ضبط الجريمة الإلكتروذية في ظل توجهات السياسة الجنائية

الباحث.محمد عبدالعالي دُوَيج **أ.د. محمد علي عبدالرضا عفلوك**

كلية القانون / جامعة البصرة

Email : dr.moali1965@gmail.com **mohmdir@gmail.com**

الملخص

شَهِدَ العالمُ في القرون الأخيرة ظهورَ تكنولوجيا المعلومات وتطورها المستمر اللامحدود، وما أنتجه على المجتمعات البشرية من الجوانب الإيجابية على مختلف الأصعدة، فجعل العالمُ في دائرة تواصل مستمر، بل إن تطور تكنولوجيا المعلومات انعكسَ أيضا على التعاملات الإدارية، إذ أصبح أداةً مهمةً في تلبيةِ حاجاتِ الدولةِ والمجتمعِ، إلا إن الأمرَ لا يقف عند هذا الدور الإيجابي وحسب، بل أُستغِلَ هذا التطور من قبل المجرمين فأصبح منفذاً لارتكاب جرائمهم، حتى ظهرت الجريمة الألكترونية، مما قابلَ ذلك توجه السياسة الجنائية على المستوى الوطني والدولي لمواجهةِ هذا النوع من الإجرام، إلا إن ضبط هذا النوع من الإجرام يختلف تماماً عن ضبط الجرائم التقليدية لما يخلفه من مشكلات عدة فيمَ يتعلقُ بالجانب الإجرائي سواء على صعيد إجراء التحري أم إجراء معاينة مسرح الجريمة أم إجراء التفتيش أم حفظ الدليل وتحرزه، ولعل ذلك يعود إلى أن ضبط الجريمة الألكترونية يتميز بخصوصيته؛ كونه يرد على محل افتراضي بخلاف الجرائم ذات المحل المادي (التقليدية).

الكلمات المفتاحية : الجريمة الالكترونية، المحل الافتراضي، السياسة الجنائية.

Tuning The Electronic Crime in Shade Directions Criminal Policy

Researcher. Mohammed Abd Al Alally Dweg
Prof.Dr. Mohammed Ail Abdul Reda Aflouk
College of Law / University of Basrah
Email : mohmdir@gmail.com dr.moali1965@gmail.com

Abstract

In recent centuries, the world has witnessed the emergence of information technology and its continuous and unlimited development, and the positive aspects that it produced on human societies at various levels, making the world in a circle of continuous communication. Rather, the development of information technology was also reflected in administrative transactions, as it became an important tool in meeting the needs of the state. And society, however, the matter does not stop at this positive role only, but this development was exploited by criminals and became an outlet to commit their crimes, until the emergence of electronic crime, which corresponded to the direction of criminal policy at the national and international levels to confront this type of crime, but this The type of crime is completely different from the control of traditional crimes because of the many problems that it causes with regard to the procedural aspect, whether in terms of the investigation procedure, the examination of the crime scene, the inspection procedure, or the preservation and preservation of evidence. Default other than physical (traditional) crimes.

key words : Cyber crime, virtual shop, criminal policy.

المقدمة

التعريف بموضوع الدراسة

عاشَ الوجودُ البشري منذ ولادته الظاهرة الإجرامية التي تعدُّ بمثابة آفة لا حدود لها، إذ تستمر كلما استمر وجودُ المجتمعات البشرية، فهي آفة تتطورُ بتطور المجالات البشرية المختلفة فتتخذ شكلَ ذلك التطور، وبظهور تكنولوجيا المعلوماتية التي أصبح من أساسيات الحياة، فأنها لم تقفْ عند حد ظهورها، إنما تمثل عالماً خيالياً لا حدود له يتطور كلما تقدمت الحياةُ والعلم، وبالرغم من مزايا هذا التطور إلا إنهُ لم يخلُ من ثغراتٍ، سمحت لآفة الظاهرة الإجرامية بالدخول اإليه وخرقه من مختلف جوانبه فلم تجعله يمتاز بالإيجابية المطلقة، بل جعلته محلَ قلقٍ لدى البشرية، مما قابل ذلك جملة انعكاسات سلبية، فأصبحت أداة ومسرحاً لارتكاب الظاهرة الإجرامية، إذ إنها أصبحت وسيلةً يلجأ إليها المجرم لارتكاب جريمته من دون عناء، إنما يتطلب منه فقط المعرفة بتقنية تكنولوجيا المعلومات ومداخلها، حتى ظهر ما يسمى **بالجريمة الألكترونية**.

إنَّ ظهور السياسة الجنائية ارتبط منذ القدم بظهور الظاهرة الإجرامية، ومن ثم فهي تتطور بتطور الجريمة؛ لأنها تهدف بالدرجة الأساس إلى مواجهة كل ما يطرأ على المجتمع من ظواهر إجرامية، وبظهور الجريمة الألكترونية أصبحت الحاجةُ ملحةً لمواكبة السياسة الجنائية للتطور التكنولوجي والتدخل من أجل مواجهة الجريمة الألكترونية التي تقع في العالم اللامادي؛ ذلك لأن ضبط هذا النوع من الإجرام بذات الإجراءات المتعلقة بالجرائم التقليدية جعل الأمرُ غيرَ مقبول من ناحية مبدأ الشرعية، فضلاً عن أن السلطات التحقيقية اعتادت على التعامل مع الجرائم التقليدية، مما أثار ذلك تحدياً أمامها في مقابل القصور التشريعي، فضاقت النصوص العقابية التقليدية عن استيعاب هذا النوع المستجد من الإجرام، ولم تكن النصوص الإجرائية أكثر حظاً منها، ولعل ما تقدم يعود إلى عجز أدوات السياسة الجنائية عن مواجهة ضبط الجريمة الالكترونية.

اولاً: أهمية البحث

تكمن أهمية الموضوع في جانبين :- **يتمثل الجانب الأول** في أن الجريمة الالكترونية تعد ظاهرةً إجرامية فهي وليدة التطور التكنولوجي الحديث، لذ أصبحت ظاهرة إجرامية مستمرة باستمرار التطور التكنولوجي، إذ أن أغلب الدول قد اتجهت نحو الحكومة الكترونية، ومن ثم فإن احتمالية تفاقم ظاهرة الجريمة الألكترونية يكاد يكون أمراً محسوماً، **أما الجانب الآخر** فيتمثل بأهمية دور الضبط في التحقيق الجنائي إذ إنّ الضبط يقوم على أدوات عدة تتمثل بالتحري ومعاينة مسرح الجريمة والتفتيش وإثبات وحفظ الدليل، ومن ثم فأن دورَ الضبط في الجريمة الألكترونية يعدُّ من الأمور التي لا يمكن الاستغناء عنها، لذا فإنّ توجه السياسة الجنائية يجب ألا يقتصرَ على تجريم الأفعال الألكترونية وحسب، بل يجب أن يركزَ على ضرورة توافر النصوص الإجرائية الخاصة لمواجهة هذا النوع من الضبط.

ثانياً: مشكلة البحث

تتجلى مشكلة البحث في ظل الجهود التي بذلتها السياسة الجنائية في الآونة الأخيرة على الصعيد الوطني والدولي لمواجهة ظاهرة الجريمة الألكترونية، سواء كانت من خلال صياغة التشريعات الخاصة أو إبرام الاتفاقيات الدولية لتجريم هذه الظاهرة الاجرامية، لكن يبقى التساؤل عن مدى كفاية هذه الجهود التي بذلتها السياسة الجنائية لمواجهة ضبط الجريمة الألكترونية، إذا ما كان يتخلفُ عن ضبط هذا النوع من الجرائم مشكلات عدة؟ فكل ذلك يقودنا إلى تساؤلات عدة يمكن طرحها وبيان تلك المشكلات التي ينتجها ضبط الجريمة الألكترونية بالآتي:

١) مدى طبيعة محل الجريمة الالكترونية؟ ومدى إمكانية تحقق الضبط في الجريمة الألكترونية؟ وهل الضبط يختلف في هذه الجريمة عنه في الجرائم التقليدية؟ إذا ما كان محل الجريمة الالكترونية لا يقتصر على المكونات المادية وحسب، وإنما يمتد إلى أنظمة الحاسب الآلي؟ فضلا عن ذلك فأن لكل جريمة مسرحاً ترتكب فيه، فالتساؤل الذي يطرح نفسه عن مدى إمكانية وجود مسرح للجريمة الإلكترونية؟؛ لكونها ترتكب غالبا في نطاق افتراضي متسع غير مادي؟.

٢) إنّ التفتيش يعد من إجراءات الضبط الذي تستعين به السلطات التحقيقية في إثناء التحقيق وهو يقتصر في البحث عن أدلة الجريمة أو عن مرتكبها، فالتساؤل الذي يطرح نفسه عن مدى إمكانية إجراء التفتيش عن أدلة الجريمة في عالم معلوماتي افتراضي غير مادي؟ ومدى تحقق إمكانية حصول التفتيش في أنظمة معلوماتية غير مملوكة للمجرم، اذا ما امتدت إليها الجريمة من خلال اتصالها بنظام الحاسب الآلي للمجرم عبر شبكة الانترنت؟.

٣) إنّ لكل جريمة دليلاً في إثباتها وغالباً ما يكون دليل الجرائم التقليدية ذا صفة مادية، فالتساؤل يكون عن مدى طبيعة الدليل في الجريمة الألكترونية؟ وما اذا كان ذو صفة افتراضية غير ملموس مادياً، فهل يمكن أن يكون محلا للضبط كغيره من الأدلة الأخرى كما في الجرائم التقليدية؟.

وفي ضوء ما تقدم فإنّ السياسة الجنائية لبعض الدول كالإمارات وقطر ومصر، اتجهت نحو صياغة قانون خاص بالجريمة الألكترونية فأن ذلك يثير الإشكال حول مدى تكامل صياغة تلك القوانين لمواجهة ضبط الجريمة الألكترونية؟ بمعنى مدى نجاح السياسة الجنائية الحديثة لمواجهة ضبط الجريمة الألكترونية، مقارنة بمدى كفاية اعتماد السياسة الجنائية التقليدية كما في العراق على أسلوب تطبيق النصوص الجزائية التقليدية على الجريمة الالكترونية؟ وبناءً على ذلك فأن إشكالية البحث لا تنحصر بصعوبة الضبط المادي لأدوات جهاز الحاسب الآلي، بل بصعوبة الضبط المعنوي المتمثل بالجوانب المعلوماتية والبيانات.

ثالثاً: منهجية البحث

ولأهمية الموضوع قررنا لغرض دراسته من جوانبه المختلفة، أن نعتمد المنهج التحليلي من خلال تحليل النصوص الجزائية المتعلقة بموضوع البحث، فضلاً عن الاعتماد على المنهج القانوني المقارن من خلال إجراء المقارنة بين توجهات السياسة الجنائية لكل من المشرع العراقي والقطري والإماراتي والمصري نحو بيان موقفهم من مواجهة ضبط الجريمة الألكترونية، على أن تتركز المقارنة بين ما تمَّ تشريعه من القوانين الخاصة وبين ما تمَّ اعتماده من النصوص الجزائية التقليدية.

رابعاً: خطة البحث

وتقتضي طبيعة موضوع البحث الإحاطة التامّة بمختلف جوانبه، لذا فإنّ من الضروري ابتداء بيان معنى الضبط و وصولاً إلى بيان محلّه في الجريمة الألكترونية، ليقتضي الأمر بعد ذلك بيان أهم تلك المشكلات التي تنتج عن ضبط الجريمة الالكترونية، ومن أجل بيان كل ذلك فأن الأمرَ يقتضي بنا تناول الموضع في تقسيم ثنائي يتكون من مطلبين على أن يتضمن كل مطلب فرعين.

المطلب الأول/ مفهوم الضبط ومحله في الجريمة الإلكترونية

يعد التحقيق الجنائي الفيصل في الدعوى الجزائية، إذ يعدّ وسيلةَ القضاء في إدانة المتهم او برائته، والذي يراد به "مجموعة من الإجراءات تستهدف التحري عن الأدلة في شأن جريمة ارتكبت وتجميعها من النواحي كافة لتحديد مدى كفايتها لإحالة المتهم إلى المحكمة المختصة"[١]. ويتضح من ذلك أن التحقيق الجنائي ما هو إلا عبارة عن مجموعة إجراءات تتخذها السلطة المكلفة بالتحقيق لغرض الوصول إلى حقيقة الجريمة المرتكبة، وبهذا فأن الإجراءات التي تتخذها الجهة التحقيقية في الجريمة التقليدية لا تختلف عنها في الجريمة الألكترونية، وفي ضوء ذلك يعد الضبط من أهم الاجراءات التي يقوم عليها عمل السلطات التحقيقية في التقصي عن الجريمة، فلا تختلف ممارسته في الجريمة الألكترونية عنه في الجريمة التقليدية، إلا إنه ثمة مشكلات تواجه عملية ضبط الجريمة الألكترونية؛ ونتيجة لأهمية الموضوع سوف نبين في شكل فرعين مفهوم الضبط ومحله في الجريمة الألكترونية، حتى يكونَ منطلقاً اإى المطلب الثاني لنبينَ أهم المشكلات التي تواجه عملية ضبط الجريمة الألكترونية تحت سقف توجهات السياسة الجنائية، وذلك كما يلي:

الفرع الأول/ مفهوم الضبط

يراد بالضبط من **الناحية اللغوية** "الضبط إن ورد على شخص عني بذلك القبض عليه، وإن ورد على شيء فيعني حفظه بالحزم"[٢].

أما من **الناحية الاصطلاحية** فقد تعددت آراء الفقه في وضع تعريف محدد لمعنى الضبط، ولا بأس بالتطرق إلى بعض تلك التعريفات، فمن جانب الفقه المصري فأنه يذهب إلى تعريفه **بأنه** "دقة التحديد، فيقال ضبط الأمر أي تحديده بدقة، وقد يرد الضبط على شخص فيكون المقصود تقييد حرية هذا الشخص في أن يتحرك كما يشاء، وقد يرد على شيء فيكون الهدف هو تصحيح هذا الشأن، والعمل على اعتداله أو الكشف عن هذا الشأن فقط"، بينما يذهب الفقه الفرنسي إلى تعريف الضبط **بأنه** "عبارة عن تلك المكنات التي يمنحها القانون لسلطات الضبط كي تستطيع بموجبها اتخاذ بعض التدابير لمنع التصرفات والأفعال المخالفة للقانون"(٣).

أما من **الناحية الجنائية** فإنَّ الضبط يعدُّ من الإجراءات المهمة التي تتخذها الجهات التحقيقية بصدد جريمة ما، ومما تجدر الإشارة إليه أن الفقه الجنائي اختلف في إيراد تعريف محدد لمصطلح ضبط الجريمة، **فمن جانب** عرّفَ البعض ضبط الجريمة **بأنه** "وضع اليد على الشيء المتصل بالجريمة والمفيد في كشف الحقيقة عنها وعن مرتكبها"(٤). في حين ذهب **جانب آخر** إلى تعريفه **بأنه** " الوسيلة القانونية التي تضع بواسطتها السلطة المختصة يدها على الأدوات جميعها التي وقعت عليها الجريمة أو نتج عنها أو استعملت باقترافها كالأسلحة والأشياء المسروقة"(٥). فضلاً عن ذلك فأن القوانين الإجرائية افتقرت إلى وضع تعريف محدد لمصطلح ضبط الجريمة.

وما يمكن الإشارة إليه أن هناك علاقة وثيقة بين الضبط وعنصر التفتيش، تتمثل بارتباط إجرائي في الغالب؛ وذلك على أساس أن الضبط ما هو إلا غاية التفتيش، إذ إنَّ أغلب شراح القانون ينظرون إلى مصطلحي الضبط والتفتيش معا في الغالب، باعتبار أن التفتيش ينتهي إلى ضبط الأشخاص أو الأشياء الخاصة بالجريمة التي يجري التحقيق فيها(٦). وهذا ما نجده بالفعل في القوانين الإجرائية، إذ تنصُّ غالبا بأنْ يجري التفتيشُ مع ضبط كل ما يتعلق بالجريمة أو أشياء أخرى ممنوعة(٧). مما يترتب على نتيجة هذا الارتباط او العلاقة بين الضبط والتفتيش بأن الضبط لا يرد إلاّ على ما يعدُّ دليلا في الجريمة التي يجري فيها التفتيش عن الأشياء المتصلة بها، فأنه يباشر من أجل الحقيقة المطلقة، بمعنى أن التفتيش مادام يستهدف الحقيقة فإن الضبط يجب أن يرد على أدلة الجريمة كلها سواء أكانت أدلة إدانة أم براءة؛ ذلك لأنَّ كل ما يتم ضبطه في الحالتين يحقق دعامة العدالة الجنائية، مما يفيد معنى الارتباط بين الضبط والتفتيش(٨).

إلاّ إنّه يؤخذ على ما تقدم بأن مصطلحي الضبط والتفتيش مستقلان عن بعضهما في الحقيقة فكما يمكن أنْ يكونَ الضبط أثراً للتفتيش فإنّه يمكن أن يكون أثراً لمعاينة مسرح الجريمة، أو أثراً لعملية التحري، بل وأكثر من ذلك فأن الضبط يمكن أن يردَ بصورة مستقلة عن أي إجراء آخر كضبط أدلة جريمة معينة أو ضبط الأشياء التي يقدمها الشاهد أو المتهم(٩).

وبناءً على ما تقدم **نرى من جانبنا** أن مصطلح ضبط الجريمة يراد به "كل عملية تقوم بها السلطات التحقيقية تهدف بكل وسائلها الوصول إلى كل ما يتصل بمكونات الجريمة من أجل وضع اليد عليها"، بمعنى أن الضبط يرد على الجريمة المشهودة وغير المشهودة؛ ذلك لأنَّ هدف الضبط لا يغدو أن ينحصرَ بوضع اليد على كل ما يتصل بمكونات الجريمة بصرف النظر عن وقت ارتكاب الجريمة هذا من جانب، ومن جانب آخر فأن ضبط الجريمة يرتبط بأدوات تستعين بها السلطات التحقيقية في كشف حقيقة الجريمة وتتمثل هذه الأدوات بالتحري والمعاينة والتفتيش وثبات الدليل وحفظه.

يتضح مما تقدم أن الضبط يرد على الجرائم المادية جميعها ويرتبط بأدوات عدة لا يمكن في الغالب التخلي عنها، وتتمثل بالتحري والتفتيش ومسرح الجريمة وإثبات الدليل وتحرزه، لكن هل بالإمكان أن يردَ الضبط على الجريمة الألكترونية بوصفها جريمةً ذات طبيعة خاصة بالنظر لمحلها الافتراضي؟، وإذا كان بالإمكان ذلك فهل بالسهولة ضبطها دون تخلف مشكلات؟ كل ذلك يقودنا إلى الخوض في الفرع الثاني ووصولاً إلى المطلب الآخر.

الفرع الثاني/ محل الضبط في الجريمة الالكترونية

إن محلَ الجريمةِ الالكترونية يندرج تحت صورتين الأولى تتمثل بمحل الجريمة المرتكبة بوساطة النظام المعلوماتي للحاسب الآلي، بينما الأخرى تتمثل بمحل الجريمة الواقعة النظام المعلوماتي للحاسب الآلي ذاته، مما يعني أن الجريمة الألكترونية قد يكون محلها النظام المعلوماتي ذاته وفي المقابل قد يكون النظام المعلوماتي وسيلة لارتكاب الجريمة التقليدية، فيكون محلها بحسب الشيء الذي تقع عليه الجريمة كالمال أو المستندات ...الخ.

وبعد استقراء تعاريف مصطلح ضبط الجريمة يتضح أن الضبط يرد على الجرائم التقليدية، مما يعني ذلك أن الضبط يرد على الأشياء المادية؛ كون الجرائم التقليدية في الغالب تنصب على محل مادي كسرقة الأموال وتزوير المستندات وغيرها، وهذا ما نصت عليه القوانين الإجرائية إذ أشارتْ هذه القوانين بأن الضبط يرد على الأشخاص أو الأشياء ضمن جريمة مادية(١٠).

وبقدر تعلق الأمر بذلك فأن ضبط الجريمة الالكترونية يدور حول محورين، **الأول** يتمثل بالمحل المادي للجريمة الألكترونية، –أي– إذا وقع السلوك الإجرامي على الأشياء المادية بوساطة نظام الحاسب الآلي، فأن محلَ الضبط في هذه الحالة لا يثير خلافاً، إذ يمكن إنْ يردَ الضبطُ بطبيعة الحالة على الجريمة الألكترونية كغيرها من الجرائم التقليدية، كما ويمكن أن يرد الضبطُ على جهاز الحاسب الآلي ومكوناته؛ لكونها تدخل في المفهوم الماي، **أما المحور الآخر** فأنه يتمثلُ بالمحل الافتراضي للجريمة الألكترونية،– أي– إذا وقع السلوك الإجرامي على البيانات والمعطيات

والبرامج وغيرها إذا ما كانت هذه الأخيرة تحمل قيمةً مادية أو معنوية كالخرائط العلمية أو الفكرية، فأنها تمثل محلاً افتراضياً غير محسوس مادياً، ومن ثم فإن ضبطها يشكل محلَ خلاف على مستوى الفقه الجنائي، لكن السؤال الذي يطرح نفسهُ هل بالإمكان أن يردَ الضبط من الناحية القانونية على المحل الافتراضي للجريمة الألكترونية في ضوء جهود السياسة الجنائية المبذولة على المستوى الوطني والدولي؟.

على صعيد مستوى الفقه الجنائي فقد اختلفت الآراء الفقهية حول إمكانية ضبط المحل الافتراضي غير المادي للجريمة الالكترونية كالبيانات والمعطيات والبرامج والملفات الإلكترونية... الخ، ويمكن بيان هذه الآراء بالآتي :

الرأي الأول: يذهب أنصاره إلى القول بعدم إمكانية ورود الضبط على المحل الافتراضي للجريمة الألكترونية مما يستتبع ذلك عدم إمكانية إجراء التفتيش أيضا عليه، على أساس أن غاية التفتيش هو ضبط الأشياء المادية، ومن ثم فأنه ليس من المتصور أن يردَ الضبط على البيانات والبرامج والمعطيات الألكترونية وغيرها، إلا إذا وسعت غاية التفتيش لتشملَ الأدلة المادية وغير المادية، فيمكن أن يردَ الضبط على المحل الافتراضي(١١).

الرأي الثاني: يذهب أنصاره إلى القول بعدم إمكانية ورود الضبط بصورة مطلقة على المحل الافتراضي للجريمة الالكترونية والمتمثل بالبيانات والمعطيات والبرامج وغيرها، بحجة أنها تفتقر إلى صفة الكيان المادي، كما في رأيهم أنها لا تصلح لأن تكون محلاً للتفيش أيضا، إلا إذا تم تجسيدها في دعامة مادية كتحويلها إلى مطبوعات عن طريق مخرجات جهاز الحاسب الآلي(١٢).

الرأي الثالث: يذهب أنصاره إلى القول بإمكانية خضوع المحل الافتراضي للجريمة الالكتروني والمتمثل بالبيانات والمعطيات والبرامج والملفات الألكترونية...الخ لعملية الضبط، بصرف النظر عمَّ إذا كانت قابلة للإحراز أو لا، ويستندون في ذلك إلى أن المشرع عندما ينص على جواز ضبط أي شيء يتعلق بالجريمة فأن عبارة (الشيء) يجب أن تفسرَ بالمعنى الواسع لتشملَ الأشياء جميعها المرتبطة بالجريمة سواء أكانت ذات دعامة مادية أم افتراضية؟، في حين يستندُ البعضُ من أصحاب هذا الرأي إلى القول بأن عبارة (الشيء) على وفق العلوم الطبيعية يُراد بها كل شيء يشغل حيزاً مادياً في الفراغ فيمكن قياس حيزه، ولما كانت البيانات والبرامج والمعطيات...الخ تشكل حيزاً داخل نطاق ذاكرة نظام الحاسب الآلي، ويمكن قياسها بوحدات الالكترونية مثل (وحدة البايت والميجابايت والجيجابايت)، فأنه بالإمكان أن يردَ عليها الضبط كغيرها من الأشياء ذات الكيان المادي، فهي بهذه الحالة لا تختلف عن الطاقة الكهربائية التي استقرَّ رأي الفقه والقضاء على عدها من الأشياء المادية القابلة للحيازة(١٣).

ومن جانبنا نجري إلى ما آل إليه الرأي الأخير لكون الضبط ورد في القوانين الإجرائية بصورة مطلقة على الأشياء، ومن ثم فلا نجد ما يمنع من ضبط محل الجريمة الألكترونية المتمثل بالبيانات والمعطيات...الخ ، بمعنى أن عبارة (الشيء) وردتْ بصورة مطلقة في القوانين الإجرائية التقليدية، وهذا ما وجدناه جليا عندما نظم المشرع العراقي عملية الضبط والتفتيش في المواد (٩٨-١٠٨) من قانون أصول المحاكمات الجزائية، إذ أورد عبارة (الشيء) بصورة مطلقة، مما يقودنا ذلك إلى القول بالرغم من أن العراق قد اتبع في سياسته الجنائية تطبيق النصوص الموضوعية التقليدية في تجريم الجريمة الالكترونية، فان بإمكان السلطات التحقيقية اجراء الضبط على البيانات والمعطيات...الخ المتمثلة بالمحل الافتراضي للجريمة الالكترونية على وفق النصوص الإجرائية التقليدية، وإن لم تكن مجسدة في كيان مادي بإحدى مخرجات الحاسب الآلي، وإن كان ضبطها لا يكون إلا بالطرائقَ الفنية وتقنية التكنولوجيا الحديثة كنسخها على الأقراص الليزرية أو تخزينها في وحدات تخزين خارجية...الخ، لكن ما تجدر الإشارة إلية أن الجريمة الالكترونية لها خصوصيتها مما يجعل ضبطها على وفق النصوص الإجرائية التقليدية أمراً يكتنفه بعض الغموض والمشكلات.

أما على صعيد مستوى السياسة الجنائية الوطنية فنجد أن بعض الدول كالإمارات بالرغم من اتجاه سياستها الجنائية نحو صياغة قانون خاص بالجريمة الالكترونية، إلا أن هذا القانون يفتقر إلى بيان ما إذا كان بالإمكان ضبط محل الجريمة الالكترونية من قبل السلطات التحقيقية، ومن ثم فأن الأمر لا يختلف عن السياسة الجنائية التي اتبعها المشرع العراقي؛ وذلك من خلال الاعتماد على القوانين الإجرائية التقليدية في إجراء الضبط على الجريمة الالكترونية[١٤]. وإن كان ذلك **يعد من جانبنا** قصوراً في صياغة مثل هذه القوانين، إذ كان يجب أن تصاغَ نصوصها بصورة دقيقة لتناسب خصوصية الجريمة الالكترونية، كما فعلت الدول الأخرى فنجد على سبيل المثال دولة مصر التي اتبعت سياستها الجنائية صياغة قانون خاص، فقد بينت ماهية محل الجريمة الالكترونية وأجازت للسلطات التحقيقية إجراء الضبط عليه متى كان ذلك يساعد في كشف الحقيقة، كما وأجازت إجراء البحث والتفتيش لغرض تحقيق الضبط؛ وذلك على وفق نصوص القانون الخاصة[١٥]. وأيضا نجد المشرع القطري أجاز بدوره ضبط كل ما يتصل بالجريمة الالكترونية على وفق القوانين الخاصة بالجريمة الألكترونية، إلا إنه لم ينص على الضبط كإجراء مستقل كما فعل المشرع المصري وإنما جعل الضبط غاية التفتيش[١٦]. وقد سبق وإن بينا أن الضبط يمكن أن يكون مستقلاً عن التفتيش.

في حين على صعيد مستوى السياسة الجنائية الدولية فهي الأخرى عنيت بموضوع ضبط المحل الافتراضي للجريمة الالكترونية، فنجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة

٢٠١٠ قد أشارتْ إلى إمكانية ضبط البيانات وكل ما تفرزه تقنية المعلومات، كما ونصت على ضرورة تبادل المساعدة بين الدول بصدد ضبط كل ما يتعلق بالجريمة الألكترونية[١٧]. لكن في المقابل لم نجدْ نصوصاً تشير إلى المعنى ذاته في القانون الإماراتي الاسترشادي لمكافحة جرائم تقنية المعلومات ٢٠١٠، وكذلك الحال بالنسبة لاتفاقية بودا بست لسنة ٢٠٠١ إذ لم تنص بصورة صريحة استخدامها لمصطلح (الضبط) على ضبط المحل الافتراضي للجريمة الألكترونية، إلاّ إنهّ من خلال استقراء بعض نصوصها نجدها قد أجازت ضبط المحل الافتراضي المتمثل بالبيانات، إذ استخدمت مصطلح (المصادرة) وهذا الأمر بطبيعة الحال يسبقه الضبط، فلا يتصور حصول مصادرة أشياء من دون ضبطها[١٨].

لذا يمكن تعريف مصطلح ضبط الجريمة الألكترونية **بأنه** "وضع اليد على المكونات المادية والافتراضية للأنظمة المعلوماتية، وكل شيء يفيد في كشف الحقيقة عن الجريمة الالكترونية"[١٩]. وأيضا عرّفهُ البعضُ **بأنه** "وضع اليد على الدعائم المادية المخزنة فيها الالكترونية او المعلومات التي تتصل بجريمة معلوماتية وقعت، وتفيد في كشف الحقيقة عنها وعن مرتكبيها"[٢٠].

وتباعاً لما تقدم فأن نطاق ضبط الجريمة الالكترونية يثير مشكلة، إذ قد لا يكون باستطاعة السلطات التحقيقية عزل البيانات والبرامج والمعطيات...الخ عن أنظمة الحاسب الآلي أو منظومة الشبكة التي تحويها، فلا يكون بيد أفراد سلطات التحقيق من حيلة حيال ضبط النظام أو منظومة الشبكة بشكل كامل، وهذا بدوره يؤدي إلى تعطيل النظام أو المنظومة عن العمل لفترة قد لا تكون محدودة على وفق إجراءات التحقيق الجنائي، مما قد يلحق ذلك ضرراً بالجهة المالكة للنظام أو المنظومة لاسيما وإذا لم تكن هي المتهمة بالجريمة[٢١].

المطلب الثاني/ مشكلات ضبط الجريمة الالكترونية

هناك مشكلات عدة تعيق ضبط الجريمة الألكترونية؛ لكون محلها ينصبُ على البيانات والمعطيات، وتتمثل هذه المشكلات بالعناصر التي يقوم عليها التحقيق الجنائي فلا يتصور قيامه من دونها، وهي كل من التحري والتفتيش وإثبات الدليل وحفظه، وعليه سوف نسلط الضوء على تلك المشكلات في فرعين كما يلي:

الفرع الأول/ مشكلات الضبط المتعلقة بالتحري والمعاينة

من المتعارف عليه أن التحري يعدُّ نقطة البداية لإجراء التحقيق في كل جريمة ويرتبط ذلك بدوره في معاينة مسرح الجريمة، إذ إن لكل جريمة مسرحها، لكن الأمر يدق عند إجراء التحري عن المحل الافتراضي للجريمة الالكترونية ومعاينته؛ لأن الأمر يختلف عن نظيراتها من الجرائم الأخرى، مما ينتج عن ذلك مشكلات عدة تتعلق بإجراء التحري والمعاينة، ويمكن بيانها بالآتي:

أولا: المشكلات المتعلقة بإجراء التحري

يعد إجراء التحري من الأمور الأساسية التي يستند إليها عمل سلطات التحقيق في تحريك الدعوى الجزائية، إذ إنّها تعد وسيلة للكشف عن الجريمة، وبهذا فأن التحري يتصل بضبط الجريمة بصورة عامة، مما يعني أن الجريمة الالكترونية كأي جريمة تقليدية تمر بمرحلة التحري إلا إن عملية التحري فيها تختلف من حيث كيفية القيام بها، والتي يراد **بها** " اجراءات تتخذها الشرطة للكشف عن الجرائم ومعرفة مرتكبيها، وجمع كل ما يتعلق بها من معلومات لازمة"[٢٢]. يتضح من استقراء ذلك أن عملية التحري تعد مرحلة تمهيدية لتحريك الدعوى الجزائية، إذ إنهّا تهدف إلى جمع المعلومات عن أدلة الجريمة ومرتكبيها، مما يعني أن عملية التحري تتصل بها الإجراءات التحقيقية كافة كمعاينة مسرحة الجريمة وحفظ الدليل وإجراء التفتيش، وبهذا **نرى من جانبنا** أن عملية التحري يراد **بها** "تلك الإجراءات الممنوحة للسلطات التحقيقية لمواجهة الجريمة المرتكبة من خلال البحث عنها وضبط ادلتها ومرتكبيها".

وبهذا الصدد فإن عملية التحري في ضبط الجريمة الالكترونية تثير مشكلات عدة، إذ إن من واجب أفراد السلطات التحقيقية القيام بالتحريات اللازمة متى ما اتصل علمهم بوقوع الجريمة عن طريق البلاغ، ولذا تثار مشكلة البلاغ[٢٣] عن الجريمة الالكترونية إذ يعد البلاغ نقطة البداية لعملية التحري من جانب السلطات التحقيقية، فلا يتصور قيام الأخيرة بإجراء التحري من دون وصول علمها بوقوع الجريمة، ومن ثم فإن محل الجريمة الالكترونية ما هو في الغالب إلا محل افتراضي، بمعنى يحتاج التحري بشأنها حصول البلاغ عنها أو كشفها بالصدفة[٢٤] . لكن المشكلة تثار عند عدم قيام المجني عليهم بالإبلاغ عن الجريمة الالكترونية ولأسباب معينة، ويظهر طبعاً ذلك جلياً إذا ما وقعت الجريمة الألكترونية على المؤسسات المالية والشركات، إذ إنها تتردد في البلاغ عن الجريمة خوفاً منها على سمعتها وفقد الثقة بها مما قد يلحقها الضرر[٢٥]. ومن ثم فأن ذلك يشكل عائقاً أمام قيام السلطات التحقيقية بإجراء عملية التحري، مما يعد ذلك بدوره مشكلة تواجه السلطات التحقيقية إثناء ضبط هذه الجريمة.

ومما تجدر الاشارة إليه ان وصول علم السلطات التحقيقية بوقوع الجريمة التقليدية واجراء التحري عنها، يكون أوسع نطاقا عنه في الجريمة الالكترونية، ذلك لان اتصال علم السلطات التحقيقية بالجريمة التقليدية يكون بطرق عدة فقد يكون عن طريق تقديم شكوى من المجني عليه او اخبار يقدم من قبل اي شخص علم بوقوعها او من قبل الادعاء العام[٢٦]. على خلاف الجريمة الالكترونية التي ينحصر البلاغ فيها بحسب طبيعتها بالمجني عليه، فمن الصعب تصور علم الغير بوقوعها، لأنها جريمة مستترة غالبا لكونها تتعلق بالبيانات والمعطيات الخاصة بالمجني عليه، لكن

السؤال الذي يطرح نفسه هل يكفي الاعتماد على وسائل البلاغ التقليدية كي تتمكن السلطات التحقيقية من اتصال علمها بالجريمة الالكترونية واجراء عملية التحري عنها؟

ان السياسة الجنائية للدول اتجهت نحو اعتماد أنماط مختلفة في مواجهة الجريمة الالكترونية، فالنسبة للدول التي اعتمدت سياسة تطبيق النصوص التقليدية كالعراق في تجريم الجريمة الالكترونية، ولم يكن حينها بيد القضاء من حيلة حيال تطبيق تلك النصوص على هذا النوع المستجد من الاجرام بالرغم من ان تطبيق تلك النصوص يعد خروجا عن مبدأ الشرعية، فان وسائل البلاغ اي وسائل وصول علم السلطات التحقيقية بارتكاب الجريمة الالكترونية لا تختلف عن الجريمة التقليدية لكون الجريمتين تخضع لنص جنائي واحد، وذلك لعدم وجود تشريع اجرائي خاصة شرع لأجلها، ومن ثم فليس بيد السلطات التحقيقية حيلة من تطبيق النصوص الاجرائية التقليدية اثناء اجراء التحري عن هذا النوع من الجرائم، بالرغم من ان تلك السلطات التحقيقية قد اتجهت في العراق نحو البلاغ الرقمي من خلال وضع مواقع الكترونية للبلاغ عن الجريمة الالكترونية، مع ذلك **نرى من جانبنا** ان الاعتماد على الوسائل التقليدية في البلاغ عن الجريمة الالكترونية يعدَّ أمرا ليس كافيا ووافيا بما ينسجم وطبيعة الجريمة الالكترونية.

لكن يمكن القول إن وسائل اتصال علم السلطات التحقيقية المختصة بالنظر في الجريمة الألكترونية بالنسبة للدول التي اتبعت سياستها الجنائية صياغة تشريع خاص كالإمارات ومصر وقطر، يجب انُ تحدد ضمن نصوص التشريع الخاص بالجريمة الالكترونية وهذا ما لم نجده في تلك التشريعات، إذ إن بعض تلك الدول كالإمارات ومصر لم تختلف عن الدول التي اتبعت سياسة تطبيق النصوص التقليدية، فيمَ يتعلق بالبلاغ عن الجريمة الالكترونية، إذ لم تتضمن قوانينها الخاصة ما ينظم عملية البلاغ عن الجريمة الالكترونية، بالرغم من انها قد تضمنت بعض النصوص الإجرائية[٢٧]. وبخلاف ذلك نجد المشرع القطري قد حدد وسيلتين تسهل عملية اتصال علم السلطات التحقيقية بالجريمة الالكترونية مما يسهل عملية التحري عنها، فقد ألزم أجهزة الدولة والهيئات التابعة لها بضرورة سرعة الإبلاغ عن الجريمة الإلكترونية في حال اكتشافها، وأيضا ألزم مزودي خدمة الانترنت بضرورة تزويد الجهات التحقيقية بالمعلومات كافة التي تساعد في كشف الجريمة، كما وأشار إلى وسيلة أخرى تمثلت بإعفاء المجرم من العقاب إذا ما بادر بالبلاغ عن جريمة ارتكبها بالمساهمة مع غيره[٢٨].

<u>أيضا ومن المشكلات</u> التي تعيق عملية التحري في ضبط الجريمة الالكترونية نقص الخبرة لدى أفراد السلطات التحقيقية، إذ أن الجريمة الالكترونية تتسم بحداثة أساليبها حيث تواكب تطور التكنولوجيا المستمر[٢٩]. فضلاً عن أنها ترد على محل افتراضي يتمثل بالبيانات...الخ التي يصعب التعامل معها بصورة مشابهة للمحل المادي كما في الجرائم التقليدية، الأمر الذي يجب معه

أن يكون أفراد سلطات التحقيق على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي وتقنية المعلومات بما يسهل عملية الوصل للدليل الافتراضي بين الكم المعلوماتي الهائل، وخلاف ذلك سوف يولد صعوبات كبيرة في أثناء التحري عن الجريمة الالكترونية، مما يؤثر بطبيعة الحال على ضبطها، الأمر الذي يتطلب إعدادَ دورات تدريبية وتأهيلية لأفراد سلطات التحقيق لمعرفة كل ما يتعلق بتقنية المعلومات وأنظمة الحاسب الآلي، إذ إن عملية التحري تهدف بكل مقوماتها للحصول على أكبر قدر ممكن من المعلومات عن الجريمة في غضون فترة قصيرة نسبياً فيمَ يتعلق بالجريمة الالكترونية(٣٠).

إن أكثرَ ما يجعل هذه المشكلة تعقيداً هو عدم النص على تطوير مهارات المحقق في التحري عن هذه الجريمة في الدول التي اعتمدت سياستها الجنائية على تطبيق النصوص التقليدية على الجريمة الالكترونية كالعراق؛ وذلك لعدم وجود تشريع خاص يحدد بصورة دقيقة الجهة التي تملك حق التحري عن الجريمة الالكترونية وتطوير افرادها بمعرفة تقنية المعلومات، وهذا مما ينعكس سلبا بطبيعة الحال على أرض الواقع، ومع ذلك فلا يختلف الأمر بالنسبة للدول التي اتبعت سياستها الجنائية صياغة تشريعات خاص كالإمارات وقطر ومصر، إذ لم تنص تلك القوانين الخاصة على إخضاع أفراد السلطات التحقيقية لدورات تدريبية.

ولعل من أهم المشكلات المتعلقة بالتحري عن الجريمة الالكترونية، هو عدم وجود آلية معينة أو إجراءات خاصة بالتحري تواكب المحل الافتراضي لها، إذ لم تتضمن القوانين الخاصة التي شرعتها بعض الدول كالإمارات لمواجهة هذا النوع من الإجرام، الإجراءات التي يجب على السلطات التحقيقية اتباعها عند التحري عن الجريمة الالكترونية، على خلاف المشرع المصري والقطري اذ نص كل منهما على الاجراءات التي تتعلق بالتحري، فقد أجازا للسلطات التحقيقية جمع وحفظ البيانات والمعلومات المتعلقة بأنظمة الحاسب الالي محل الجريمة، فضلا عن النص على ضبطها وإجراء التفتيش والاستعانة بالخبراء وأيضا حجب المواقع محل الجريمة ووصولاً إلى تحرير محضر بتلك الاجراءات كلها(٣١).

وعليه فإذا كان بالإمكان أو بالضرورة رجوع المحقق إلى النصوص الإجرائية التقليدية في إجراء عملية التحري عن الجريمة الالكترونية، لعدم وجود نصوص إجرائية في القوانين الخاصة بهذا النوع من الإجرام، فهل تعد تلك الوسائل التقليدية كافية للتحري عن الجريمة الإلكترونية، لاسيما وإنها تنصب على محل افتراضي، فضلا عن أنها ترتكب في الغالب من مجرم مجهول يقوم عادة بمسح آثار الجريمة ؟.

وبما أن القوانين الخاصة بالجريمة الألكترونية التي شرعتها بعض الدول كالإمارات، وكذلك الحال بالنسبة للدول التي اعتمدت النصوص الموضوعية التقليدية في تجريم الجريمة الالكترونية كالعراق فأنها لم تتضمنْ نصوصاً إجرائية خاصة، **فنرى من جانبنا** بأن ليس بيد القضاء والسلطات التحقيقية حيلة من تطبيق النصوص الإجرائية في أثناء إجراء التحري عن هذا النوع من الإجرام[٣٢]؛ ذلك لأن القوانين الإجرائية تعد قوانين عامة تطبق على كل مالم يرد فيه النص في القوانين الخاصة، وإن كان هذا الأمر يؤدي بطبيعة الحال إلى التوسع في تفسير تلك النصوص ليؤدي في النهاية إلى الخروج عن مبدأ الشرعية الإجرائية كما سوف نبين ذلك في نهاية المبحث.

وترتيبا على ذلك **نرى من جانبنا** إن وسائل التحري المنصوص عليها في القوانين الإجرائية التقليدية لا تكفي للتحري عن الجريمة الألكترونية؛ لان هذه الجريمة تنصب على محل افتراضي يتمثلُ بالبيانات والمعطيات ومن ثم فأن التعامل معها لا يكون بسهولة التعامل مع المحل المادي هذا من جانب. ومن جانب آخر فإن الجريمة الألكترونية يصعب معها تحديد الاختصاص المكاني، فقد يرتكب السلوك الإجرامي في مكان معين مروراً بمكان آخر إلى أن تتحقق نتيجته في مكان آخر[٣٣]. الأمر الذي يتطلب صلاحياتٍ واسعة لأفراد سلطات التحقيق كمنح صلاحية إجراء المراقبة عن طريق التقنيات الالكترونية أو التنصت على المكالمات ورسائل مواقع التواصل الاجتماعي أو القيام بإرسال برمجيات إلى خوادم مختلفة بقصد التوصل إلى مرتكبي الجريمة، بالرغم من أن هذا الأمر قد يؤدي إلى المساس بحرمة الحياة الخاصة لغير المتهم[٣٤].

ثانيا : المشكلات المتعلقة بإجراء المعاينة

عندما ترتكب أية جريمة بصورة عامة فأن الجاني في أغلب الأحوال يترك خلفه أدلة تدل على شخصيته الإجرامية وكيفية ارتكابه للجريمة، فيبقى هذا الدليل في مكان وقوع الجريمة ويطلق على هذا الدليل بالشاهد الصامت والذي قد يكون عرضة للهلاك مما يجب على السلطات التحقيقية حمايته من خلال الإسراع في معاينة مسرح الجريمة[٣٥].

وبيد أن لكل جريمة مسرحاً ترتكب فيه ويعد هذا الأخير جزءاً لا يتجزأ من مكونات الجريمة، إذ قد يكون حجر الزاوية للبحث عن وقوع الفعل الجرمي أو نفي، فتبرز أهميته في بيان كيفية وقوع الجريمة والظروف المحيطة بها ومدى علاقتها بالمتهم، كما ويلقي الضوء على الأماكن التي يجب فيها إجراء التفتيش وضبط أدلة الجريمة أيضاً، وعليه **يراد بمسرح الجريمة** "المكان أو مجموعة الأماكن التي تشهد مراحل تنفيذ الجريمة واحتوائه على الاثار المختلفة عن مرتكبها ويعتبر ملحقا لمسرح الجريمة كل مكان شهد مرحلة من مراحلها المتعددة"[٣٦].

يتضح من استقراء ما تقدم أن مسرح الجريمة يعد مرآة السلطات التحقيقية في معرفة كيفية وقوع الجريمة وجمع أدلتها، كما ويتضح أن مسرح الجريمة يتمثل بكل مكان وقع فيه أي فعل من

أفعال السلوك الجرمي، مما يعني أن مسرح الجريمة ينصب على مكان مادي يدرك بالحواس، وبما أن لكل جريمة مسرحها، ففي المقابل يجب أن يكون للجريمة الالكترونية مسرحٌ ترتكبُ فيه أسوة بنظيراتها من الجرائم الأخرى، لكن الأمر ليس سهلا فالجريمة الالكترونية لا ترتكب في مكان مادي يمكن إدراكه بإحدى الحواس؛ ذلك لأنها ترتكب في ظل محل افتراضي لاوجود له في العالم المادي، مما قد يؤدي ذلك إلى خلق مشكلات عدة تتعلق بمسرح الجريمة الالكترونية سواء ما تعلق بمعاينة السلطات التحقيقية لمسرح الجريمة، أو ضبط ما يتم معاينته من الأدلة ويمكن بيان تلك المشكلات بالآتي:

١) يفيد مسرح الجريمة في معرفة كيفية وقوع الجريمة والظروف المحيطة بها، لذا يقتضي التحقيق الجنائي ضرورة قيام السلطات التحقيقية في أغلب الأحوال بإجراء معاينة مسرح الجريمة، **ويراد بالمعاينة** "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه كيفية وقوعها، ويجمع آثارها التي تفيد في كشف الحقيقة [٣٧].

ويتضح من ذلك إن لمعاينة مسرح الجريمة أهمية كبيرة في مجال التحقيق الجنائي في أغلب الجرائم، اذ تساعد المعاينة على معرفة الأسلوب الذي وقعت فيه الجريمة وتحديد مكان وزمان وقوعها، لكن بقدر تعلق الأمر فأن معاينة مسرح الجريمة الالكترونية هو ليس بالأمر السهل مقارنة بالجرائم التقليدية؛ ذلك لآن معاينة مسرح الجريمة الالكترونية تندرج تحت **صورتين الأولى** تتمثل بمعاينة المكونات المادية كمعاينة أجهزة الحواسيب الآلية وملحقاتها، وهذه الحالة لا تثير الاشكال فقد يترك الجاني بصماته على تلك المكونات المادية، ومن ثم تسري القواعد العامة على تلك المعاينة لكونها تحصل خارج البيئة الافتراضية للجريمة الالكترونية[٣٨].

أما الصورة الأخرى فأنها تتمثل بمعاينة المكونات المعنوية أو الافتراضية أي المعاينة داخل البيئة الالكترونية، ولما كانت الجريمة الألكترونية تقع على محل افتراضي فأن ذلك سوف يقابله بطبيعة الحال إجراء المعاينة الافتراضية أيضا؛ ذلك لأن الجريمة الالكترونية التي يكون محلها نظام الحاسب الآلي ذاته لا تترك غالبا آثاراً مادية كقيام أحد الموظفين بالتلاعب في البيانات الالكترونية المتعلقة بالنظام المالي لدائرته، وبما أن محل الجريمة الألكتروني يتمثل بالنظام المعلوماتي للحاسب الآلي فأن كثيراً ما يتردد أشخاص آخرون على مسرح الجريمة خلال الفترة ما بين وقوع الجريمة واكتشافها مما يؤدي ذلك الى اتلاف معالم الجريمة وضياعها ، وهذا الامر يقتضي من السلطات التحقيقية الإسراع بمعاينة مسرح الجريمة الالكترونية[٣٩].

ونرى من جانبنا إن المعاينة الافتراضية لمسرح الجريمة الالكترونية، لا يمكن أن تسريَ عليها النصوص الإجرائية التقليدية، إذ إنّ هذه النصوص تشترط حصول المعاينة والانتقال الحسي

الى مسرح الجريمة، ومن ثم فليس بالإمكان تحقق هذه المعاينة الحسية في مسرح الجريمة الالكترونية، فضلا عن ذلك فان هذه النصوص تشترط حضور المتهم والمشتكي أو حضور وكيلهم أو شهود في حال غيابهم(٤٠). فالسؤال الذي يطرح نفسه كيف يمكن إجراء الكشف الحسي وبحضور من فرض القانون حضورهم، وخصوصاً ما إذا امتدت المعاينة إلى أنظمة حواسيب آليه لغير المتهم موجودة في مكان بعيد سواء أكان داخل حدود الدولة أم خارجها؟ وفي الحقيقة هناك آراء عدة طرحها الفقه الجنائي حول هذا الامتداد سوف نبينها لاحقا عند التطرق إلى المشكلات المتعلقة بالتفتيش.

أما بصدد موقف السياسة الجنائية من ذلك فنجد هذه المشكلة تظهر بصورة جلية في الدول التي اتجهت سياستها الجنائية نحو اعتماد النصوص التقليدية في تجريم الجريمة الألكترونية كالعراق، ولم يختلف الحال بالنسبة لبعض الدول التي اتجهت سياستها الجنائية نحو صياغة قوانين خاصة بالجريمة الألكترونية كالإمارات وقطر ومصر، وهذا بطبيعة الحال يشكل نقصاً حاداً في صياغة تلك القوانين الخاصة، إذ لم تنصْ صراحة فيمَ اذا كان بالإمكان إجراء معاينة مسرح الجريمة، لكن يمكن الاستدلال من نصوص تلك القوانين أنها قد أجازتْ إجراء المعاينة عندما سمحت بإجراء البحث والتفتيش عن أدلة الجريمة وضبطها؛ لآن هذه الإجراءات جميعها لا يمكن أن تتحققَ فيه دون معاينة مسرح الجريمة أو البيئة الافتراضية(٤١). باستثناء المشرع الاماراتي فأنه لم يُشر إلى المعاينة لا بصورة صريحة ولا ضمنية. وفي السياق ذاته أشارت كل من اتفاقية بود ابست لسنة ٢٠٠١ والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠وبصورة ضمنية إلى إمكانية إجراء المعاينة على مسرح الجريمة الالكترونية(٤٢).

٢) إن الغاية التي يسعى إليها المحقق عند معاينة مسرح الجريمة هو معرفة كيفية وقوعها والظروف التي أحيطت بها، وقد تسفر هذا الأمور عن ضبط أشياء توجد في نطاق مسرح الجريمة والتي تشكل دليلا لإثباتها، ومن ثم فأن إثبات الدليل وحفظه في الجريمة الكترونية بصورة عامة يؤدي إلى العديد من المشكلات، بمعنى أن الغاية من معاينة مسرح الجريمة هو الحصول على الدليل، لكن كيف يتم الحصول على ذلك الدليل في البيئة الألكترونية وكيف يتم حفظه ونقله اذا ما تمثل بالبيانات والبرامج والمعطيات...الخ؟ سوف نبين ذلك عند الحديث عن المشكلات المتعلقة بالدليل.

الفرع الثاني/ مشكلات الضبط المتعلقة بالتفتيش والدليل المرئي

يسفر عادة عن كل من إجراء التحري ومعاينة مسرح الجريمة نتائج تتمثل في التفتيش والحصول على الدليل، إذ إن كلاً من التفتيش وإثبات الدليل وحفظه يتصلان اتصالاً وثيقاً بإجراءات

التحري والمعاينة مما يجعلهما إحدى أدوات الضبط، لذا سوف نتناول في هذا الفرع المشكلاتِ المتعلقة بإجراء التفتيش في الجريمة الالكترونية، ووصولا بعد ذلك لمعرفة الدليل المرئي وبيان المشكلات التي تتعلق بإثباته وحفظه، كالآتي :

أولا: المشكلات المتعلقة بإجراء التفتيش

يعد التفتيش من الأمور الجوهرية التي يستند إليها عمل السلطات التحقيقية في أثناء إجراء التحقيق في جريمة ما، فقد يقتضي التحقيق الجنائي تفتيشَ شخص المتهم أو محل إقامته او أيّ مكان يتصل بأدلة الجريمة، ومن ثم فأنه يعد من أخطر الإجراءات التحقيقية لما يترتب عليه من انتهاكات للحياة، ولذا فأنه **يراد به بوجه عام** "إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جُنحة يتحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص؛ وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقاً لإجراءات قانونية محددة"(٤٣). ويتضح من استقراء التعريف السابق أن للتفتيش علاقة وثيقة بأدلة الجريمة، إذ لا يتصور حصول التفتيش من دون البحث عن أدلة الجريمة، بمعنى أن التفتيش ما هو إلا وسيلة للإثبات المادي، –أي– إن التفتيش كإجراء يستهدف ضبط الأشياء المادية المتصلة بالجريمة، ولذا بقدر تعلق الأمر فأن التفتيش يختلف في الجرائم التقليدية عنه في الجريمة الألكترونية؛ ذلك لأن الأخيرة كما هو معلوم تقع في أغلب الأحوال في محل افتراضي يتمثل بالبيانات والبرمجيات...الخ، وهذا المحل بطبيعة الحال ليس له مظهر مادي ملموس في العالم الخارجي، مما يخلق هذا الأمر صعوبة في إجراء التفتيش داخل هذا النطاق الافتراضي(٤٤).

وعليه فأن التفتيش في الجريمة الألكترونية يدور حول محورين، يتمثلُ **المحور الاوُل** بالمكونات المادية للحاسب الآلي، وهنا لا تثار أية مشكلة تتعلق بإجراء التفتيش، إذ يمكن تفتيش المكونات المادية للحاسب الآلي لغرض البحث عن أدلة الجريمة أو عن مرتكبها، فيخضع التفتيش في هذا المحور لحكم القواعد التقليدية(٤٥).

إلا إن المشكلة تثار في **المحور الآخر** المتمثل بالمكونات الافتراضية لمحل الجريمة الألكترونية، إذ إن هناك مشكلات عدة تتعلق بإجراء التفتيش في تلك المكونات، فالسؤال الذي يطرح نفسه عن مدى إمكانية خضوع تلك المكونات للتفيش وفقا لنظيراتها من المكونات المادية؟.

لقد ثار الخلاف بين فقهاء القانون الجنائي بصدد إمكانية ضبط المكونات الافتراضية للجريمة الألكترونية، والذي أسفر في النهاية إلى إمكانية إجراء التفتيش، أما على المستوى التشريعي فنجد الدول التي اتجهت سياستها الجنائية نحو صياغة قوانين خاصة كقطر ومصر فقد أشارت ضمن نصوص قوانينها الخاصة إلى إمكانية إجراء التفتيش داخل أنظمة الحاسب الآلي بما يتضمنه

من برامج وبيانات ومعطيات وملفات...الخ[٤٦]. على خلاف ذلك نجد بعض تلك الدول كالإمارات بالرغم من صياغتها لقانون خاص بالجريمة الألكترونية، إلا إن ذلك القانون لم يُشرُ إلى إمكانية إجراء التفتيش عن هذه المكونات، وهي بذلك لا تختلف عن السياسة الجنائية للمشرع العراقي الذي اعتمد على القوانين التقليدية في مواجهة هذا النوع من الجرائم، ومن ثم فأنه يتم الاعتماد على القوانين الإجرائية التقليدية لإجراء التفتيش في تلك المكونات الافتراضية، بالرغم من أن ذلك قد لا يحقق الغرض المرجو من التفتيش، وقد يصعب معه إجراء التفتيش.

ويتضح من ذلك ان بالإمكان اجراء التفتيش على المكونات او المحل الافتراضي للجريمة الالكترونية، الا إنّ هذا الأمر ليس بتلك السهولة، إذ ثمة مشكلات تتعلق بإجراء التفتيش في تلك المكونات منها ما يتعلق بمكان اجراء التفتيش وأخرى تتعلق بنطاق التفتيش، فضلا عن تلك الصعوبة المتعلقة بالإجراءات التي يستلزمها هذا التفتيش.

ان الطبيعة التي تتميز بها أنظمة الحواسيب الآلية إنها تتصل ببعضها البعض من خلال شبكة الانترنت، فان من شأن ذلك ان يجعل أدلة الجريمة الالكترونية في نظام حاسب آلي موجودة في مكان آخر غير المكان والحاسب الذي ارتكبت فيه الجريمة كما لو ارتكبت الجريمة عبر البريد الالكتروني، وقد يكون بالإمكان الوصول الى أدلة الجريمة عن طريق الحساب الآلي ذاته الذي ارتكبت بواسطته او عن طريق حاسب أخر، مما يخلق ذلك أزمة تتعلق بتحديد الاختصاص القضائي، بمعنى هل يمكن أن يمتد أذن التفتيش إلى حواسيب أخرى مرتبطة بذلك الحاسب الآلي المعني بالتفتيش؟ فقد يكون هذا الامتداد داخل دولة واحدة وقد يمضي قدما إلى دول أخرى بحثاً عن تلك الأدلة المتمثلة بالبيانات والمعطيات...الخ؟ وقد يكون هذا الامتداد إلى حاسب آلي لا يملكه الجاني مما قد يؤدي التفتيش فيه إلى انتهاك الخصوصية؟ [٤٧]. وتظهر هذه المشكلة بصورة جلية في الدول المعتمدة على تطبيق القوانين الاجرائية التقليدية في إجراء التفتيش وتلك التي لم تنظم للاتفاقيات الدولية، ولغرض إيضاح ذلك فإن هناك صورتين نبينها كما يلي:

<u>الصورة الأولى:</u> تتمثل باتصال الحاسب الآلي للمتهم بحاسوب آخر مملوك له أو لغيره داخل إقليم الدولة الواحدة، وهذا بطبيعة الحال سوف يؤدي إلى خلق مشكلة، ففي هذه الحالة هل يقتصر التفتيش على الحساب الآلي للمتهم وحسب أو بالإمكان أن يمتد إلى الحواسيب الأخرى التي تقع خارج الاختصاص القضائي لمكان ارتكاب الجريمة؟[٤٨]. بالرجوع إلى القواعد الإجرائية التقليدية بهذا الخصوص، نجدها لا تجيز تفتيش غير شخص المتهم ومنزله إلا بعد استحصال الأذن من السلطات المختصة، ومن ثم فأنه يجوز أن يمتدَ التفتيش إلى مكان آخر مملوك للمتهم إذا ما وجد فيه حاسب آلي آخر، إلا إن الأمر ليس بهذه السهولة عندما يتعلق التفتيش بحاسب آلي مملوك للغير أو للجاني موجود في مكان غير مملوك للجاني، فمن البديهي وبحسب طبيعة القواعد التقليدية

فأنه لابد من استحصال الأذن من السلطة المختصة لإجراء التفتيش فيه[٤٩]. غير أن هذا الإجراء في العادة يتطلب وقتا، الأمر الذي يمكن أن يترتب عليه ضياع معالم أدلة الجريمة، كما أن الجاني قد يجدها فرصةً لإخفاء أدلته بصورة سريعة، إذ قد يجد المكلف بالتفتيش ضرورة الدخول إلى نظام حاسب آلي موجود في مكان غير مملوك للمتهم في أثناء قيامه بالتفتيش، لذا جرى الفقه الألماني نحو إمكانية امتداد التفتيش عن البيانات والمعطيات والبرامج...الخ الموجودة في نظام حاسب آلي في مكان آخر سواء أكان مملوكا للمتهم أم لغيره؟، مستنداً في ذلك على المادة ١٠٣ من قانون الإجراءات الجزائية الالماني[٥٠].

ومن جانبنا نجري إلى ما وصل إليه الفقه الألماني من ضرورة امتداد أذن التفيش، ولهذا نرى ضرورة معالجة هذا الأمر؛ ذلك لأن الاعتماد على القواعد الإجرائية التقليدية في هذا الشأن سيؤدي بطبيعة الحال إلى التوسع في تفسير تلك القواعد بشكل غير مألوف، فضلا عن ذلك فأن هذا الامرَ سيؤدي إلى ضياع أدلة الجريمة الالكترونية إذا ما وُجِدَ المكلفُ بالتفتيش نفسه أمام ضرورة استحصال إذن جديد من السلطة المختصة، وقد نجد ظهور هذا الأمر بصورة جلية في العراق لاعتماده على سياسة تطبيق النصوص التقليدية، ولابد أيضا من الإشارة إلى أن وضع المشرع الاماراتي لا يختلف عن وضع المشرع العراقي، بالرغم من تشريعه قانوناً خاصاً ، إلا إن ذلك القانون لم يتضمن ما يشير إلى موضع التفيش كما أشرنا سابقا، على خلاف ذلك نجد كلاً من المشرع القطري والمصري قد أشارَ في القانون الخاص بتجريم الجريمة الألكترونية إلى إمكانية امتداد أذن التفتيش من دون الحاجة الى أذن آخر بالتفتيش شريطة أن يتعلقَ الأمرُ بالجريمة[٥١].

<u>الصورة الثانية:</u> تتمثل باتصال الحاسب الآلي للمتهم بحاسب آخر موجود في مكان خارج نطاق حدود الدولة، إذ إن المجرم المعلوماتي يتميزُ في الغالب بذكاء ومعرفة جيدة بتقنية المعلومات، مما ينعكس ذلك على طريقة إخفائه لأدلة جريمته بصورة يصعب معها اكتشافها، فقد يسعى إلى تخزين البيانات والمعطيات...الخ محل الجريمة في حاسب آلي موجود خارج الدولة محل ارتكاب الجريمة؛ وذلك عن طريق استغلاله شبكة الانترنت، مما يشكل ذلك عائقاً أمام السلطات التحقيقية في إجراء التفتيش في حواسيب آلية موجودة خارج حدود الدولة، إذ إن امتداد التفتيش في هذه الصورة يختلف تماماً عن الصورة السابقة، لتعلقها بسيادة الدول الأخرى[٥٢].

فقد اختلفت آراء الفقه الجنائي بين مؤيد ومعارض حول إمكانية امتداد التفتيش إلى أنظمة حواسيب آلية موجودة خارج حدود الدول، إذ **جرى بعض الفقه** إلى القول بعدم إمكانية حصول هذا الأمر بذريعة انطوائه على انتهاك سيادة الدولة المقابلة، وكالعادة على خلاف ذلك **جرى جانب آخر** من الفقه إلى القول بإمكانية حصول مثل هذا الامتداد للتفتيش شريطة أن يتمَ ذلك بموجب اتفاقية

خاصة تجيز هذا الامتداد بين الدول الأطراف أو وجود أذن من الدولة المقابلة[٥٣]. **ومن جانبنا** نجري إلى ما ذهب إليه الرأي الأخير؛ ذلك لأن عدم وجود اتفاق خاص بين الدول سيؤدي هذا الامتداد بطبيعة الحالة إلى انتهاك خصوصية وسيادة الدولة المقابلة.

ومما تجدر الإشارة إليه أن اتفاقية بودا بست لسنة ٢٠٠١ أخذت بما اتجه إليه الرأي الثاني، إذ أجازت لدول الأطراف إمكانيةَ إجراء التفتيش أو الدخول إلى أنظمة حواسيب موجودة في دولة طرف في الاتفاقية من دون الحصول على إذنها، شريطة أن يتعلق التفتيش بمعلومات وبيانات متاحة للجميع، واذا ما كانت تلك البيانات مملوكةً لأحد الأشخاص، فلا بد من استحصال موافقته للكشف عن تلك البيانات والمعلومات، وبالمعنى ذاته أجازتْ أيضا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠ للدول الأطراف بناء على طلب تقدمهُ الدولةُ لإجراء التفتيش في النظم المعلوماتية الموجودة في أقليم دولة أخرى طرف في المعاهدة[٥٤]. وتجدر الاشارة الى ان العراق قد انضم الى الاتفاقية العربية بموجب قانون التصديق رقم ٣١ لسنة ٢٠١٣، بالرغم من عدم اتجاه سياسته الجنائية نحو صياغة قانون خاص بتجريم الجريمة الالكترونية.

وعليه فأن توقف امتداد التفتيش إلى أنظمة حواسيب آلية موجود في دولة أخرى على وجود اتفاق خاص او أذن من الدولة المقابلة، يعد مشكلة تواجه السلطات التحقيقية في اجراء التفتيش بحثا عن أدلة الجريمة الالكترونية، في حال لم تكن الدولة منظمة الى مثل هذه الاتفاقيات او امتناع الدولة الأخرى عن اعطاء الأذن بالتفتيش، الامر الذي يتطلب وجود تعاوناً دولياً فعالاً لغرض تحقيق ذلك الامتداد.

فضلا عن تلك الصورتين فان هناك صورة أخرى تتمثل **بالمراقبة والتنصت الالكتروني** كإحدى وسائل التفتيش عن الدليل في الجريمة الالكترونية، وما يميز هذه الصورة انتشارها في الوقت الحاضر كمراقبة المكالمات والرسائل الهاتفية ومراقبة الحساب الخاص لمواقع التواصل الاجتماعي...الخ، إذ أصبحت أداةً لا يمكن الاستغناء عنها في إجراء التحري والتفتيش عن مثل هذا النوع من الإجرام، إلا إن هذه الصورة تثير مشكلةً بالغةَ الأهميةِ؛ لكونها تمثل انتهاكا لحقَ الخصوصية سواء تعلق ذلك بالمتهم أم بغيره مما تقتضي هذه المراقبة وجودَ سندٍ قانوني[٥٥]. وتظهر هذه المشكلة بصورة جلية في الدول المعتمدة على سياسةِ تطبيق النصوص التقليدية كالعراق، ومع ذلك لم نجد كلاً من المشرع الأماراتي والقطري والمصري قد تبنى النصَ عليها ضمن نصوص القانون الخاص بتجريم الجريمة الألكترونية، مما يشكل ذلك نقصاً تشريعياً، إذ لا يكون أمام السلطات التحقيقية سوى الرجوع إلى النصوص الإجرائية التقليدية مما قد يؤدي ذلك إلى التوسع في تفسيرها[٥٦].

واستنادا لما تقدم فان امتداد التفتيش إلى نظام حاسب آلي مملوك لغير الجاني، يشكل بطبيعة الحال انتهاكاً لخصوصية ذلك الغير في حال إجراء التفتيش من دون إذنه أو حضوره، كما لو أُجري التفتيش في أنظمة الحواسيب الآلية المملوكة لصحاب المقهى أو الدخول في نظام حاسب آلي لشخص إجراء اتصالات مؤخراً مع المتهم دون إذنه أو علمه، مما يسفر عن ذلك اختلاف إجراء التفتيش في الجريمة الألكترونية عنه في الجرائم التقليدية؛ ذلك لأن الأخيرة يجري فيها التفتيش بحضور صاحب المنزل سواء أكان متهماً أو غير متهم، مما يقتضي الأمر حتى يتم إجراء التفتيش بصورة صحيحة في الجريمة الالكترونية، أن يكون ذلك التفتيش بحضور صاحب الحاسب الألي، وهذا الأمر قد يتعذر حصوله في أغلب الأحوال بسبب طبيعة المحل الافتراضي للجريمة الالكترونية، مما يقتضي ذلك وجود نص إجرائي خاص دون الاعتماد على النصوص التقليدية[٥٧].

ثانيا: المشكلات المتعلقة بإثبات الدليل المرئي وحفظه

إن الهدف الأساسي الذي يسعى إليه إجراء التحري والتفتيش ومعاينة مسرح الجريمة هو الحصول على الدليل اللازم للجريمة المرتكبة، ومن ثم فإن الدليل وإن كان يمثل غاية الأدوات الأخرى لضبط الجريمة، فإن إثباته وحفظه يبقى ضمن إحدى أدوات ضبط الجريمة.

تنحصر أعمال السلطات التحقيقية في الدرجة الأساس بتحقيق هدفها المتمثل بالحصول على الدليل الجنائي، والذي يولد بمولد الجريمة وقد يكون معاصراً او لاحقاً على ارتكابها، فالدليل عادة ما يوجد بوجود الجريمة والذي يتواجد في مسرح ارتكابها أو في أي مكان لا يمت بصلة لمسرح الجريمة، كما وأن الدليل غالبا ما يتمثل بصورة مادية يدرك بالحواس، ففي المقابل يتمثل أيضا بصورة معنوية كأثر نفسي منطبع لدى شخص المتهم أو الشاهد، وعليه يراد بالدليل **اصطلاحا** "هو ما يلزم من العلم به علم شيء آخر وغايته أن يتوصلَ العقل إلى التصديق اليقيني بما كان يشك في صحته"[٥٨]. أما مفهوم الدليل الجنائي فقد اختلف الفقه الجنائي في إيراد تعريف له فقد ذهب البعض إلى تعريفه **بأنه** "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها".[٥٩]

ويتضح من استقراء التعاريف السابقة أن الدليل الجنائي يعد من الأمور الجوهرية في مجال التحقيق والمحاكمة، فهو السبب الرئيسِ الذي يستند إليه القرار والحكم الجنائي، وعليه بما أن لكل جريمة دليلها فأن للجريمة الألكترونية دليلها أيضا ، إلا إن الطبيعة الفنية التي أفرزتها نتج عنها في مجال الإثبات الجنائي نوع جديد من الأدلة وهو ما **يسمى بالدليل المرئي**، ولكن إذا كان للجريمة الألكترونية دليلها في ظل محلها الافتراضي، فهل يمكن اكتشاف هذا الدليل بسهولة اكتشاف الدليل المادي؟ واذا كان بالإمكان ذلك فهل يمكن أيضا حفظه أو تحريزه كأقرانه من الأدلة المادية؟.

بالنظر للخصائص التي يتمتع بها الدليل المرئي للجريمة الألكترونية من كونه يتكون من بيانات ومعطيات وبرامج...الخ، فهو وأن كان لا يدرك بالحواس المادية، فأن ذلك لا يثير مشكلة بقدر تعلق الأمر حيث يمكن معاينته أو اكتشافه عن طريق الأنظمة المعلوماتية للحواسيب الآلية وأن كان هذا الأمر يتطلب توافر الخبرة لدى القائم بالتحقيق، ومن ثم فإن باستطاعة السلطات التحقيقية حفظَ الدليل المرئي عن طريق استخراجه من نظام الحاسب الآلي كطباعته على ورق أو طباعته بأقراص الليزر...الخ[٦٠]. لكن هذا الأمر ليس سهلاً وإنما يثير **من جانبنا** مشكلات عدة يمكن بيانها في صورتين تتعلق بمستوى امتداد نطاق الدليل المرئي، نبينها بالآتي:

الصورة الأولى: أن ينحصرَ وجود الدليل المرئي في مسرح الجريمة من دون امتداده لأنظمة حواسيب أخرى، ففي هذه الحالة يكون أمام السلطات التحقيقية خيارين **أولهما** يتمثل بأجراء التحرز على الحاسب الآلي ذاته، فيتم التحرز أو الحفظ للحاسب الآلي وفقاً للقواعد التقليدية التي تشترط حفظَ الدليل لدى السلطات التحقيقية وختمه، فعلى ضوء ذلك يتم حفظ الحاسب الآلي بأكمله وختمه بختم السلطة التحقيقية [٦١].

أما الخيار الآخر أمام السلطات التحقيقية فإنه يتمثلُ بإخراج الدليل المرئي بإحدى مخرجات الحاسب الآلي ليتم إجراء التحرز أو الحفظ على الشيء الذي يحتوي الدليل المرئي كالأوراق والأقراص الليزرية...الخ، وختمها أيضا بختم السلطات التحقيقية، إلاّ إنّ ذلك لا يؤدي إلى حفظ الدليل المرئي بشكل كامل لدى السلطات التحقيقية، إذ يبقى بالإمكان الرجوع إليه لدى الحاسب الآلي للمتهم حتى ولو تم حذفه فان بالإمكان إعادته بوساطة تقنية المعلومات[٦٢] . فضلا عن ذلك فإن التحرز أو الحفظ لا يقع على الدليل المرئي ذاته، وإنما في هذه الحالة سوف يقع على الشيء الذي يتضمن أو يحتوي ذلك الدليل، ومن ثم **نرى من جانبنا** ليس بالإمكان إجراء حفظه وفقا للقواعد الإجرائية التقليدية التي تشترط حفظ الدليل بعينه ووضع الختم عليه كما هو الشأن في الدليل المادي كحفظ السلاح الذي ارتكب فيه القتل أو الأوراق التي وقع عليها التزوير...الخ.

الصورة الثانية: تتمثل بامتداد نطاق الدليل المرئي إلى أنظمة حواسيب أخرى غير مسرح الجريم سواء أكانت موجودة ضمن نطاق حدود الدولة الواحدة أم في دول أخرى؟، فلا يختلف الأمر هنا عن امتداد إذن التفتيش كما أوضحنا ذلك سابقاً، **لكن المشكلة** التي نراها **من جانبنا** هو عن كيفية قيام السلطات التحقيقية بحصر وحفظ الدليل المرئي الموجود في أنظمة حواسيب آلية متعددة، فلا يختلف الأمر عن الصورة الأولى إذ ليس بالإمكان الاستناد إلى القواعد الإجرائية التقليدية؛ ذلك لأن محل الحفظ أو التحرز في هذه الحالة لا ينحصر بيد السلطات التحقيقية، فلا جدوى من إخراج الدليل المرئي وحفظه أو التحرز على الحاسب الآلي ذاته إذا ما كان ممتداً إلى أنظمة حواسيب

أخرى ليس بالإمكان محوه أو حذفه، فضلا عن ذلك فإن امتدادَ الحفظ أو التحرز سيؤدي إلى اختراق قواعد الاختصاص المكاني(٦٣).

وعليه فإن هذه المشكلات تظهر بصورة جلية أيضا كما رأينا في الدول التي اتبعت سياسة تطبيق النصوص التقليدية كالعراق، ولم يختلف الأمر بالنسبة للمشرع الإماراتي بالرغم من اتجاه سياسته الجنائية نحو صياغة قانون خاص، إلا إنه كما في أدوات الضبط الأخرى لم يتضمن قانونه الخاص بالجريمة الالكترونية ما يشير إلى حفظ الدليل المرئي، وبخلاف ذلك كما رأينا سابقا فقد تضمنت القوانين الخاصة بالجريمة الالكترونية للمشرع القطري والمصري نصوصاً أشارت إلى الدليل المرئي المتحصل عن طريقة تقنية وأنظمة المعلومات وشبكات ومواقع الأنترنت، كما بينت إمكانية حفظ الدليل المرئي للجريمة الالكترونية، إذ أشارت إلى حفظ الأجهزة والأدوات ووسائل تقنية المعلومات وأنظمة الحاسب الآلي وما يتعلق بها من بيانات ومعلومات، بالرغم من ذلك فأنها لم تبينْ طرائقَ إجراء حفظ الدليل المرئي وكيفية معالجة امتداده إلى أنظمة ومواقع متعددة(٦٤). ففي المقابل سارت الاتفاقيات الدولية على هذا النهج بعدم بيان كيفية حفظ الدليل المرئي والوسائل اللازمة لذلك، وإنما اكتفت بتنظيمه بين الدول الأطراف، فنجد كلاً من اتفاقية بودا بست لسنة ٢٠٠١ والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠، قد نظمت بدروها إجراءات حفظ الدليل المرئي المتمثل بالبيانات والمعلومات المتحصلة عن الجريمة الالكترونية بين الدول الأطراف، مع ذلك فإن المشكلة تبقى رغم ذلك بالنسبة للدول التي لم تنظم إلى مثل هذه الاتفاقيات، وأيضا تلك التي انضمت إلى مثل هذه الاتفاقيات من دون اتجاه سياستها الجنائية نحو صياغة تشريع خاص.

فضلا عمَّ تقدم فأن مسألة إثبات الدليل المرئي أيضا تثير مشكلة، فإذا كان بإمكان السلطات التحقيقية كشف الدليل المرئي عن طريقة أنظمة الحواسيب الآلية، فأنه ليس سهلاً في بعض الأحيان إثباته وخصوصاً أنه يتمثل بالبيانات والمعطيات...الخ، وقد تكمن هذه الصعوبة بسبب اتساع نطاق شبكة الانترنت التي تمثل ظاهرةً دوليةً تنعدم مركزيتها وتتساوى أمامها الدول مما يخلق صعوبة أمام الجهات التي تتعقب الدليل المرئي، إذ بالإمكان ارتكاب الجريمة عبر القارات مما يؤدي ذلك إلى صعوبة تعقب الدليل المرئي خصوصا ما إذا ارتكبت الجريمة عبر أنظمة حواسيب متعددة في أماكن مختلفة، فضلاً عن ما تتضمنه شبكة الانترنت من الكم الهائل من البيانات والمعلومات وما يقابله من سهولة إخفاء الدليل المرئي، الأمر الذي يتطلب توافر المعرفة والأجهزة الخاصة التي تساعد رجالَ التحقيق في كيفية إثبات الدليل المرئي(٦٥).

خلاصة ما تقدم ذكره أن الضبطَ يعدُّ من الأمور المهمة في مرحلة التحقيق والذي يقوم على إدوات عدة تتمثل بكل من التحري ومعاينة مسرح الجريمة والتفتيش والتي تهدف جميعها إلى تحقيق غاية واحدة وهي الحصول على الدليل الجنائي ومن ثم فإن الضبط يسري على الجريمة الألكترونية كغيرها من الجرائم التقليدية، لكن لا يمكن أن يستندَ ضبط الجريمة الألكترونية إلى النصوص الإجرائية التقليدية المعتمدة في الجرائم المادية، كما رأينا سابقاً لصعوبة قدرة تلك النصوص الإجرائية على استيعاب ضبط هذا النوع من الإجرام، بمعنى آخر لا يمكن للسياسة الجنائية أن تتجه نحو تطبيق النصوص الإجرائية التقليدية لضبط الجريمة الالكترونية؛ لكونها مستندة إلى تطبيق النصوص الموضوعية في نطاق التجريم والعقاب؛ وذلك لأسباب عدة يمكن بيانها بالآتي فضلا عن الأسباب التي سبق بيانها في الفصل السابق:

١- إن الضبط بأدواته في الجريمة الألكترونية يتم في بيئة افتراضية لا حدود لها ولا مكان فيها للأدلة المادية، مما يجعل مسألة تطبيق النصوص الإجرائية التقليدية لا تتفق مع البيئة الافتراضية؛ لأنها وضعت في الأصل من أجل مواجهة الاعتداءات المادية، ولا شك أن الجريمة الالكترونية تخرج عن هذا الإطار؛ لأنها ترتكب في البيئة الافتراضية، مما ينعكس ذلك بدوره على حالة التلبس في الجريمة الالكترونية، فمن الصعب تصور إمكانية ضبط جريمة الكترونية مشهودة على وفق النصوص الإجرائية التقليدية، وكذلك الحال بالنسبة للجرائم التقليدية التي ترتكب عن طريق نظام الحاسب الآلي فمن الصعب مثلا ضبط جريمة الرشوة التي ترتكب عن طريق عرض وقبول الكتروني إذا ما تم تحويل المبلغ المطلوب إلى بطاقة ائتمان تابعة للمرتشي؛ ذلك أن جريمة الرشوة تتطلب حصولَ واقعة مادية على وفق النصوص الإجرائية التقليدية، وكذلك الحال بالنسبة لجريمة الاختلاس وغيرها من الجرائم الأخرى.

٢- تعدّ القوانين الإجرائية بمثابة الوثيقة الأساسية لحماية حقوق الأفراد، فهي تهدف إلى إيجاد نوع من التوازن بين مصلحة الدولة ومصلحة وحقوق الأفراد، ومن ثم فإن مسألة تطبيق النصوص التقليدية تصطدم مع حقوق الأفراد، إذ يجب أن يكون ضبط الجريمة الألكترونية على وفق مبدأ شرعية الإجراءات، بمعنى أن تكون إجراءات الضبط موافقةً للقانون ومن ثم فأن التوسعَ في تفسيرِ النصوص الاجرائية يهدد حقوق وحريات الأفراد؛ ذلك لأنّ النصوص الإجرائية التقليدية تمثل قيداً على حرية الفرد، مما يجعل قياس تلك النصوص على المحل الافتراضي للجريمة الالكترونية محظوراً لمخالفته لمبدأ الشرعية الإجرائية[٦٦].

الخاتمة

بعد الخوض في موضوع البحث من جوانبه كافة توصلنا إلى نتائج عدة، وهناك توصيات عدة تقابل ما توصلنا إليه من نتائج، لذا نبينها بالآتي :

النتيجة الاولى

بعد ظهور تكنولوجيا المعلومات وتطورها المتزايد ورغم الايجابيات التي أنتجها هذا التطور، إلا إنه في المقابل استغل من قبل المجرمين حتى أصبح وسيلة لارتكاب أفعالهم الإجرامية فظهر **ما يسمى** بالجريمة الالكترونية، لتصبح محلَ اهتمام على مستوى الفقه الجنائي والسياسة الجنائية الوطنية والدولية، إذ تهدف هذه الأخيرة إلى مواجهة الظواهر الإجرامية في الأزمان كلها.

التوصية

وبالاستناد إلى ما تقدم نقترح بأن تتوجه السياسة الجنائية في العراق نحو ما اتجهت إليه السياسة الجنائية في قطر والأمارات ومصر بصياغةِ تشريع خاص للجريمة الألكترونية من خلال تفعيل مسودة قانون مكافحة الجريمة الألكترونية لسنة ٢٠١٩، مع إجراء التعديلات اللازمة لمواجهة مشكلات ضبط الجريمة الألكترونية.

النتيجة الثانية

يعد الضبط الركيزة الأساسية في التحقيق الجنائي، والذي يراد به كل إجراء يتخذ من أجل الحصول على أدلة الجريمة، وبهذا المعنى فأنه يرد على الجرائم كله ذات المحل المادي، وبما أن الجريمة الألكترونية لا تختلف عن نظيراتها من الجرائم الأخرى من حيث توافر أركانها، فإن إمكانية تحقق الضبط فيها أمراً وارداً لا يختلف عن الجرائم الأخرى، إلا إن الضبط فيها له خصوصيته إذ يرد على محل افتراضي للجريمة الألكترونية كالبيانات والبرامج...الخ، ولهذا فأنه ثمة مشكلات عدة يخلقها الضبط في هذه النوع من الإجرام، سواء على مستوى إجراء التحري كمشكلة البلاغ عنها أو نقص الخبرة لدى أفراد السلطات التحقيقية أو الحاجة لآلية معينة للتحري عنها، أو سواء على صعيد معاينة مسرح الجريمة والتفتيش إذ يشترط في الجرائم التقليدية حصول المعاينة أو التفتيش المادي وأن يكون بحضور المتهم أو صاحب المكان المعني وهذا مالا يمكن تصوره في المحل الافتراضي، فضلا عن إمكانية تحقق امتداد المعاينة والتفتيش إلى أنظمة حواسيب آلية موجودة في أماكن أو دول أخرى، وأيضا على صعيد إثبات الدليل وتحرزه فثمة صعوبة في إثبات وتحرز الدليل

الافتراضي، ومن ثم فإن هذه المشكلات تظهر بصورة جلية عند الاعتماد على النصوص الإجرائية التقليدية، إذ أن هذه النصوص صيغة لمعالجة ضبط الجرائم المادية وليست المحل الافتراضي ذاته، مما يجعلها غير كافية لضبط الجريمة الألكترونية، فضلا عن ذلك فان تطبيق هذه النصوص على هذه الجريمة يؤدي الى الخروج عن مبدأ الشرعية الاجرائية، ومن ثم فأن توجه السياسة الجنائية نحو وضع قانون خاص بالجريمة الألكترونية كما فعلَ المشرع القطري والأماراتي والمصري، دون أن يتضمنَ هذا القانون النصوص الإجرائية التي تعالجُ الضبط، فإنَّ الأمر لا يختلف عن تلك السياسة الجنائية التي اعتمدت على تطبيق النصوص التقليدية كما فعلَ المشرعُ العراقي، إذ لا يكون أمام القضاء إلا الرجوع إلى النصوص التقليدية لسد النقص التشريعي في القانون الخاص لمعالجة ضبط الجريمة الالكترونية.

التوصية

وبالاستناد إلى ما تقدم نهيبُ بالسياسة الجنائية لكل من المشرّع القطري والاماراتي والمصري وكذلك المشرّع العراقي عند صياغته مستقبلا قانوناً خاصاً ، بضرورة اتباع أصول صياغة النص الجزائي ومعالجة المشكلات التي يخلقها ضبط الجريمة الألكترونية بشكل يجنب الرجوع إلى النصوص الإجرائية التقليدية، على أن يقتدوا في ذلك ببعض النصوص الإجرائية التي صاغتْها بعضُ الدول المتطورة كالجزائر وفرنسا والولايات الأمريكية والتي عالجتْ بعضَ هذه المشكلات كمشكلة امتداد المعاينة والتفتيش إلى حواسيب أخرى، ومعالجة الحضور الافتراضي، وإن كان كل من قانون مكافحة الجريمة الألكترونية القطري رقم ١٤ لسنة ٢٠١٤ و قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لعام ٢٠١٨، لم تخلُ من النصوص الإجرائية التي عالجت بعض تلك المشكلات كمشكلة القيمة القانونية للدليل المرئي، وهذا ما يجب على المشرع العراقي والاماراتي الاستفادة من تلك النصوص، وبمعنى خاص نهيب بالمشرِّع الجنائي العراقي عند صياغته قانوناً خاصاً بالجريمة الالكترونية أن ينظرَ إلى خصوصية هذه الجريمة من خلال إيراد النصوص الاجرائية الكفيلة لمواجهة ضبط هذا النوع من الجرائم، كوضع نص إجرائي يُجيز الرقابة الالكترونية ويسمحُ بامتداد التفتيش والمعاينة من دون الحصول على موافقة الجهة التحقيقية ضمن الاختصاص القضائي، وأيضا النص على جعل الإخبار عنها وجوبياً بالنسبة لبعض الجرائم الألكترونية من خلال فرض الرقابة على مزودي خدمة الانترنت وموظفي الدولة، فضلا عن إيراد نص إجرائي يعطي إثبات الدليل الافتراضي وتحرزه القيمة القانونية ذاته للدليل المادي ويجيزُ الحضور الافتراضي في أثناء إجراء التفتيش والمعاينة.

الهوامش

(١) عمار مزاحم مهدي، مبادئ التحقيق الجنائي في الجرائم الالكترونية والمعلوماتية عبر الانترنت وسبل معالجتها، مطبعة الكتاب، بغداد، ٢٠٢٢، ص١٠٩.

(٢) سعود علي عبدالله، السياسة الجنائية في مكافحة الجريمة الألكترونية، اطروحة دكتوراه، جامعة الشارقة، كلية القانون، ٢٠١٦، ص٣٥٧.

(٣) د. إبراهيم محمود إبراهيم، اختصاص سلطة الضبط القضائي بالتحقيق الابتدائي في النظام اللاتيني والانجلو أمريكي، ط١، دار وليد للنشر والتوزيع والبرمجيات، القاهرة، ٢٠٢١، ص٦٧.

(٤) محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار كتاب الجمهورية، مصر، ٢٠١٠، ص٧٩.

(٥) د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري ١٧٥ لسنة٢٠١٨، دار الجامعة الجديدة، الاسكندرية، ٢٠١٩،ص٤٥٤.

(٦) رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، ٢٠١٣، ص١٤٥.

(٧) تنص المادة ٤١ من قانون أصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة ١٩٧١ على انه (... ويجري التفتيش في منزله ويضبط ما يعثر علية من مواد جرمية او اشياء...)، وأيضا وبالمعنى ذاته نصت المادة ٩٨ من القانون ذاته.

(٨) د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الألكترونية، دار النهضة العربية، القاهرة، ط١، ٢٠٠٨، ص٢٠٩.

(٩) رشاد خالد عمر، مرجع سابق، ص١٤٥.

(١٠) تنص المادة المادة (٢٩) من قانون أصول المحاكمات الجزائي العراقي رقم (٢٣) لسنة ١٩٧١ على أنه (تعد الجريمة مشهودة ... الجريمة التي يضبط فيها مع شخص أشياء أو أسلحة أو أوراق يستدل منها على أنه مرتكبها...)، وإلى المعنى ذاته أشارت المادة ٤٦ من قانون الإجراءات الجنائية المصري رقم ١٥٠ لسنة ١٩٥٠على أنه (لمأمور الضبط القضائي في حال التلبس بجناية أو جنحة أن يفتش منزل المتهم ويضبط فيه الأشياء...).

(١١) نبيل محمد عثمان، الحماية الجنائية للحق في جريمة المراسلات عبر البريد الالكتروني، ط١، المصرية للنشر والتوزيع، القاهرة، ٢٠١٧، ص١٥٧.

(١٢) محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، مرجع سابق، ص٨٠.

(١٣) د. طارق ابراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠٠٩، ص٤٨٤.

(١٤) للمزيد من التفاصيل يُنظر نصوص قانون مكافحة جرائم تقنية المعلومات الأماراتي رقم ٥ لسنة ٢٠١٢.

(١٥) نصت المادة ٦ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة٢٠١٨ على أنه (لجهة التحقيق المختصة أن تصدر أمراً مسبباً ... متى كان لذلك فائدة في ظهور الحقيقة... مما يأتي ١- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة الكترونية أو تكون موجودة فيه... ٢- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات... لغرض الضبط).

(١٦) نصت المادة ١٤ من قانون مكافحة الجريمة الالكترونية القطري رقم ١٤ لسنة ٢٠١٤ على انه (... فاذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل لها صلة بالجريمة...).

(١٧) انظر المواد ٢٧و٣٧و٣٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠.

(١٨) انظر المادة ١٩ من اتفاقية بود ابست لسنة ٢٠٠١.

(١٩) محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، الاسكندرية، ٢٠١٨، ص٣١٩.

(٢٠) خالد محمد المهيري، محمد محرم علي، قانون الاجراءات الجزائية الاتحادي لدولة الامارات العربية المتحدة، معهد القانون الدولي، دبي، ٢٠٠١، ص٦٧٦.

(٢١) رشادا خالد عمر، مرجع سابق، ص١٤٨.

(٢٢) حنان ريحان مبارك، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠١٤، ص٣٦٠.

(٢٣) نفس المرجع اعلاه، ص٣٦١.

(٢٤) نبيلة هبة هروال، ط١، الجوانب الإجرائية لجرائم الانترنت، دار الفكر الجامعي، الاسكندرية، ٢٠٠٦، ص١٨٤-١٨٥.

(٢٥) انظر المادة ١ من قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١.

(٢٦) انظر كل من قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم ٥ لسنة ٢٠١٢، و قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.

(٢٧) انظر المواد ٢١و ٢٢و٥٤ من قانون مكافحة الجريمة الالكترونية القطري رقم ١٤ لسنة ٢٠١٤.

(٢٨) د. غازي حنون خلف، د. عماد فاضل ركاب، د. وصفي هاشم عبد الكريم، القصد الجرمي في تزوير التوقيع الالكتروني، بحث منشور في موقع https://www.researchgate.net/profile/Ghazi-Hanoon ، ص ٣.

(٢٩) نبيل محمد عثمان، الحماية الجنائية للحق في حريمة المراسلات عبر البريد الالكتروني، ط١، المصرية للنشر والتوزيع، القاهرة، ٢٠١٨، ص١٤١.

(٣٠) انظر كل من قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم ٥ لسنة ٢٠١٢، و قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.

(٣١) د. ايمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٥، ص١٧٠.

(٣٢) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٤٥٠.

(٣٣) محمد كمال شاهين، مرجع سابق، ص٢٥٢.

(٣٤) نفس المرجع اعلاه، ص٢٧٥.

(٣٥) السيد مهدي، مسرح الجريمة ودلالته في تحديد شخصية الجاني، دار النشر، الرياض، ١٩٩٣، ص١٩و٢٩.

(٣٦) للمزيد انظر، محمد علي سكيكر، مرجع سابق، ص٦٨.

(٣٧) رشاد خالد عمر، مرجع سابق، ص١٢٤.

(٣٨) محمد كمال شاهين، مرجع سابق، ص٢٦٢.

(٣٩) تنص المادة ٩٨ من قانون اصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة ١٩٧١على أنه (لقاضي التحقيق ان ينتقل مع كاتبه لأجراء الكشف الحسي على مكان وقوع الجريمة... يتم الكشف أو التفتيش بحضور المدعي الشخصي والمدعي علية إذا لم يحضر احدهما أو تعذر عليه الحضور فيحصل بحضور وكيله أو شاهدين...).

(٤٠) تنص المادة ٦ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ على أنه (البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات...)، وإلى المعنى ذاته أشارت المادة ١٤ من قانون مكافحة الجريمة الالكترونية القطري رقم ١٤ لسنة ٢٠١٤ .

(٤١) تنص المادة ٢٦/فقرة١ من اتفاقية بود ابست لسنة ٢٠٠١ على أنه (تعتمد كل دولة ما يلزم من تدابير تشريعية وغيرها... من أجل تمكين السلطات المختصة من التماس الكشف عنها...)، وإلى المعنى ذاته أشارتْ المادة ٣٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠ .

(٤٢) د. محمود رجب فتح الله، مسرح الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١، ص٢٥٦.

(٤٣) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، مرجع سابق، ص٢٢٣.

(٤٤) انظر المادة ٩٨ من قانون أصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة .

(٤٥) انظر المادة ١٤ من قانون مكافحة الجريمة الالكترونية القطري رقم ١٤ لسنة ٢٠١٤، والمادة ٦ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.

(٤٦) سعود علي عبدالله، مرجع سابق، ٣٢٦.

(٤٧) د. خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، ط١، دار الفكر الجامعي، الاسكندرية،٢٠١٠، ص٢٠٣.

(٤٨) تنص المادة ٧١ من قانون اصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة ١٩٧١ على انه (لا يجوز تفتيش –أي – شخص أو دخول او تفتيش منزله أو أي مكان تحت حيازته إلا بناء على أمر صادر من سلطة مختصة)، وإلى المعنى ذاته أشارت المادة ٥٣ من قانون الإجراءات الاماراتي رقم ٣٥ لسنة ١٩٩٢.

(٤٩) د. محمود رجب فتح الله، مرجع سابق، ص٣٥٦.
(٥٠) انظر المادة ١٤ من قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم ٥ لسنة ٢٠١٢، والمادة ٦ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.
(٥١) د. خالد ممدوح ابراهيم ، فن التحقيق في الجرائم الإلكترونية، مرجع سابق، ص٢٠٥.
(٥٢) د. حسين بن سعيد الغافري، مرجع سابق، ص٤٨٤.
(٥٣) انظر المادة ٣٢ من اتفاقية بود ابست لسنة ٢٠٠١، والمادة ٣٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠.
(٥٤) د. محمود رجب فتح الله، مرجع سابق، ص ٣٥٨.
(٥٥) انظر المادة ١٠٢، من قانون أصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة ١٩٧١، والمادة ٧٥ من قانون الإجراءات الاماراتي رقم ٣٥ لسنة ١٩٩٢.
(٥٦) تنص المادة ٣٣ قانون أصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة ١٩٧١ على أنه (للنائب العام أن يدخل إلى منزل المشتبه فيه للتفتيش عن المواد التي يقدرها أنها تساعد على إنارة التحقيق، وله أن يضبط ما يجده منها...ويجري التفتيش بحضور المشتبه فيه أو المدعي علية...)، والى المعنى ذاته أشارت المادة ٥١ من قانون الإجراءات الجنائية المصري رقم ١٥٠ لسنة ١٩٥٠.
(٥٧) د. خالد ممدوح ابراهيم، الجرائم المعلوماتية، ط١،دار الفكر الجامعي، الاسكندرية، ٢٠٠٩،ص١٦٠.
(٥٨) حنان ريحان مبارك، الجرائم المعلوماتية، مرجع سابق، ص٣٥٤.
(٥٩) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط١،دار الثقافة، عمان، ٢٠١١، ص ٢١٣.
(٦٠) تنص المادة ٩٨ من قانون أصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة ١٩٧١على أنه (ينظم قاضي التحقيق محضراً مفصلا بإجراءات الكشف...وعليه أن يحفظ المواد والاشياء المضبوطة بحسب طبيعتها وأن يختمها بختم دائرة التحقيق وأن يلصق عليها ورقة يذكر فيها المحتويات المضبوطة...).
(٦١) د. خالد ممدوح ابراهيم ، الجرائم المعلوماتية، مرجع سابق،ص١٨٢و٢٠٢.
(٦٢) د. محمود رجب فتح الله، مسرح الجريمة الالكترونية، مرجع سابق، ص٥٣١.
(٦٣) انظر المواد ١٥و١٨ من قانون مكافحة الجريمة الالكترونية القطري رقم ١٤ لسنة ٢٠١٤، والمادة ٦من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.
(٦٤) د. أمير فرج يوسف، حقوق الملكية الفكرية الألكترونية والمساس بها باعتبارها جريمة معلوماتية، ط١، مكتبة الوفاء القانونية، الإسكندرية، ٢٠١٦، ص ٤٠٢-٤٠٣.
(٦٥) د. أمير فرج يوسف، حقوق الملكية الفكرية الألكترونية والمساس بها باعتبارها جريمة معلوماتية، ط١، مكتبة الوفاء القانونية، الإسكندرية، ٢٠١٦، ص ٤٠٢-٤٠٣.
(٦٦) د. محمود رجب فتح الله، مسرح الجريمة الالكترونية، مرجع سابق، ص١٨٦.

قائمة المصادر

(الكتب القانونية)

١. إبراهيم محمود إبراهيم، اختصاص سلطة الضبط القضائي بالتحقيق الابتدائي في النظام اللاتيني والانجلو أمريكي، دار وليد للنشر والتوزيع والبرمجيات، القاهرة، ط١، ٢٠٢١.

٢. أمير فرج يوسف، حقوق الملكية الفكرية الألكترونية والمساس بها باعتبارها جريمة معلوماتية، مكتبة الوفاء القانونية، الاسكندرية، ط١، ٢٠١٦.

٣. أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٥.

٤. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٩.

٥. حنان ريحان مبارك، الجرائم المعلوماتية، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٤.

٦. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط١، دار الثقافة، عمان، ٢٠١١.

٧. خالد محمد المهيري، محمد محرم علي، قانون الإجراءات الجزائية الاتحادي لدولة الامارات العربية المتحدة، معهد القانون الدولي، دبي، ٢٠٠١.

٨. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، ط١، ٢٠٠٩.

٩. خالد ممدوح ابراهيم، فن التحقيق في الجرائم الإلكترونية، دار الفكر الجامعي، ط١،الاسكندرية، ٢٠١٠.

١٠. رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، ٢٠١٣.

١١. السيد مهدي، مسرح الجريمة ودلالته في تحديد شخصية الجاني، دار النشر، الرياض، ١٩٩٣.

١٢. طارق إبراهيم الدسوقي، الامن المعلوماتي، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠٠٩.

١٣. عمار مزاحم مهدي، مبادئ التحقيق الجنائي في الجرائم الألكترونية والمعلوماتية عبر الانترنت وسبل معالجتها، مطبعة الكتاب، بغداد، ٢٠٢٢.

١٤. محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار كتاب الجمهورية، مصر، ٢٠١٠.

١٥. محمد كمال شاهين، الجوانب الإجرائية للجريمة الألكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، الاسكندرية، ٢٠١٨.

١٦. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري ١٧٥ لسنة٢٠١٨، دار الجامعة الجديدة، الاسكندرية، ٢٠١٩.

١٧. محمود رجب فتح الله، مسرح الجريمة الالكترونية، دار الجامعة الجديدة، الاسكندرية، ٢٠٢١.

١٨. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٨.

١٩. نبيل محمد عثمان، الحماية الجنائية للحق في جريمة المراسلات عبر البريد الألكتروني، ط١، المصرية للنشر والتوزيع، القاهرة، ٢٠١٧.

٢٠. نبيل محمد عثمان، الحماية الجنائية للحق في جريمة المراسلات عبر البريد الالكتروني، ط١، المصرية للنشر والتوزيع، القاهرة، ٢٠١٨.

٢٠. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.

أطاريح الدكتوراه

١. سعود علي عبدالله، السياسة الجنائية في مكافحة الجريمة الالكترونية، أطروحة، جامعة الشارقة/كلية القانون، ٢٠١٦.

الأبحاث العلمية

١. د. غازي حنون خلف، د. عماد فاضل ركاب، د. وصفي هاشم عبد الكريم، القصد الجرمي في تزوير التوقيع الالكتروني، بحث منشور.

القوانين والاتفاقيات الدولية

١. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠.
٢. اتفاقية بودابست لسنة ٢٠٠١.
٣. قانون أصول المحاكمات الجزائي العراقي رقم ٢٣ لسنة ١٩٧١.
٤. قانون الإجراءات الجنائية المصري رقم ١٥٠ لسنة ١٩٥٠.
٥. قانون الإجرائي الاماراتي رقم ٣٥ لسنة ١٩٩٢.
٦. قانون مكافحة الجريمة الإلكترونية القطري رقم ١٤ لسنة ٢٠١٤.
٧. قانون مكافحة جرائم تقنية المعلومات الأماراتي رقم ٥ لسنة ٢٠١٢.
٨. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لعام ٢٠١٨.

المواقع الالكترونية

https://www.researchgate.net/profile/Ghazi-Hanoon AM : 10:25 /2022/9/10.