أتاح الاستعانة بخبراء غير مقيد أسمائهم في الجدول، كما أنه لم يضع شروط تحدد جنسية الخبير ومكان وجوده، وبذلك فإن المشرع الإماراتي يكون قد وسع نطاق الاستعانة بالخبرة في مجال الجرائم المعلوماتية من خلال السماح بالاستعانة بخبراء دوليين من خارج الدولة في العالم الافتراضي العالمي لهذه الجرائم.

ومن شروط الخبرة ما يتعلق بتقرير الخبرة فيجب على الخبير بعد الانتهاء من عمله وفقاً للأسس والقواعد العلمية والفنية أن يعد تقريراً يتضمن خلاصة ما تم التوصل إليه من نتائج، كما يشترط أن يقدم الخبير تقريره خلال المدة المحددة له في امر الندب، وإذا لم يقم بذلك يجوز استبدال الخبير ما لم يقدم طلباً بتمديد هذه المهلة (المؤمني، 2010)، وفي هذا الصدد نصت المادة (98) من قانون الإجراءات الجزائية الإماراتي على أن " يقدم الخبير تقريره كتابة ويحدد عضو النيابة العامة للخبير ميعاداً لتقديمه وله أن يستبدل به خبيراً أخر إذا لم يقدم التقرير في الميعاد المحدد أو استدعى التحقيق ذلك"

(1) بعض التشريعات لم تكتفي بالنصوص التقليدية المنظمة للخبرة، بل أنها اتجهت إلى سن نصوص قانونية خاصة تنظم أعمال الخبرة في مجال الجرائم المعلوماتية ومثال ذلك التشريع البلجيكي من خلال المادة (88) من قانون الجرائم المعلوماتية الصادر في 23 /11 /2000م والتي تنص على أن " يجوز للقاضي والشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق"، قورة، نائلة عادل (2010). جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، بيروت، ص 94.

ومما سبق يتبين أنه إذا كانت تقارير الخبرة ذات أهمية في مجال الجرائم التقليدية فهي أكثر أهمية في مجال الجرائم المعلوماتية لأنها تتضمن جوانب تقنية وفنية معقدة تتطلب وجود ملاحق وآليات توضيحية ورسومات لتوضيح وتحليل واستخلاص النتائج والأدلة الرقمية.

المطلب الثاني: التفتيش المعلوماتي

التفتيش بوجه عام هو أحد إجراءات البحث والتحقيق يهدف إلى جمع أدلة مادية تساهم في كشف الحقيقة، يتضمن البحث في مستودع سر المتهم أو حياته الخاصة، كما يتضمن الجبر والإكراه حيث يتم تنفيذه جبراً إذا لم يوافق الشخص على الخضوع له طواعية، لذلك فقد تضمنت قوانين الإجراءات الجزائية قواعد تقضي بعدم التفتيش إلا بموجب القانون بأمر كتابي من السلطة المختصة.(1)

الفرع الأول: طبيعة التفتيش المعلوماتي ومحله:

اولاً: تعريف التفتيش المعلوماتي: عرفه المجلس الأوروبي بأنه " إجراء يتيح جمع الأدلة المسجلة أو المخزنة بشكل قانوني" (حسني، 2016)، ويتبين من هذا التعريف أن مفهوم التفتيش في مجال الجريمة المعلوماتية لا يختلف عن مدلوله في قوانين الإجراءات الجزائية، فهو إجراء من إجراءات التحقيق تقوم به سلطة مختصة من خلال الدخول إلى نظم المعالجة الآلية للمعلومات التي تتكون من مكونات مادية مثل الحاسبات الآلية والهواتف الذكية وأجهزة أخرى، ومكومات غير مادية مثل البرامج والتطبيقات المختلفة ومواقع التواصل والتخاطب، وما تتضمنه من مدخلات وبيانات ومخرجات مخزنة، والبحث فيها عن أفعال غير مشروعة ونسبتها للمتهم، لكن التفتيش المعلوماتي يتضمن عدة تحديات تتعلق بقدرة الجناة على التخلص من البيانات أو المعلومات المخزنة أو المنقولة المطلوب تفتيشها، أو تشفيرها من خلال برامج أو تقنيات معينة أو حجبها برقم سري، فضلاً عن التحديات التي تتعلق بالمساس بالخصوصية عندما يتعلق الأمر ببيانات أو معلومات محل الحماية القانونية أو لأنها تتعلق بجهات أخرى، وذلك عندما يمتد نطاق التفتيش المعلوماتي إلى أنظمة معلوماتية أخرى غير المشتبه بها خاصة في ظل انتشار الشبكات الداخلية والمحلية والإقليمية والدولية، أي أن التفتيش المعلوماتي لابد أن يتميز بخصائص معينة من

(1) تنص المادة (51) من قانون الإجراءات الجزائية الإماراتي على أنه " لمأمور الضبط القضائي أن يفتش المتهم في الأحوال التي يجوز فيها قانوناً القبض عليه، ويجري تفتيش المتهم بالبحث عما بجسمه أو ملابسه أو أمتعته من آثار أو أشياء تتعلق بالجريمة أو تكون لازمة للتحقيق فيها"، وكذلك تنص المادة " لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم بغير إذن كتابي من النيابة العامة ما لم تكن الجريمة متلبساً بها وتتوفر أمارات قوية على أن المتهم بخفي في منزله أشياء أو أوراق تفيد كشف الحقيقة ويتم تفتيش منزل المتهم وضبط الأشياء والأوراق على النحو المبين بهذا القانون.

حيث ضوابطه الموضوعية والشكلية (إبراهيم، 2017)، الأمر الذي تساؤلاً حول إمكانية تطبيق القواعد التقليدية للتفتيش الواردة في قوانين الإجراءات الجزائية على الجرائم المعلوماتية فيما يتعلق بمعايير الضبط المعلوماتي ومعايير التحريز والخصوصية

ثانياً: محل التفتيش المعلوماتي: قد يقع التفتيش المعلوماتي على المكونات المادية للنظام المعلوماتي مثل الحواسيب الآلية والأجهزة الملحقة بها من طابعات وماسحات ضوئية وأي أجهزة طرفية أخرى، وقد يقع التفتيش المعلوماتي على المكونات غير المادية للنظام الالكتروني مثل البرامج والتطبيقات المختلفة، وقد يقع التفتيش المعلوماتي على الشبكات المتصلة بالحاسب الآلي، وسوف نفصل ذلك فيما يلي:

1. **تفتيش المكونات المادية للحاسب الآلي:** لا يتضمن تفتيش المكونات المادية للحاسب الآلي مشكلة تتعلق بإمكانية خضوعها للتفتيش ويتوقف ذلك على طبيعة المكان التي توجد فيه هذه المكونات المادية، فإذا كان هذا المكان عاماً فلا يجوز تفتيشه إلا وفقاً للقيود والضمانات التي يقرها القانون الخاصة بتفتيش الأشخاص، أما إذا كان هذا المكان خاصاً فلا يجوز تفتيشه إلا وفقاً للقيود والضمانات التقليدية التي يقرها القانون.
2. **تفيش المكونات غير المادية للحاسب الآلي:** لقد ثار بشأنها خلاف فقهي فيما يتعلق بصلاحية أن تكون محل للتفتيش وذلك بسبب طبيعتها المعنوية حيث أنها تتخذ شكل النبضات والاشارات الإلكترونية غير المحسوسة، حيث يتعارض ذلك مع الهدف من التفتيش وهو الحصول على أدلة مادية، حيث يرى بعض الفقه أن تفتيش هذه المكونات المعنوية بتطلب أحكام خاصة تلائم الطبيعة غير المحسوسة لهذه المكونات، (أبو راس، 2016) وعلى جانب أخر يرى بعض الفقه أن هذه المكونات غير المادية تصلح للتفتيش وفقاً للقواعد الإجرائية الواردة في قوانين الإجراءات الجزائية والتي تمنح سلطات التحقيق إمكانية ضبط أي شيء ضروري لجمع الأدلة وضمن ذلك المكونات غير المادية للحاسب الآلي سواء بيانات أو معلومات يتم معالجتها وتحزينها في الأنظمة الالكترونية أو أي تطبيقات أو برامج تستخدم لهذه المعالجة. (السعيد، 2019)

أما على الجانب التشريعي في الإمارات العربية المتحدة فقد أشار المشرع بصورة غير مباشرة إلى إمكانية التفتيش للمكونات المعنوية للحاسب الآلي من خلال المادة (72) من قانون الإجراءات الجزائية الإماراتي التي تنص على أن " لعضو النيابة العامة تفتيش منزل المتهم بناء على تهمة موجهة إليه بارتكاب جريمة أو بالاشتراك بها، وله أن يفتش أي مكان ويضبط فيه أي أوراق أو اسلحة وكل ما يحتمل أنه استعمل في ارتكاب الجريمة

أو نتج منها أو وقعت عليه وكذلك كل ما يفيد في كشف الحقيقة"، وكذلك من خلال المادة (75) من نفس القانون التي تنص على أنه "... يجوز 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 استوجب مقتضيات التحقيق ذلك ".

ويرى البعض أن هذه النصوص السابقة غير كافية للدلالة القاطعة على جواز وإمكانية تفتيش المكونات المعنوية للحاسب الآلي حيث لم يتم النص صراحة على ذلك (المؤمني، 2010)، ويرى البعض الأخر أن هذه النصوص تدل على جواز التفتيش للمكونات المعنوية للحاسب الآلي، ويفهم ذلك من خلال عبارة (كل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج منها أو وقعت عليه وكذلك كل ما يفيد في كشف الحقيقة)، كما يفهم ذلك أيضاً من خلال المادة (75) بالقياس على ما أقره المشرع من جواز مراقبة وتسجيل المحادثات اللاسلكية (حسني، 2016)، ومن جانبنا نرى أن النصوص الواردة في قانون الإجراءات الجزئية الإماراتي فيما يتعلق بالتفتيش للمكونات المعنوية للحاسب الآلي غير حاسمة أو غير صريحة، لكن بالبحث في نصوص القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية تبين أن المشرع الإماراتي ومن خلال المادة (65) منه قد أقر بمشروعية تفتيش المكونات المعنوية للحاسب الآلي، حيث تنص هذه المادة على أنه " يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الالكترونية أو النظام المعلوماتي أو برامج الحاسب الآلي أو من أي وسيلة لتنقية المعلومات حجية الأدلة الجنائية المادية في الاثبات الجنائي"، ويدل هذا النص بشكل قاطع على مشروعية تفتيش المكونات المعنوية للحاسب الآلي.

3. **تفتيش شبكات الحاسب الآلي:** قد يكون تفتيش هذه الشبكات في نفس الدولة التي ينتمي إليها أو التي تحققت فيها الجريمة الإلكترونية أو في عدة دول، ويمكن تفصيل ذلك وفقاً لما يلي:

أ. **التفتيش المعلوماتي في شبكة الحاسب الآلي في نفس الدولة:** توجد بعض التحديات الناتجة عن عدم صلاحية النصوص التقليدية الواردة في بعض قوانين الإجراءات الجزئية والتي قد تمنع تفتيش مواقع أو بيانات لأشخاص أخرين على نفس النظام المعلوماتي أو لشبكة معلومات أخرى في نفس الدولة، لكن بعض الفقه القانوني يقول بجواز امتداد التفتيش المعلوماتي إلى سجلات البيانات التي توجد في موقع أخر في نفس الشبكة. (1)

(1) أخذ المشرع الألماني بهذا النهج من خلال قانون الإجراءات الجنائية الألماني، كما اتجهت بعض التشريعات إلى

ب. **التفتيش المعلوماتي في شبكة الحاسب الآلي خارج حدود الدولة:** قد يتطلب التفتيش المعلوماتي أن يكون عابراً للحدود الوطنية بأن يمتد إلى شبكات أخرى خارج الإقليم الوطني للدولة، ويمثل ذلك تحدياً قانونياً حيث يتعارض مع مبدأ سيادة كل دولة على اقليمها، حيث لا يتم التفتيش إلا من خلال اتفاقيات دولية أو إقليمية أو ثنائية، أو على الأقل الحصول على إذن من الدولة المراد امتداد التفتيش إليها، وبخلاف ذلك يكون التفتيش المعلوماتي الممتد إلى شبكات في دول أخرى يمثل خرقاً لسيادة الدولة الأخرى. (شاهين، 2016)

أي أن التحدي الذي يعترض التفتيش المعلوماتي العابر للحدود يمكن التغلب عليه من خلال آليات التعاون الدولي سواء على المستوى الأمني والفني والقضائي في إطار الاتفاقيات الدولية والإقليمية والثنائية بين الدول أو في إطار المعاملة بالمثل.

الفرع الثاني: ضوابط التفتيش المعلوماتي:

لقد اتجهت التشريعات الإجرائية إلى وضع مجموعة من الضوابط أو الشروط أو الضمانات الشكلية والموضوعية للتفتيش الجنائي لتعلقه بحقوق وحريات الأفراد وحرمه حياتهم الخاصة ومسكنهم، وسوف نعرض هذه الضمانات ومدى ملاءمتها أو صلاحيتها لطبيعة وخصائص التنفيش المعلوماتي، وفقاً لما يلي:

أولاً: الضوابط أو الضمانات الموضوعية للتفتيش المعلوماتي: وهي تتضمن الشروط الواجب توافرها في التفتيش الصحيح والتي تتعلق بما يلي: (البشري، 2008)

1. **سبب التفتيش:** لا يتم التفتيش إلا بصدد جريمة فعليه سواء جناية أو جنحة يوجه الاتهام فيها لشخص معين بناء على أدلة أو قرائن قوية تدل على تورط هذا الشخص في هذه الجريمة [1]، ويبطل التفتيش ولا يكون مشروعاً في حالة عدم وجود السبب الذي يبرر المساس بحقوق الفرد وحرياته وحرمة حياته الشخصية ومسكنه.
2. **محل التفتيش المعلوماتي:** حيث يجب لصحة ومشروعية التفتيش إن يكون محل معين، وهو في التفتيش المعلوماتي يتمثل في المكونات المعنوية أو المادية للنظام المعلوماتي. ويجب أن يكون هذا المحل معيناً تعييناً نافياً للجهالة، وألا يكون محظور

جواز امتداد التفتيش المعلوماتي إلى نظام معلوماتي أخر في نفس الدولة، مثل قانون التحقيق الجنائي البلجيكي لسنة 2000م، والذي تنص المادة (88) منه على أن " يمتد التفتيش المعلوماتي إلى نظام معلوماتي أخر في الدولة إذا حالة الضرورة لكشف الحقيقة، وإذا وجدت مخاطر تتعلق بضياع الأدلة".

(1) المادة (72) من قانون الإجراءات الجزئية الإماراتي

تفتيشه، فلا يجوز تفتيش أجهزة الحاسب أو الهواتف المحمولة الخاصة بكل أفراد عائلة المتهم، كذلك لا يجوز تفتيش الفئات التي تتمتع بالحصانة مثل أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية، وكذلك مكاتب المحامين وسياراتهم ومساكنهم.[1]

3. **السلطة المختصة بالتفتيش المعلوماتي:** فلا يكون التفتيش المعلوماتي صحيحاً إلا إذا صدر عن السلطة المختصة بالتفتيش والبحث عن أدلة ارتكاب الجريمة المعلوماتية التي تتطلب مهارة وخبرة فنية خاصة من أجل تتبع والحصول والحفاظ على الأدلة المعلوماتية من التلف أو التعديل، ويمكن في هذا الصدد الاستعانة بالخبراء المختصين بناء على طلب السلطات المختصة بالتحقيق.

ثانياً: الضوابط أو الضمانات الشكلية للتفتيش المعلوماتي: بالإضافة إلى الضوابط أو الشروط الموضوعية سابقة الذكر، توجد عدة ضوابط شكلية أو أخرى يجب مراعاتها عند القيام بالتفتيش المعلوماتي والتي تتعلق بالحقوق والحريات الشخصية للفرد، وأهم هذه الضمانات ما يلي:

1. **الحدود المكانية للتفتيش المعلوماتي:** إذا كانت المكونات المادية للحاسب الآلي في حوزة المتهم، عند ذلك فهي تعد من توابع المتهم حتى لو لم تكن مملوكة له، ويخضع تفتيشها لضمانات وشروط تفتيش الأشخاص الواردة في قوانين الإجراءات الجزائية، أما في حالة وجود هذه المكونات في مسكن المتهم أو في أي مكان له حرمة خاصة عند ذلك يخضع تفتيش هذه المكونات لشروط تفتيش المساكن الواردة في قوانين الإجراءات الجزائية، لكن الطبيعة الخاصة للمكونات المعنوية للحاسب الآلي وشبكات الإنترنت تتطلب نصوص إجرائية جديدة تتعلق بامتداد نطاق التفتيش المعلوماتي إلى مواقع أو بيانات لأشخاص أخرين على نفس النظام المعلوماتي أو لشبكة معلومات أخرى في نفس الدولة أو في دولة أخرى. (خليفة، 2016)

2. **الحدود الزمنية للتفتيش المعلوماتي:** لقد اختلفت التشريعات الإجرائية بصدد تحديد وقت القيام بالتفتيش، فمن هذه التشريعات ما حدد وقتاً محدداً للتفتيش مثل قانون الإجراءات الجنائية الفيدرالي الأمريكي الذي حده ما بين الساعة السادسة صباحاً والعاشرة مساءاً (قورة، 2010)، وهناك بعض التشريعات الإجرائية الأخرى لم تحدد وقتاً محدداً للتفتيش ومنها قانون الإجراءات الجنائية البلجيكي (أبو الدهب، 2015)، وكذلك التشريع الإماراتي، حيث لم يرد نص في قانون الإجراءات

(1) المواد ((75 – 78) من قانون الإجراءات الجزئية الإماراتي.

الجزائية الإماراتي بشأن تحديد وقت معين للتفتيش، وبذلك يمكن القيام به في أي وقت من النهار أو الليل، ونري أن نهج المشرع الإماراتي في هذا الصدد يعتبر مناسباً لطبيعة الجرائم المعلوماتية التي لسرعة وسهولة محو وإزالة آثارها.

3. **القيام بإجراءات التفتيش بحضور المتهم أو من ينوب عنه:** من الضمانات الشكلية للتفتيش عدم جواز إجراء التفتيش إلا بحضور المتهم أو من ينوب عنه، وقد نصت المادة (59) من قانون الإجراءات الجزائية الإماراتي على أنه " يجرى التفتيش بحضور المتهم أو من ينوب عنه كلما أمكن ذلك، وإلا تم بحضور شاهدين ويكون هذان الشاهدان بقدر الإمكان من أقاربه الراشدين أو من القاطنين معه بالمنزل أو من جيرانه ويتثبت ذلك بالمحضر".

ومن خلال النص السابق يتبين أن المشرع الإماراتي قد أجاز عدم حضور المتهم أو من ينوب عنه للتفتيش، ويفهم ذلك من عبارة (كلما أمكن ذلك) الواردة في هذه المادة، ونرى أن هذا الاتجاه ملائم ويحقق متطلبات السرعة في التنفيش المعلوماتي خاصة فيما يتعلق بالمكونات المعنوية للحاسب الآلي

4. **تحرير محضر التفتيش:** من الضوابط او الضمانات الشكلية للتفتيش أن يحرر محضر يسجل فيه كافة المعلومات بالتحقيق وما تم التوصل إليه من أدلة، وأن يتضمن كافة الإجراءات المتخذة بشأن كل الوقائع المراد إثباتها، ولم يتطلب المشرع شروط خاصة لهذا المحضر بخلاف ما تتطلبه القواعد العامة بأن يكون مكتوب باللغة الرسمية، ويتضمن تاريخ تحرير المحضر وتوقيع محرره. (البكري، 2016)

5. **إصدار إذن بالتفتيش:** من الضوابط الشكلية للتفتيش الجنائي وجوب استصدار إذن به؛ إذ تنص المادة (53) من قانون الإجراءات الجزائية الإماراتي على أنه " لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم يغير إذن كتابي من النيابة العامة ما لم تكن الجريمة متلبساً بها وتتوافر أمارات قوية على أن المتهم يخفي في منزله أشياء أو أوراق تفيد كشف الحقيقة ويتم تفتيش منزل المتهم وضبط الأشياء والأوراق على النحو المبين بهذا القانون ".

ومن هذا النص يتبين أن المشرع الإماراتي لم ينص صراحة على ضرورة استصدار إذن لتفتيش المكونات المعنوية للحاسب الآلي، وهذا يعني أن يطبق هذا النص بشأن التفتيش المعلوماتي بشقه المادي والمعنوي.

المطلب الثالث: ضبط الأدلة الرقمية

من أهم الآثار المترتبة على التفتيش المعلوماتي بشقيه المادي والمعنوي أن يتم ضبط الأدلة المتحصل عليها، وبقصد بالضبط أن يتم حجز المعطيات المتحصل عليها من التفتيش بوضع اليد على كل ما تتصل بالجريمة للوصول إلى مرتكبيها وتقديمهم للمحاكمة. (المؤمني، 2010)

الفرع الأول: طبيعة ضبط الأدلة الرقمية:

يثار بشأن ضبط الأدلة في الجرائم المعلوماتية تساؤلاً هام يتعلق بمدى إمكانية هذا الضبط، خاصة أن الأشياء محل الضبط في الجرائم المعلوماتية قد تكون مكونات مادية أو مكونات معنوية، ولا يمثل ضبط المكونات المادية للحاسب الآلي تحدياً إجرائياً حيث يسري بشأنها القواعد الإجرائية التقليدية الواردة في قانون الإجراءات الجزائية، أما ضبط المكونات المعنوية المتمثل في البيانات والمعلومات والبرامج فهي محل جدل فقهي حول صلاحية ضبطها، وقد اتجه غالبية الفقه إلى هذه المكونات المعنوية تصلح محلاً للضبط على اعتبار أنها تسجل وتحفظ على مكونات مادية يمكن ضبطها، ففي حالة العثور على دليل رقمي يمكن تفريغه على وسائط تخزين مختلفة لحفظه، كما يمكن تفريغه على الأوراق ويتم ذلك وفقاً لمحضر يثبت فيه كافة تفصيل الأدلة الرقمية التي تم ضبطها. (حسني، 2016)

لكن في الواقع التطبيقي فإن ضبط الأدلة الرقمية أو المكونات المعنوية في الجريمة المعلوماتية يواجه عدة تحديات فنية أهمها كبر حجم البيانات أو الشبكات التي توجد عليها البيانات والمعلومات المراد ضبطها، فضلاً عن أنه أحياناً قد يترتب على الضبط المعلوماتي المساس بحق الخصوصية وحرمة الحياة الخاصة للأشخاص، الأمر الذي يتطلب إقرار ضمانات خاصة لحماية هذه الخصوصية، وقد اتجهت قوانين الإجراءات الجنائية في بعض الدول إلى وضع قواعد إجرائية لضبط الأدلة الرقمية ومن هذه القوانين قانون الإجراءات الجنائية البلجيكي الذي منح للنيابة العامة سلطة الأمر بغلق البيانات لمنع الوصول إليها للحفاظ عليها، الحصول على نسخة منها من لدى الأشخاص الذين يستخدمون النظام المعلوماتي لمقارنتها مع النسخة المستخرجة من جهاز المتهم، كما أجاز لسلطات التحقيق سحب هذه البيانات من الجهاز في حال إذا كانت محل للجريمة أو من نتائجها أو إذا كانت تمثل تعدي على الآداب العامة والنظام العام، أو إذا كانت تمثل خطراً على الأنظمة المعلوماتية أو المعلومات المتداولة أو المخزنة عليها. (أبو الدهب، 2015)

الفرع الثاني: ضمانات ضبط الأدلة الرقمية:

يتطلب ضبط الأدلة الرقمية في الجرائم المعلوماتية عدد من الضمانات، أهمها: (أبو الذهب، 2015)

1. الحصول على إذن من السلطات المختصة للتفتيش والضبط، على أن يتضمن هذا الأذن تحديداً للنظام المزمع تفتيشه بدقه وعنوان المتهم واسمه والحيز الذي يقوم بالدخول عليه.
2. أن يتوفر لدى القائم بالضبط المعلوماتي القدرة الفنية على التعامل من الدليل الرقمي والمحافظة عليه من التكلف أو الخذف، وأن يكون على دربة فنية متخصصة وقواعد تحرير الدليل الرقمي المضبوط.
3. نسخ الأدلة الرقمية على وسائط التخزين المناسبة بأن تكون قابلة للحجز.
4. وضع هذه الأدلة في أحراز وفقاً لما يقره قانون الإجراءات الجزائية.
5. العمل الدائم على الحفاظ على الأدلة الرقمية وعدم تعريضها لمجالات كهربائية أو مغناطيسية أو مناخية تؤثر عليها.
6. يمكن استخدام أساليب أو سائل تقنية مختلفة لتشكيل أو أعادة ترتيب معطيات الدليل الرقمي بحيث يكون قابل للاستغلال والاستفادة منه في التحقيق والإثبات بشرط ألا يؤدي ذلك إلى المساس بمحتوى أو مضمون الدليل الرقمي.

وبالنظر إلى القواعد الإجرائية الواردة في قانون الإجراءات الجزائية الإماراتي المتعلقة بالتفتيش وضبط الأدلة، وهي المواد من (53 إلى 64) من هذا القانون، تدور حول ضبط الأشياء أو الأوراق أو العناصر المادية التي يمكن وضعها في حرز مغلق مختوم بالشمع الأحمر، وبالتالي فإن هذه النصوص لم تشير من قريب أو بعيد إلى أي أدلة أو عناصر غير مادية مثل المكونات المعنوية أو الأدلة الرقمية، وبذلك نرى أن هذه النصوص المشار إليها الواردة في قانون الإجراءات الجزائية الإماراتي، وإن كانت تلاءم ضبط المكونات المادية للحاسب الآلي، إلا أنها قد لا تكون كافية لضبط المكونات المعنوية أو الأدلة الرقيمة، وبذلك نرى أن ضبط المكونات المعنوية أو الأدلة الرقمية يتطلب صياغة عدد من القواعد الإجرائية الخاصة التي تتعلق بضبطها واستخلاصها وتحليلها وضوابط التعامل معها بوجه عام

المبحث الثالث: إجراءات التحري والتحقيق المستحدثة في الجريمة الإلكترونية

لقد اتجهت بعض الدول إلى تعديل أو إضافة نصوص تتضمن قواعد وضوابط تحكم وتنظم التحري والتحقيق في الجرائم المعلوماتية، في حين اتجهت دول أخرى إلى صياغة قوانين خاصة للمواجهة الموضوعية والإجرائية للجرائم المعلوماتية، وسوف نسعى من خلال هذا المبحث للتعرف على أهم الإجراءات المستحدثة للتحري والتحقيق فيها من خلال مطلبين، هما: إجراءات تتعلق بالبيانات الإلكترونية المتحركة، إجراءات تتعلق بالبيانات الإلكترونية الساكنة

المطلب الأول: إجراءات تتعلق بالبيانات الإلكترونية المتحركة

لقد أدى التطور الهائل في تكنولوجيا الاتصالات والمعلومات سهولة وسرعة حركة وتداول المعلومات، ويقصد بالإجراءات المتعلقة بالبيانات المتحركة تلك التي تتعلق بمتابعة حركة الجاني وأنشطته واتصالاته الحالية والمستقبلية مع الغير وقت حدوثها، ومن أهم الإجراءات المستحدثة المتعلقة بالبيانات المتحركة، المراقبة السرية للاتصالات والمراسلات الإلكترونية، التسرب، وسوف نفصل ذلك وفقاً لما يلي:

الفرع الأول: المراقبة السرية للاتصالات والمراسلات الإلكترونية:

لقد أدى قصور الإجراءات التقليدية الواردة في قوانين الإجراءات الجزائية لغالبية الدول في مواجهة الجرائم المعلوماتية خاصة فيما يتعلق بشقها المعنوي، إلى قيام بعض الدول باستحداث ترتيبات تقنية للمراقبة السرية للاتصالات والمراسلات الإلكترونية، وتجميع وتسجيل محتوياتها وحفظها أو حجبها لمقتضيات التحقيق وحماية النظام والآداب العامة

أولاً: تعريف المراقبة الإلكترونية السرية وصورها: تعرف بأنها ما يقوم به المراقب لجمع البيانات والمعلومات حول الشخص أو الشيء محل التحري والتحقيق مستخدماً بذلك والوسائل والتقنيات الإلكترونية " (البدري، 2019)، وقد تأخذ هذه المراقبة صورتين، هما:

1. **المراقبة السرية لشبكات المعلوماتية:** وذلك عندما تجيز بعض التشريعات المراقبة السرية للمواقع والمحادثات ومواقع التواصل وغرف الدردشة المفتوحة، وتتم هذه المراقبة من خلال استخدام تقنيات تعقب المواقع التي تحتوي على بيانات أو معلومات أو محتويات غير مشروعة مثل المواقع الإباحية أو تلك التي تروج للإرهاب أو المخدرات، لكن في الواقع العملي لا تكون المراقبة السرية للشبكات المعلوماتية أمراً سهلاً، حيث تتطلب مؤهلات ومهارات تقنية خاصة لدى سلطات التحقيق والضبط القضائي، فضلاً عن المعرفة والدراية القانونية اللازمة للتعرف على ما يدخل ضمن الحياة الخاصة للأفراد وما يجوز مراقبته

وما لا يجوز مراقبته إلا بأذن قضائي، سواء بعد حدوث الجريمة أو قبل حدوثها كإجراء واحترازي لتتبع أشخاص سبق إدانتهم في جرائم معلوماتية، أو لتورطهم بتصريحات تحرض على الممارسات الإرهابية والاخلال بأمن الدولة والسكينة العامة فيها. (السعدي، 2018)

2. **المراقبة الإلكترونية السرية من خلال مراقبة محتوى الاتصالات الإلكترونية:** أو ما يطلق عليها اعتراض المراسلات السلكية واللاسلكية، وقد عرفها المشرع الجزائري بأنها " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية وتأخذ هذه المراسلات صورة البيانات أو الأصوات أو الصور القابلة للتداول والتخزين"، وبصفة عامة تعد المراقبة الإلكترونية السرية إجراء من إجراءات التحري والتحقيق التي تمس بحق الفرد في الخصوصية، ويرى بعض الفقه أن هذه المراقبة تعد من قبيل التفتيش على اعتبار أنها تهدف مثلها التفتيش إلى البحث وضبط ما يوصل للحقيقة (السعدي، 2018) ، لكن البعض الآخر يرى أن هناك فرق بينهما لأن التفتيش يرد على البيانات الإلكترونية الساكنة أي الاتصالات المنتهية المخزنة (أبو الدهب، 2015)، أما المراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة أي الاتصالات الإلكترونية الحالية والمستقبلية وقت حدوثها وذلك للحصول على اتصالات إلكترونية مخزنة من خلال تسجيل محتوى هذه الاتصالات سواء كان صوتي أو مرئي وتخزينه على وسائط تخزين تسهل نقله واستخدمه في إثبات جريمة معينة. (البكري، 2016)

أما المشرع الإماراتي فلم يحدد الجوانب الإجرائية لمراقبة محتوى الاتصالات الإلكترونية أو اعتراض المراسلات السلكية واللاسلكية إلا بعد حدوث الجريمة ووفقاً لمقتضيات التحقيق في الجريمة، وذلك من خلال نص المادة (75) من قانون الإجراءات الجزائية الإماراتي والتي تنص على " ... ويجوز بموافقة النائب العام أن يضبط لدى مكتب 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 ".

ونرى أن هذا النص قد يعبر أو يتضمن إجراء مراقبة محتوى الاتصالات الإلكترونية، في حالة القيام بتتبع محتوى الاتصالات الإلكترونية للمتهم بعد حدوث الجريمة وأثناء مراحل التحقيق معه، وفي ظل هذا الفرض نرى أن هذا النص لم يشير إلى مراقبة محتوى الاتصالات الإلكترونية في صورتها المسموعة والمرئية، فلم يحدد النص السابق شروطها وضوابطها وإجراءات تنفيذ ها.

ثانياً: ضمانات المراقبة السرية للاتصالات والمراسلات الإلكترونية: تقضي القاعدة العامة بأنه لا يجوز مراقبة الاتصالات والمراسلات أو تسجيل المكلمات أو التقاط الصور دون علم ورضا الشخص المستهدف بهذه المراقبة، إلا أن العديد من التشريعات قد أقرت استثناءات من هذه القاعدة من خلال السماح بهذه المراقبة لتحقيق مصلحة عليا للمجتمع تتمثل في الكشف عن الجرائم من مطلق أن هذه المصلحة هي الأولى بالرعاية من المصلحة الخاصة التي تتمثل في الحفاظ على الحياة الخاصة للشخص، لكن المشرع قد أحاط هذا الاستثناء بمجموعة من الضمانات، أهما: (السعدي، 2018)

1. قصر استخدام المراقبة السرية للاتصالات والمراسلات الإلكترونية على جرائم محددة، فقد حددت بعض التشريعات مثل التشريع الجزائري نطاق استخدام هذه المراقبة فقط بصدد التحري والتحقيق في حالة التلبس بالجريمة أو بصدد التحقيق الابتدائي في جرائم محددة على سبيل الحصر وهي الجرائم التي تشكل خطراً على أمن الدولة والجرائم الإرهابية وجرائم الاعتداء على المنظومة المعلوماتية بصورة تهدد النظام العام وأمن الدولة ومؤسساتها. لكن المشرع الإماراتي من خلال المادة (75) من قانون الإجراءات الجزائية الإماراتي لم يحدد جرائم بعينها واكتفي بنص عام يقضي بإمكانية القيام بهذا الإجراء متى استوجبت مقتضيات التحقيق ذلك، وبذلك يتبين أن المشرع الإماراتي قد ربط استخدام المراقبة السرية للاتصالات والمراسلات الإلكترونية بتقدير سلطات التحقيق وفقاً لحاجة التحقيق لهذه المراقبة.

2. الحصول على إذن أو تصريح بالمراقبة من السلطات المختصة وهي وفقاً لنص المادة (75) من قانون الإجراءات الجزائية الإماراتي تتمثل في موافقة النائب العام، لكن المشرع الإماراتي لم يحدد طبيعة وشروط هذا الإذن، لكن وفقاً للقواعد العامة فيجب أن هذا الإذن مكتوب ومسبب ويتضمن تفاصيل عن نوع الجريمة الاتصال أو المراسلات المقصود مراقبتها، وكذلك النطاق المكاني والزمني لهذا الإذن.

3. وجوب تحرير محضر من قبل القائم بالتحري والتحقق لكل عملية مراقبة أو اعتراض الاتصالات والمراسلات أو تسجيل للمكالمات أو للصور، ويجب أن يتضمن هذا المحضر كافة الترتيبات التي تمت والنتائج التي تم التوصل إليها، ووفقاً للقواعد العامة يجب إحصاء الأدلة المتحصل عليها من المراقبة في أحراز مختومة لضمان عدم العبث فيها أو تعرضها للتلف.

4. الحفاظ على الاسرار المهنية من خلال اتخاذ كافة التدابير اللازمة لضمان إتمام كافة وفقاً لمقتضيات السرية المهنية، فضلاً عن ضرورة الاستعانة بأصحاب الخبرة الفنية في مجالات تكنولوجيا الاتصالات.

الفرع الثاني: التسرب المعلوماتي:

سوف نتعرف على التسرب المعلوماتي وفقاً لما يلي:

أولاً: تعريف التسرب المعلوماتي: هو إجراء من إجراءات التحري والبحث التي استحدثتها بعض الدول في قوانين الإجراءات الجزائية الخاصة بها، بصدد جرائم معينة على سبيل الحصر منها الجرائم المعلوماتية (خليفة، 2016)، وقد عرف التسرب المعلوماتي بأنه " إجراء يقوم به مأمور الضبط القضائي أو أحد أعوانه تحت مسؤوليته بتنسيق العملية لمراقبة الأشخاص المشتبه فيهم من خلال إيهامهم أنه فاعل معهم أو شريك لهم".[1]

ووفقاً للنص السابق يكون دور القائم أو المنفذ لإجراء التسرب هو البحث والتحري في الجرائم المعلوماتية، بأن يدخل إلى العالم الافتراضي ويقوم بالمشاركة في المحادثات مواقع التواصل الاجتماعي وغرف الدردشة بهوية مستعارة، ولا يجوز إظهار هوايته الحقيقية في أي مرحلة من مراحل التحقيق، ويتعرض كل من يكشف عن هوايته للعقاب، ويهدف التسرب المعلوماتي إلى جمع البيانات والدلائل التي ترشد إلى الأعمال الإجرامية، والتعرف على الإمكانيات البشرية والمادية للجناة وكذلك التعرف على طرق ووسائل الاتصال التي يستخدمها الجناة لتنفيذ أعمالهم الغير الإجرامية، وفي سبيل قيام العنصر القائم بالتسرب فقد أحاطه المشرع بمجموعة من الضمانات لحمايته هو وأسرته كما أعفاه من المسؤولية الجنائية عن ما يقوم به من أفعال غير مشروعة أو جرائم أثناء تنفيذه للتسرب. (أبو الذهب، 2015)

لكن المشرع الإماراتي لم يورد إجراء التسرب ضمن قانون الإجراءات الجزائية الإماراتي، ونرى أن هذا الإجراء يعرف (بالتحريض الصوري) تملكه سلطات الضبط القضائي في كافة الجرائم ضمن ضوابط إجرائية راسخة ومتعارف عليها، وبالتالي فلا يشترط أن يحدد المشرع ضوابط أو القواعد خاصة به بشأن الجريمة المعلوماتية، وسوف نعرض أهم القواعد والضمانات والشروط والتحديات التي تواجه استخدام التسرب المعلوماتي، وذلك وفقاً لما يلي:

ثانياً: شروط أو ضوابط التسرب المعلوماتي: نظراً لما يتضمنه التسرب المعلوماتي من ممارسات تمثل انتهاكاً للحياة الخاصة للأفراد المستهدفين به، لذلك فقد حرص المشرع على إحاطته بمجموعة من الضمانات أو الضوابط الموضوعية والشكلية، وذلك وفقاً لما يلي: (قادري، 2014)

(1) وفقاً لنص المادة (65) مكرر من القانون رقم (6 ــ22) المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

1. **الشروط الموضوعية للتسرب:** وتتمثل فيما يلي:

أ. السبب: أو المبرر الذي يقنع السلطات المختصة بمنح الإذن بالقيام بالتسرب، حيث يجب أن يتوافر سبب مقنع يبرر المساس بالحياة الخاصة للمتهم.

ب. نوع الجريمة: حيث لا يتم التصريح بالتسرب إلا بصدد البحث والتحري عن جرائم محددة على سبيل الحصر وهي التي تمثل تهديداً لأمن واستقرار الدولة لسرعة انتشارها وخطورة آثارها المرتكبين لها، مثل الجرائم المنظمة العابرة للحدود الوطنية، وجرائم غسيل الأموال والمخدرات، وجرائم الإرهاب، وجرائم الفساد، والجرائم المعلوماتية.

2. **الشروط الشكلية للتسرب:** وتتمثل فيما يلي: (مراد، 2018)

أ. صدور إذن قضائي به سواء من النائب العام أو قاضي التحقيق، ويجب أن يكون هذا الإذن مكتوب ويذكر فيه سببه ومدته والجريمة التي تبرره، وكذلك هوية مأمور الضبط القضائي المكلف بالقيام بالتسرب، ويجب أن يبقى هذا الأذن خارج ملف الإجراءات لحين الانتهاء من إتمام التسرب من أجل الحفاظ على سرية أعمال التسرب.

ب. تحرير محضر يتضمن ممارسات وانشطة مأمور الضبط المنفذ للتسرب، فضلاً عما يتوصل إليه المتسرب من نتائج، وكذلك ما قد يتعرض له من خطر.

نخلص مما سبق أن النص الذي أورده المشرع الإماراتي بشأن المراقبة السرية للاتصالات والمراسلات الإلكترونية لم يحدد الحالات التي تستدعي اللجوء إليها، فلم يحدد جرائم بعينها على غرار المشرع الجزائري على سبيل المثال، أي أن المشرع الإماراتي قد ربط استخدام المراقبة السرية للاتصالات والمراسلات الإلكترونية بتقدير سلطات التحقيق وفقاً لحاجة التحقيق لهذه المراقبة.

المطلب الثاني: إجراءات تتعلق بالبيانات الإلكترونية الساكنة

ينصرف مفهوم البيانات الساكنة إلى البيانات المخزنة خاصة المتعلقة بالاتصالات الإلكترونية التي تم الاحتفاظ بنسخة منها في الخادم المعلوماتي الخاص بمقدم خدمة الاتصالات والإنترنت، حيث يمكن لسلطات التحقيق الاستعانة بها واستخدامها في حال قيام الجاني أو أي شخص بالتلاعب بهذه البيانات أو محاولة إخفائها أو إتلافها، حيث تكون النسخة المخزنة لدي الخادم الخاص بمقدم الخدمة بمثابة دليل في مواجهة الجاني خاصة فيما يتعلق بالاتصالات الإلكترونية غير المشروعة، فضلاً عن دور هذه البيانات

الساكنة في معرفة هوية المجرم المعلوماتي وتتبع أثره، حيث غالباً ما تلزم التشريعات مزودي خدمات الاتصالات والإنترنت[1]، بمجموعة من الإجراءات العامة والخاصة يكون الهدف منها مراقبة ومتابعة استخدام وسائل وتقنيات وتطبيقات الاتصالات خاصة الحديثة منها، وتسجيل والاحتفاظ البيانات المخزنة بأجهزة الاتصالات والإنترنت وضمان سلامتها وسريتها، والتي قد تفيد سلطات التحقيق في اكتشاف الجرائم المعلوماتية وضبط أدلتها. (قادري، 2014)

وفي ظل ما تم الإشارة إليه فيما سبق حول عدم كفاية الإجراءات التقليدية للتحري والتحقيق في الجرائم المعلوماتية خاصة فيما يتعلق بالمكونات المعنوية للحاسب الآلي، ومن ثم صعوبة استخلاص الدليل الإلكتروني بالطرق والأساليب التقليدية مع قدرة الجناة إخفاء أو إتلاف أو إزالة هذه الأدلة من المنظومة المعلوماتية، فكان لابد من اللجوء إلى التزام مزودي الخدمة بالقيام بإجراءات عامة وخاصة، وفي هذا الصدد قد حددت العديد من التشريعات الالتزامات العامة والخاصة لمزودي الخدمة، لكن في المشرع الإماراتي لم يحدد بصورة واضحة للالتزامات العامة أو الخاصة لمزودي خدمات الاتصالات والإنترنت، إلا من خلال البند (2) من المادة (66) الذي ينص على أنه " للنائب العام متي قامت أدلة على قيام موقع إلكتروني من داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أصور أو أفلام أو أي مواد دعائية، أو ما في حكمها بما يعد جريمة من الجرائم المنصوص عليها في المادة (71) من هذا المرسوم بقانون، أو يشكل تهديداً للأمن الوطني أو يعرض أمن الدولة أو اقتصادها الوطني للخطر، أن يأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنياً أو إصدار أي من الأوامر المنصوص عليها بهذا المرسوم بقانون".

ونرى أن هذا النص غير كافي للتحديد الواضح والدقيق للإجراءات المستحدثة المتعلقة بالجرائم المعلوماتية فيما يتعلق بالبيانات الساكنة، وهذا ما يضع القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية موضع النقد فيما يتعلق بعدم احتوائه أو تحديده للإجراءات المستحدثة يصدد التحري والتحقيق في الجرائم المعلوماتية، خاصة أن عدد من التشريعات العربية قد تضمنت وحددت وعددت هذه الإجراءات بشكل صريح ومن أمثلة ذلك التشريع الجزائري والمصري، وسوف نعرض هذه الإجراءات المستحدثة للتحري والتحقيق في الجرائم المعلوماتية المتعلقة بالبيانات الإلكترونية الساكنة،

(1) عرفت المادة الأولى من القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية مزود الخدمة بأنه " مل شخص طبيعي أو اعتباري عام أو خاص يزود المستخدمين بخدمات الوصول بواسطة تقنية المعلومات إلى الشبكة المعلوماتية"، كما عرفته المادة الأولى من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الجزائري بأنه " أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

والتي تمثل التزامات عامة أو خاصة على مقدمي خدمة الاتصالات والإنترنت، من واقع التشريعات التي حددت هذه الالتزامات بصورة صريحة، وذلك وفقاً لما يلي:

الفرع الأول: الإجراءات العامة من قبل مقدمي خدمات الاتصالات والإنترنت:

تتمثل هذه الالتزامات أو الإجراءات العامة، فيما يلي:

أولاً: مساعدة سلطات التحري والتحقيق: تضمنت المادة (18) من اتفاقية بودابست بإلزام مقدمي خدمة الاتصالات والإنترنت بتقديم المساعدة لسلطات التحري والتحقيق في الجرائم المعلوماتية من خلال مدها بمعلومات أو معلومات محددة، حيث نصت هذه المادة على أنه " تعتمد كل دولة طرق ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة إصدار أمر إلى أي مزود خدمة بعرض خدماته داخل أراضي الدولة الطرف في الاتفاقية بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة في حوزته أو تحت سيطرته"[1]، وتتضمن هذه البيانات أي معلومات موجودة على حواسيب مزود الخدمة تتعلق بالمشترك في الخدمات التي يقدمها المزود وتتضمن هذه البيانات: هوية المشترك وعنوانه البريدي والجغرافي ورقم هاتفه ورقم ولوجه والبيانات الخاصة بفواتير الدفع، كذلك نوع الخدمة المشترك فيها ومدة الخدمة وشروطها الفنية، أي معلومات أخرى تتعلق بمواقع تركيب أجهزة ومعدات الاتصالات لدى المشترك، وتتضمن المساعدة التي يقدمها المزود أن يقوم بكتمان سرية العمليات التي يقومون بها في إطار التحري والتحقيق أو أي معلومات تتعلق بهذه الأعمال، ويقع المزود عند مخالفة ذلك تحت طائلة العقوبة المقررة بصدد إفشاء أسرار التحري والتحقيق. (خليفة، 2016)

أما المشرع الإماراتي فلم يضع نص في القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية، يتضمن هذا الالتزام

ثانياً: حفظ المعطيات المتعلقة بحركة السير: ويقصد بها المعطيات التي تتعلق بالاتصال من خلال منظومة معلوماتية، وتتضمن هذه المعطيات مصدر الاتصال، والوجهة المرسلة اليها والطريق الذي يسلكه، ووقت وتاريخ وحجم مدة الاتصال ونوع الخدمة، وبذلك فهو يعد أداة مستحدثة للتحقيق في الجرائم المعلوماتية، وهو خطوة تمهيدية الهدف منها الاحتفاظ بالبيانات قبل فقدها، يتم من خلال قيام سلطات التحقيق بتوجيه أمر لمزودي الخدمة بالتحفظ على بيانات معينة مخزنة لديه وتحت سيطرته، انتظاراً لاتخاذ إجراءات قانونية لاحقة مثل التفتيش أو أمر المزود بتقديم بيانات معلوماتية. (أبو راس، 2016)

(1) المادة رقم (18) من اتفاقية بودابست (2001) الخاصة بالجريمة الإلكترونية، الصادرة عن المجلس الأوربي.

كما ألزمت المادة (1) من قرار الجمعية العامة للأمم رقم (63 ـــ 55) الصادر في 22 يناير 2001م بشأن مكافحة اساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، الدول بالسماح بحفظ البيانات الالكترونية التي تتعلق بالتحقيقات الجنائية الخاصة وتيسير سرعة الحصول عليها. (حجازي، 2008)

لكن المشرع الإماراتي لم يضع نص في القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية، يتضمن هذا الالتزام

الفرع الثاني: الإجراءات الخاصة من قبل مقدمي خدمات الاتصالات والإنترنت:

تتمثل هذه الالتزامات أو الإجراءات الخاصة، فيما يلي:

أولاً: التدخل الفوري لسحب المحتويات غير القانونية أو غير المشروعة: وهو إجراء يلزم به مقدمي خدمات الاتصالات والإنترنت بالتدخل على وجه السرعة دون تراخي لسحب المحتويات المتاح الاطلاع عليها، مثل المواد والممارسات الاباحية المتعلقة بالأطفال، والفيروسات والبرامج الضارة بالمعطيات المعلوماتية، وجرائم الاحتيال المعلوماتي وتزوير البطاقات البنكية (القطاوية، 2010)، ولم ينص المشرع الإماراتي صراحة على هذا الإجراء، لكنه أشار إلى إجراء أخر في المادة (1) من القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية، من خلال تعريف (أوامر التصحيح وإزالة البيانات الزائفة)، بأنها " الاشعارات التي تصدرها الجهات المختصة إلى شخص معين أو أكثر بتصحيح أو إزالة أو حذف المحتوى غير القانوني أو بتصحيح أو إزالة أو حذف المعلومات أو البيانات الزائفة "

ويتبن من التعريف السابق أن إجراء "أوامر التصحيح وإزالة البيانات الزائفة" الذي أشار إليه المشرع الإماراتي وأن كان يقارب في مضمونه لإجراء التدخل الفوري لسحب المحتويات غير القانونية، إلا أن الجهة الملزمة في إجراء التدخل الفوري هي كيان تنظيمي هو مقدمو خدمة الإنترنت، أما الجهة الملزمة في إجراء أوامر التصحيح وإزالة البيانات الزائفة هم الاشخاص.

ثانياً: وضع ترتيبات تقنية لمنع وصول الجمهور إلى الأنشطة والممارسات المعلوماتية غير المشروعة: ويتضمن هذا الإجراء بإلزام مزود الخدمة بحذر الدخول إلى الموزعات التي تحتوي على معلومات تخالف النظام العام أو الآداب العامة من خلال العمل على وضع ترتيبات تقنية تمنع الوصول إلى الأنشطة والممارسات المعلوماتية غير المشروعة، فضلاً عن وجوب أخبار المشتركين لدي مزودي الخدمة بوجود هذه الممارسات أو الأنشطة غير المشروعة. (حسني، 2016)

وقد أشار المشرع الإماراتي إلى هذا الأجراء من خلال البند (2) من المادة (66) من القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية، الذي ينص على أنه " للنائب العام متي قامت أدلة على قيام موقع إلكتروني من داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أصور أو أفلام أو أي مواد دعائية، أو ما في حكمها بما يعد جريمة من الجرائم المنصوص عليها في المادة (71) من هذا المرسوم بقانون، أو يشكل تهديداً للأمن الوطني أو يعرض أمن الدولة أو اقتصادها الوطني للخطر، أن يأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنياً أو إصدار أي من الأوامر المنصوص عليها بهذا المرسوم بقانون".

وقد أقر المشرع الإماراتي حجب الموقع أو المواقع التي تتضمن محتويات أو ممارسات تعد من قبيل الجرائم المعلوماتية من خلال وضع ترتيبات تقنية لمنع وصول الجمهور إلى الأنشطة والممارسات المعلوماتية غير المشروعة من خلال أمرين هما "أوامر التعطيل"، "أوامر حظر الوصول"، فقد عرفت المادة (1) من القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية، أوامر التعطيل بأنها " الاشعارات التي تصدرها الجهات المختصة إلى وسيط شبكة معلوماتية ينشر من خلاله محتوى غير قانوني أو بيانات زائفة، يطلب منه تعطيل وصول المستخدمين إلى المحتوى أو البيانات المشار إليها، بالشكل أو الطريقة التي تراها تلك الجهات مناسبة خلال المدة المحددة في الإشعار"

ويتبين من هذا التعريف أن أمر التعطيل هو إجراء مؤقت محدد بمدة معينة، وتحدد الجهات المختصة طريقة تنفيذه

كما عرفت المادة السابقة أوامر حظر الوصول بانها " الأوامر التي تصدرها الجهات المختصة إلى مزود الخدمة بالدولة عند عدم إمكانية تنفيذ التعليمات الأخرى المشار إليها بهذا المرسوم بقانون وذلك لاتخاذ تدابير تعطيل المستخدمين في الدولة إلى الموقع أو الحساب الإلكتروني"

أي أن المشرع الإماراتي قد وضع ترتيبات تقنية كلما أمكن تحقيق ذلك، لمنع وصول الجمهور إلى الأنشطة والممارسات المعلوماتية غير المشروعة من خلال إقرار الأمر بحجب الموقع أو المواقع التي تحتوي هذه الأنشطة والممارسات، أو من خلال إصدار أوامر التعطيل أو أوامر حظر الوصول

خاتمة الدراسة

لقد سعت هذه الدراسة إلى الوقوف على مدى صلاحية أو كفاية الآليات الإجرائية التقليدية الواردة في قانون الإجراءات الجزائية الإماراتي لضبط الجريمة الإلكترونية، وما مدى احتواء القوانين السارية في دولة الإمارات على آليات إجرائية مستحدثة لضبط الجريمة الإلكترونية، وسوف نعرض فيما يلي النتائج التي توصلت إليه هذه الدراسة والتوصيات بصددها.

أولاً: النتائج: لقد توصل الباحث من خلال هذه الدراسة إلى مجموعة من النتائج التي يمكن عرضها فيما يلي:

1. تخضع الجريمة الإلكترونية لنفس إجراءات وآليات البحث والتحري والتحقيق التي تمر بها الجرائم التقليدية، ولا تثير بعض القواعد الإجرائية التقليدية مشاكل أو تحديات للتطبيق بصدد الجرائم الإلكترونية مثل إجراءات التحقيق التي تتضمن سماع المتهم والشهود والاستجواب والمواجهة، لكن بعض الإجراءات التقليدية الأخرى تتضمن الكثير من الصعوبات أو التحديات عند تطبيقها بشأن هذه الجرائم، ومن أهم هذه الإجراءات المعاينة الرقمية والخبرة، والتفتيش المعلوماتي، وضبط الأدلة الرقمية.

2. فيما يتعلق بالإجراءات التقليدية لضبط الجرائم الإلكترونية الواردة في قانون الإجراءات الجزائية الإماراتي تبين ما يلي:

- أن إجراءات المعاينة والخبرة غير كافية لضبط الجرائم الإلكترونية، وأن غالبية الضوابط أو الضمانات الواردة في هذا القانون بشأن التفتيش الجنائي صالحة للتطبيق على تفتيش المكونات المادية للحاسب الآلي، أما إجراءات تفتيش المكونات المعنوية للحاسب الآلي فهي تتطلب ضوابط وأحكام خاصة تلاءم الطبيعة الخاصة لهذا المكونات المعنوية.

- أن القواعد الإجرائية الواردة في هذا القانون بشأن ضبط الأدلة، تلائم ضبط المكونات المادية للحاسب الآلي، إلا أنها غير كافية لتنظيم ضبط المكونات المعنوية أو الأدلة الرقيمة، ويتطلب الأمر ضرورة استحداث عدد من القواعد الإجرائية الخاصة التي تتعلق بالمعاينة والخبرة الرقمية، والتفتيش المعلوماتي، وضبط الأدلة الرقمية في الجرائم المعلوماتية.

4. فيما يتعلق بإجراءات التحري والتحقيق المستحدثة في الجريمة الإلكترونية، تبين ما يلي:

- بصدد الإجراءات الخاصة بالبيانات الإلكترونية المتحركة تبين أن النص الذي أورده المشرع الإماراتي من خلال نص المادة (75) من قانون الإجراءات الجزائية الإماراتي قد يعبر أو يتضمن إجراء مراقبة محتوى الاتصالات الإلكترونية، في حالة القيام بتتبع محتوى الاتصالات الإلكترونية للمتهم بعد حدوث الجريمة وأثناء مراحل التحقيق معه، ونرى أن هذا النص لم يشير إلى مراقبة محتوى الاتصالات الإلكترونية في صورتها المسموعة والمرئية، فلم يحدد النص السابق شروطها وضوابطها وإجراءات تنفيذ ها، ولم يحدد المشرع الإماراتي الحالات التي تستدعي اللجوء إليها، لكنه ربط استخدام المراقبة السرية للاتصالات والمراسلات الإلكترونية بتقدير سلطات التحقيق وفقاً لحاجة التحقيق لهذه المراقبة ولم يحدد جرائم بعينها على غرار المشرع الجزائري على سبيل المثال، فضلاً عن أن المشرع الإماراتي لم يورد إجراء التسرب ضمن قانون الإجراءات الجزائية الإماراتي، ويعرف هذا الإجراء (بالتحريض الصوري) وتملكه سلطات الضبط القضائي في كافة الجرائم ضمن ضوابط إجرائية راسخة ومتعارف عليها، وبالتالي فلا يشترط أن يحدد المشرع ضوابط أو القواعد خاصة به بشأن الجريمة المعلوماتية.

- بصدد الإجراءات المتعلقة بالبيانات الساكنة، لم يتناول المشرع الإماراتي من خلال القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية ضمن نصوصه تحديداً واضحاً للالتزامات العامة أو الخاصة لمزودي خدمات الاتصالات والإنترنت، إلا من خلال البند (2) من المادة (66) منه، لكن هذا النص غير كافي للتحديد الواضح والدقيق للإجراءات المستحدثة المتعلقة بالجرائم المعلوماتية فيما يتعلق بالبيانات الساكنة، وهذا ما يضع القانون الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية موضع النقد فيما يتعلق بعدم احتوائه أو تحديده للإجراءات المستحدثة بصدد التحري والتحقيق في الجرائم المعلوماتية، أما فيما يتعلق بالإجراءات الخاصة من قبل مقدمي خدمات الاتصالات والإنترنت، فلم ينص المشرع الإماراتي صراحة على إجراء التدخل الفوري لسحب المحتويات غير القانونية أو غير المشروعة، لكنه أشار إلى إجراء أخر مشابه هو أوامر التصحيح وإزالة البيانات الزائفة، وفيما يتعلق بوضع ترتيبات تقنية لمنع وصول الجمهور إلى الأنشطة والممارسات المعلوماتية غير المشروعة فقد وضع المشرع الإماراتي ترتيبات تقنية لمنع وصول الجمهور إلى

الأنشطة والممارسات المعلوماتية غير المشروعة من خلال إقرار الأمر بحجب الموقع أو المواقع التي تحتوي هذه الأنشطة والممارسات، أو من خلال إصدار أوامر التعطيل أو أوامر حظر الوصول.

ثانياً: التوصيات: من واقع ما توصلت إليه هذه الدراسة من نتائج، قام الباحث بصياغة مجموعة من التوصيات نعرضها فيما يلي:

1. **على الجانب التشريعي**، دعوة المشرع الإماراتي تضمين قانون الإجراءات الجزائية الاتحادي فصل خاص لضبط الجرائم الإلكترونية تتلاءم مع الطبيعة الخاصة لهذه الجرائم وذلك كبديل شامل ودقيق لتفرق هذه القواعد الإجرائية ما بين عدد من القوانين، مع مراعاة إضافة إجراءات التحري والتحقيق المستحدثة التي لم ينص عليها المشرع الإماراتي المشار إليها في نتائج هذه الدراسة.

2. **على الجانب التطبيقي**، العمل على التطوير المستمر وزيادة فعالية الوحدات أو الإدارات أو الأقسام المنوط بها القيام بإجراءات التحري والتحقيق في الجرائم الإلكترونية، وزيادة وتكثيف البرامج التدريبية المتخصصة لزيادة وتحديث المعارف والمهارات التقنية المعلوماتية لسلطات الضبط القضائي والتحري والتحقيق في الجرائم الإلكترونية دائمة التطور.

3. **على الجانب القضائي**، العمل على دعم وتطوير والتأهيل الفني لأعضاء نيابة وقضاة تحقيق وقضاة المحاكم المختصين بالتعامل مع الجرائم الإلكترونية، من خلال زيادة معارفهم ومهاراتهم الفنية التقنية بصورة تمكنهم من القيام بأدوارهم بكفاءة وفعالية.

4. **على الجانب التوعوي**، العمل على تنمية الوعي المعلوماتي لدى الأفراد والمؤسسات، ودورهم الوقائي في الحد من الجرائم الإلكترونية، ودورهم في المساعدة والدعم لضبط هذه الجرائم ورصد مرتكبيها من خلال إبلاغ السلطات المختصة بممارسات غير المشروعة أو المشتبه فيها ومرتكبيها، وكل ذلك من خلال حملات توعية من قبل الجهات الأمنية في الدول باستخدام كافة الوسائل والقنوات الإعلامية المرئية والمسموعة والمكتوبة.

5. **على الجانب الأكاديمي:** حث الجامعات وخاصة كليات القانون وأكاديميات الشرطة على زيادة التعمق في دراسة الابعاد القانونية المختلفة للجرائم الإلكترونية في شقها الموضوعي أو الإجرائي في التشريع، وإجراء البحوث والدراسات باستمرار لتقييم فعالية القوانين في المواجهة الموضوعية والإجرائية في ضوء كل ما يستجد من سلوكيات إجرامية ترتكب بها الجرائم الإلكترونية.

قائمة المصادر والمراجع:

إبراهيم، خالد ممدوح (2008). أمن الجريمة المعلوماتية. دار الفكر الجامعي.

إبراهيم، خالد ممدوح (2017). الجرائم المعلوماتية. دار الفكر الجامعي.

البدري، محمـود حسين (2019). التحقيق الجنائي الرقمي. دار النهضة العربية.

البكري، يوسف محمـد (2016). التفتيش في الجرائم المعلوماتية. دار الفكر الجامعي.

السعيد، عماد صالح (2019). التحقيق الجنائي الرقمي في الجرائم المعلوماتية. دار الكتب القانونية.

الشوابكة، محمـد (2013). جرائم الحاسب الآلي الاقتصادية. منشورات الحلبي.

العازمي، فهد عبدالله العبيد (2016). الإجراءات الجنائية المعلوماتية. دار الجامعة الجديدة.

المومني، نهلة عبد القادر (2010). الجرائم المعلوماتية. دار الثقافة للنشر والتوزيع.

أبـو الذهـب، حامـد السـعيد (2015). البحـث والتحقيـق الجنـائي الرقمـي في الجرائـم المعلوماتيـة. دار الكتـب القانونيـة.

أبـو راس، إيـاد حـسين (2016). إجـراءات التحـري والتحقيـق في جرائـم الكمبيوتـر والإنترنـت. دار الثقافـة للـمشر والتوزيـع.

حجازي، عبد الفتاح بيومي (2008). الاثبات في جرائم الكمبيوتر والإنترنت. دار الكتب القانونية.

حجـازي، عبـد الفتـاح بيومـي (2012). مكافحـة جرائـم الكمبيوتر والإنترنـت في القانـون العربي النموذجـي. دار الفكر الجامعي.

حسني، خلود محمد (2016). التحقيق في الجرائم المعلوماتية دراسة مقارنة. دار الكتب القانونية.

شاهين، محمد كمال (2016). التحقيق في الجرائم المعلوماتية دراسة مقارنة. دار الكتب القانونية.

موسى، مصطفى محمـد (2015). دليل التحري عبر شبكة الإنترنت. دار الكتب القانونية.

البـشري، محمـد الأمين (2005). التحقيـق في جرائـم الحاسـب الآلي. [بحـث]. مؤتمـر القانـون والكمبيوتـر والإنترنت. كليـة الحقـوق والشريعـة، جامعـة الإمارات. 21 مايـو 2005م.

البـشري، محمـد الأمين (2008). الأدلـة الرقميـة ودورهـا في الاثبـات الجنـائي. المجلـة العربيـة للدراسـات الأمنيـة والتدريـب، *15*(38)

القطاوية، مصعب (2010). الإجراءات الجناية الخاصة بالجرائم المعلوماتية. شبكة قانون الأردن.

المعـيني، سرحـان حسـن (2011). التحقيق في جرائـم تقنية المعلومات. مركز بحوث الشرطـة، دورية الفكر الشرطي، *2*(اكتوبر).

خليفـة، محمـد (2016). خصوصيـة الجريمـة الإلكترونيـة وجهـود الـمشرع الجزائـري في مواجهتهـا. مجلـة دراسـات وأبحـاث، *1*(1)

السـعدي، خليفـة راشـد (2018). الحمايـة الجرائيـة لمعيطـات الحاسـب الآلي في القانون المقارن [رسـالة ماجسـتير، جامعـة نايـف العربية للعلـوم الأمنية].

قـادري، سـارة (2014). أسـاليب التحـري الخاصـة في قانـون الإجـراءات الجزائيـة [رسـالة ماجسـتير، جامعـة قاصدي

بريـاح ورقلـة كليـة الحقـوق والعلوم السياسـية].

مـراد، عـادل محمـد (2018). الجرائـم الإلكترونية وتحديات إثباتها [رسـالة ماجسـتير، أكاديمية نايـف العربية للعلوم الشرطية].

الترجمة الصوتية لمصادر ومراجع اللغة العربية: Romanized Arabic References:

ʾibrāhīmu khālid mamdūḥin (2008). ʾamnu aljarīmati almaʿliwimmitya dāru alfikri aljāmiʿiyyi

ʾibrāhīmu khālid mamdūḥin (2017). aljarāʾimi almaʿliwimmitya dāru alfikri al-jāmiʿiyyi

albadriyyu mḥmwd ḥusaynu (2019). al-taḥqīqu al-jjināʾiyyi al-raqmiyyu dāru al-nahḍati alʿarabiyyati

albakriyyu yūsufa mḥmd (2016). al-taftīshi fī aljarāʾimi almaʿliwimmitya dāru alfikri al-jāmiʿiyyi

al-saʿīdu ʿimādu ṣāliḥin (2019). al-taḥqīqu al-jjuniʾiʾiuy al-raqmiyyu fī aljarāʾimi almiʿliwwamiātya dāru al-kutubi al-qānūniyyati

al-shwābakatu mḥmd (2013). jarāʾimu alḥāsibi alʾālī aliāqtiṣādiyyatu munshawarit alḥalabiyyi

alʿāzimiyyu fahdu ʿbdāllh alʿabbaydi (2016). alʾijrāʾātu aljināʾiyyatu al-miʿliwwamuātya dāru aljāmiʿati aljadīdati

almūminiyyu nahlatu ʿabdi alqādiri (2010). aljarāʾimi almaʿliwimmitya dāru al-thaqāfati lil-nashri wa-l-tawzīʿi

ʾabū al-dhahabi ḥāmidu al-saʿīdi (2015). al-baḥthu wa-l-taḥqīqu al-jjināʾiyyi al-raqmiyyu fī aljarāʾimi almaʿliwimmitya dāru al-kutubi al-qānūniyyati

ʾabū rāsin ʾīādu ḥusaynin (2016). ʾijarāʾāʾut al-taḥarrī wa-l-taḥqīqi fī jarāʾimi alkambyiwtr wa-l-ʾintarnit dāru al-thaqāfati lil-mashari wa-l-tawzīʿi

ḥijāziyyun ʿabdu al-fattāḥi bayūʾimyyin (2008). aliāthbātu fī jarāʾimi al-kkimbīūtr wa-l-ʾintarnit dāru al-kutubi al-qānūniyyati

ḥijāziyyun ʿabdu alfattāḥi bayūʾimyyin (2012). mukāfaḥati jarāʾimi alkimabyiwtr wa-l-ʾintarnit fī alqānūni alʿarabiyyi alnimawdhijjī dāru alfikri aljāmiʿiyyi

ḥasaniyyun khulūdi muḥammad (2016). al-taḥqīqu fī aljarāʾimi almiʿliwwamiātya dirāsatun muqārinatun dāru alkutubi al-qānūniyyati

shāhīnu muḥammadu kamālin (2016). al-taḥqīqu fī aljarāʾimi almiʿliwwamiātya dirāsatun muqārinatun dāru al-kutubi al-qānūniyyati

mūsā muṣṭafā mḥmd (2015). dalīlu al-taḥarrī ʿabra shabikati alʾintrnt dār al-kutubi al-qānūniyyati

albashariyyi muḥammadu alʾamīni (2005). al-taḥqīqu fī jarāʾimi alḥāsibi alʾālayi] baḥthun.[muʾutamaru alqānūni wa-l-kumbyiwatri wa-l-ʾintarnat kulliyyatu alḥuqūqi wa-l-sharīʿati

jāmi'atu al'imārāti 21 māyū 2005m.

albashariyyi muḥammadu al'amīni (2008). al'adillatu al-raqmiyyatu wadawruhā fī aliātthibāti aljuni'i'ī almajallatu al'arabiyyatu lil-dirāsāti al'amniyyati wa-l-tadrībi 15(38.(

alqaṭāwiyyatu muṣ'abin (2010). al'ijrā'ātu aljināyatu alkhāṣṣatu bi-l-jarā'imi alma'liwimmitya shabakatu qānūni al'urdunni

almu'īniyyu sirḥānu ḥasan (2011). al-taḥqīqu fī jarā'imi tiqniyyati alma'lūmāti markazu buḥūthi al-shurṭati dawriyyatu alfikri al-sharṭiyyi 2)aktwbr.(

khalīfatu muḥammad (2016). khuṣūṣiyyatu aljarīmati al'ilktrūniyyati wajuhūdu almusharri'i al-jazā'iriyyi fī mūājahatihā mijallatu dirāsātin wa'abḥāthin 1(1.(

al-sa'diyyu khalīfatu rāshidun (2018). alḥimāyatu aljirā'iyyatu limu'ayṭāti alḥāsibi al'ālyi fī alqānūni almuqārini] risālatu miājastyr jāmi'atu nāyifin al'arabiyyati lil-'ulūmi al'amniyyati

qādiriyyun sāratu (2014). 'asālību al-taḥarrī alkhāṣṣati fī qānūni al-'ijrā'āti aljazā'iyyati] risālatu miājastyr jāmi'atu qāṣidī birayāḥi warqala kulliyyati alḥuqūqi wa-l-'ulūmi al-sīāsiyyati

murād 'ādil muḥammad (2018). aljarā'imu al-'iliktirūniyyatu wataḥaddīātu 'ithbātihā] risālatu māajsityr ukā'udyamiya nuāyfi al'arabiyyati lil-'ulūmi al-sharṭiyyati

Procedural Mechanisms Tackling Cybercrime: An Analytical Study in the UAE Legislation

Mohammad Ibrahim ALaleeli(1)
Halima Khalid Almidfa(2)

Abstract:

This study seeks identify the procedural mechanisms for addressing cybercrime in light of its unique characteristics and legal nature. It explores both the traditional and newly developed procedural mechanisms for tackling cybercrime, in addition to assessing the adequacy of traditional procedural mechanisms outlined in the UAE Criminal Procedure Law for addressing such crimes. It also examines whether current UAE laws on combating information technology crimes incorporate updated procedural mechanisms for tackling cybercrime.

The study concluded that the traditional and new procedural rules in UAE law regarding the control of electronic crime are not sufficient to regulate the control of intangible components or digital evidence related to cybercrime. It recommended that the UAE legislator include a special section in the federal penal procedures law dedicated to cybercrime that aligns with the special nature of these crimes, as a comprehensive and accurate alternative due to the dispersion of these procedural rules across various laws. It also recommended establishing special units, departments, or sections to investigate cybercrimes, in addition to adopting specialized training programs to enhance and update the technical and informational skills of judicial authorities in handling cybercrime.

Keywords: Electronic crime, Digital inspection, Information inspection, Seizing digital evidence.

(1) College of Law – University of Sharjah (Sharjah – U.A.E.)
alaleeli7@gmail.com

(2) College of Law – University of Sharjah (Sharjah – U.A.E.)