إجراءات التحقيق في الجريمة الإلكترونية

م.م. صلاح محمود خضير(*)

الملخص

أن الايجابيات العديدة التي احدثها التطور التكنلوجي في تسهيل نقل وتبادل المعلومات والبيانات، رافقها بعض الاغراض الجانبية المتمثلة في استغلال هذا التطور من قبل بعض الشبكات والهيئات والعصابات والافراد لارتكاب افعال تتقاطع مع القوانين والاعراف والاخلاق والآداب السائدة في المجتمع، ومن هنا كان من الضروري ان تواكب التشريعات المختلفة هذا التطور الملحوظ في الجرائم الإلكترونية، فالتقدم العلمي والتكنلوجي لا يمكن ان يسير، او يعمل وحده بمعزل عن أي تقدم قانوني يحافظ عليه ويكفل حمايته ويضع الحلول لما قد يطرأ من معوقات بسبب استعماله، ففي هذه الحالة يمكن للتقدم التكنلوجي ان يصبح اداة للبناء واساسًا لكل تطور، على انه في ذات الوقت اذا اسيئ استخدامه، يمكن ان يصبح اداة للجريمة ووسيلة لارتكابها، ومما لا شك فيه ان هذه الجرائم تعد من اخطر واعقد الجرائم على الاطلاق، وذلك تأسيسًا على طبيعتها المتميزة والمعقدة من حيث ذاتية اركانها، وحداثة اساليب ارتكابها، والبيئة التي ترد عليها، وخصوصية مرتكبيها ووسائل كشفها والتحقيق فيها.

الكلمات المفتاحية: الجرائم الالكترونية_ الاختراق_ التحقيق_ الشهادة الالكترونية

المقدمة

اصبحت هذه الجرائم صعبة التكييف على اساس النصوص الجزائية التقليدية، الامر الذي يقتضي ضرورة التصدي لهذه الجرائم بنصوص جزائية جديدة تتوافق مع هذه الانشطة الاجرامية المستحدثة، ولم تقف الصعوبة عند هذا الحد، بل امتدت الى نطاق القانون الجزائي الاجرائي التي صيغت نصوصه لتنظم الاجراءات المتعلقة بجرائم تقليدية لا تثير صعوبة في اثباتها والتحقيق فيها وجمع الادلة المتعلقة بها، فالجهات المختصة بالتحقيق في الجريمة التقليدية تتعامل مع واقع مادي ملموس، مما يمكنها من اجراء عمليات البحث والتحري بسهولة، في حين ان الجرائم الإلكترونية ترتكب في بيئة افتراضية الكترونية تختلف تمامًا عن البيئة التي ترتكب فيها جرائم الإلكترونية، كما ان المجرم المعلوماتي لا يترك خلفه اية اثار، بسبب دقة وسرعة اقتراف الجريمة، وسهولة اخفاء الادلة عقب وقوعها مباشرة، وهو ما يجعل سلطات التحقيق عاجزة عن مواجهة هذه الجريمة.

اهمية البحث

تكمن اهمية البحث في حداثته، إذ أنه مرتبط بجرائم معاصرة في مجال البحث

(*) كلية الامال / قسم القانون Salahhdndjj253@gmail.com

الاكاديمي والدراسات القانونية، وما زالت النصوص القانونية بشقيها الموضوعي والاجرائي تثير العديد من التساؤلات التي تتطلب المناقشة والبحث العلمي، كما يستمد الموضوع اهميته من كونه مرتبطاً بأهم اجراء يتخذ في الدعوى الجزائية، وهو اجراء التحقيق في جرائم الإلكترونية، الذي يستلزم البحث في خصوصياته المتعلقة بجرائم الكترونية.

اشكالية البحث

: تتمثل اشكالية البحث اساسًا في الفراغ التشريعي الموجود في التشريع العراقي بخصوص الجرائم الإلكترونية، وما نتج عنه من معوقات عديدة واجهت اجراءات التحقيق في هذا النوع من الجرائم، والمتمثلة في خفاء الجريمة الإلكترونية وسهولة وسرعة محو او تدمير ادلتها، والضخامة البالغة لكمية البيانات المراد فحصها، وكذلك صعوبات متصلة في اجراءات جمع الادلة كالمعاينة والتفتيش والضبط وغيرها من الاجراءات الأخرى، ومن الاشكاليات الاخرى، تضاؤل الخبرة لدى اجهزة التحقيق التي يفتقر اعضاؤها الى التأهيل الكافي في الميدان التقني، مما يزيد من صعوبة وصولهم الى الدليل المعلوماتي، وعدم معرفتهم بطريقة ضبطه والمحافظة عليه.

منهجية البحث

نظرًا لطبيعة موضوع البحث سيتم الاعتماد على المنهج الوصفي التحليلي بطريقة متكاملة ومتناسقة، لتأصيل عناصر الموضوع وتوصيف مشكلته، مع تحليل النصوص القانونية واستعراض الآراء الفقهية ذات الصلة بموضوع البحث، وتحليلها لترجيح احدها مع بيان اسباب ومبررات ذلك.

هيكلية البحث

لأجل الاحاطة الكافية بموضوع البحث، سنتناوله في مبحثين، وكما يأتي:

المبحث الاول: سنخصصه لدراسة مبادئ التحقيق الجنائي في الجرائم الإلكترونية.

المبحث الثاني: سنخصصه لدراسة إجراءات التحقيق الجنائي في الجرائم الإلكترونية.

المبحث الاول

مبادئ التحقيق الجنائي في الجرائم الإلكترونية

إن التحقيق الجنائي وكما هو معروف يتولاه قاضي التحقيق أو المحقق بالشكل المحدد قانوناً بهدف تدقيق الأدلة وتمحيصها والكشف عن الحقيقة، والتأكد فيما إذا كانت الأدلة المتوفرة كافية لإحالة المشتبه به الى المحكمة المختصة أو أنها غير كافية للإحالة أو أنه لا توجد جريمة لكون الواقعة غير معاقب عليها قانوناً، وهذه الإجراءات على قدر كبير من الأهمية لأن الأحكام التي تصدر من قاضي التحقيق غالباً ما يبني عليها قاضي المحكمة المختصة قراراته، وأهم القرارات أو الأحكام التي يصدرها قاضي التحقيق هي إما إحالة الدعوى إلى المحكمة المختصة أو إطلاق سراح المتهم مؤقتاً أو رفض الشكوى وغلق التحقيق.

ولأجل ذلك فإن النصوص الاجرائية الجزائية قد أحاطت إجراءات التحقيق الجنائي بمبادئ وضمانات عديدة، لكي يحقق الغاية المرجوة منه والمتمثلة بضمان فاعلية التحقيق ذاته، وحماية حقوق الدفاع المقررة للمشتبه

بـــه، بالإضافة حرمـــة الحياة الخاصـــة عمومًا، وضمـــان الحق فـــي الخصوصيـــة الإلكترونية للإفـراد فـــي الجرائـــم الإلكترونيـــة، ولغرض الاحاطـــة الكافيـــة بمبادئ التحقيـــق الجنائي في الجرائم الإلكترونية، سنقسـم هذا المبحث على مطلبين، وعلى النحو الاتي:

المطلب الاول

ضمانات التحقيق الجنائي الجرائم الالكترونية

ان الجرائـم الإلكترونيـة تأخذ شـكلاً غير الـذي عليه الحـال بالنسـبة للجرائـم التقليدية، ويرجع ذلك الى طبيعة شبكة المعلومات الدولة (الانترنـت)، كمـا أن الوصـول إلـى المجرم المعلوماتي يشـكل عبئاً فنياً وتقنياً على القائمين بأعمـال التتبـع والتحليـل لملابسـات الوقائـع الإجراميـة، لذا يتوجب علـى المحقق عدد من المبـادئ ينبغـي تطبيقهـا عند التحقيـق، فعليه أن يسـتظهر الركـن المادي والركـن المعنوي للجريمـة محل التحقيق فضـلا عن تحديد وقت ومكان ارتكاب الجريمـة الإلكترونية، وتدوين اجراءات التحقيق وسـريتها، وهذا ما سنحاول بيانه في ثلاث فروع، وعلى النحو الاتي:

الفرع الأول

استظهار اركان الجريمة الإلكترونية وتحديد وقت ومكان ارتكابها

يتوجـب على القائم بالتحقيق عند مباشـرته لإجـراء التحقيـق الجنائي أن يسـتظهر الركن المـادي، والركـن المعنـوي للجريمـة محـل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة الإلكترونيـة، إذ يمثـل الركن المـادي للجرائم الإلكترونيـة السـلوك المـادي الـذي يتحقـق وجـوده فـي بيئـة رقميـة من خـلال الاتصال بشـبكة المعلومات الدولية، إذ ينبغي على القائم بالتحقيق معرفة بداية هذا السلوك والشروع فيه ونتيجته، فعلى سبيل المثال يقوم الجاني بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميـل الكمبيوتر ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسـه[1]، علمًا ان الاعمال التحضيرية الممهدة لارتكاب السـلوك الجرمي حتـى وان كان القانـون لا يعاقب عليها، الا انه فـي اطار الجرائـم الإلكترونية كشـراء برامج الاختـراق او الفايروسـات تمثـل جريمة بحد ذاتها.

كمـا يتوجـب ايضًا علـى القائـم بالتحقيق اسـتظهار الركن المعنوي للجرائم الإلكترونية والذي يمثل الارادة التي يصدر عنها السـلوك، فهو الحالة النفسـية للجاني والعلاقة التي تربط بين ماديات الجريمة وشـخصية الجاني، وتتخذ هذه الارادة عـدة صور منها القصـد الجنائي، والخطأ[2].

اما بخصوص مسـألة تحديـد وقت ومكان ارتكاب الجريمة الإلكترونيـة فإنها تثير العديد من المشـاكل، فعلى سـبيل المثال مكان وزمان تحقـق النتيجة الجرمية، كقيام أحد الاشـخاص في جمهوريـة العراق باختراق نظام معلوماتي لأحد البنوك العائدة لدولة البحرين، وهذا النظام موجود في جمهورية لبنان، فكيف يمكن معرفة وقـت حدوث الجريمة هل هو توقيت جمهورية العراق بعدّه (بلد الشخص المُخترق)، أم توقيت دولة البحرين (بلد البنـك المُخترَق)، ام توقيت لبنـان (البلد المتواجـد فيه النظـام المُخترَق)،

الامـر الـذي يثير مشـكلة أخرى وهـي مكان ارتـكاب الجريمـة الإلكترونيـة، ممـا يصعب معه تحديـد القانون الواجب التطبيق، لذا ينبغي ايجاد تعاون دولي لمواجهة هذه الجرائم ووضع الاطر القانونية الوطنية والدولية التي تكفل عدم المساس بخصوصية الافراد والمجتمعات[٣].

الفرع الثالث

تدوين اجراءات التحقيق

يُعـد تدوين اجراءات التحقيـق الجنائي من المبادئ الأساسية في التشـريعات الجزائية، إذ أن مبـدأ وجوبيـة تودين الاجـراءات (الكتابة) أصبح الدليل الأسـاس الـذي يثبت حصول هذه الإجراءات، وامر لازم ليكون حجة على الكافة، لذلك فإن تدوين التحقيق شرط جوهري وقاعدة مهمـة فـي كل إجراء مـن إجـراءات التحقيق الجنائـي، وهـذا يعني أن عدم وجـود محاضر التحقيـق يفتـرض عـدم مباشـرة الإجـراءات التحقيقيـة، ويقصـد بتدويـن التحقيـق تحريره وكتابتـه[٤]، امـا محاضر التحقيـق فيقصد بها مجموعة من الوسـائل والاجراءات المشروعة قانونًـا، يقـوم بها المحقق لكشـف واسـتجلاء غموض الجريمة ومن ثم الوصول الى مرتكبها واسـناد التهمة اليه، وبمعنى اخر مجموعة من الاوراق التـي تتضمـن اجـراءات التحقيق في الجريمـة، وينبغـي ان يكون المحضـر عنوانا للحقيقة والواقع[٥].

وتتجلـى أهميـة تدوين اجـراءات التحقيق الجنائي في كونه يسهم في الحفاظ على إجراءاته من التشـويه والتحريف، سـيما وأن إجراءات التحقيـق متعددة وأسـاليب مباشـرتها مختلفة، فضلاً عن أن انجاز بعضها يستلزم وقتاً طويلاً لا يمكـن معه اعتماد على ذاكـرة المحقق التي قد تخونه بمرور الزمـن، علاوة على ذلك فإن الآثـار المتخلفة عن الجريمـة قابلة للمحو بفعل الزمن، الأمـر الذي يوجب القـول إن المبادرة بتسـجيل تلك الإجراءات والآثـار وتوثيقها من شـأنه أن يبقي عليها ويحافـظ عليها من التأثير بعامل الوقـت، كما ان إثبـات التحقيق بالكتابة في المحضر التحقيقي يمكن المحكمة من تقدير قيمـة الأدلة التـي يتضمنها محضـر التحقيق، فالمحكمـة مثـلاً تسـتطيع تقديـر قيمـة الأدلة المتحصلة من المعاينة بحسـاب الزمن الفاصل بين فتح المحضر وتلقي البلاغ ومباشـرة سلطة الاسـتدلال أو التحقيق من المعاينة التي أجرتها في مسرح الجريمة[٦].

وهنـاك قواعـد عديـدة لتدوين اجـراءات التحقيـق الجنائـي والتـي يتوجب علـى القائم بالتحقيـق مراعاتها عند فتـح محضر التحقيق، اهمها ان يتضمن المحضر تاريخ وساعة ومحل الشروع فيه، وتاريخ البلاغ وساعة وصوله إلى علـم المحقق وكيفية وصوله اليه، كما يشـترط ان يتضمن سـاعة وتاريخ انتهاء التحقيق، كما يتوجب مراعاة تدوين اقوال جميع ذوي الشـأن والعلاقـة في الدعوى، بالاعتمـاد على الالفاظ السـهلة والجمل المتينة والمترابطة، ومناقشـة وسـؤال كل من المجني عليه والمتهم باستخدام ادوات الاسـتفهام الخاصة بالأسـئلة المشهورة والمتعلقـة بالجريمة وهي ما؟ (ما معلوماتك او ما تفصيـلات ما حدث)، واين؟ ومتى؟ وكيف؟ ولمـاذا؟ وهل؟، كمـا يتوجب ايضًـا ان يُحرر محضـر الكشـف (المعاينة) المرفـق بمحضر التحقيـق بجمـل واضحـة ودقيقـة بعيـدة عن الإبهـام والغموض، وتثبيت كل ما يراه المحقق ضروريًا في التحقيق[٧].

وقد حرصت اغلب التشريعات على إيراد نصوص قانونية تلزم السلطة القائمة بالتحقيق مراعاة التدوين عند مباشرتها لإجراءاته، فالمشرع العراقي مثلًا اوجب على السلطة المختصة بالتحقيق عندما تشرع في اجراءات التحقيق ان تقوم بتدوين الافادات، وهذا ما اكدت عليه المادة (٥٨) من قانون اصول المحاكمات الجزائية، والتي نصت على ان: "بتدوين إفادة المشتكي أو المخبر ثم شهادة المجني عليه وشهود الإثبات الآخرين ومن يطلب الخصوم سماع شهاداتهم، وكذلك شهادة من يتقدم من تلقاء نفسه للإدلاء بمعلوماته إذا كانت تفيد التحقيق وشهادة الاشخاص الذين يصل الى علم القاضي او المحقق ان لهم معلومات تتعلق بالحادث"، في حين نصت المادة (١٢٨) من ذات القانون على ان: "تدون في المحضر اقوال المتهم من قبل القاضي او المحقق ويوقعها المتهم والقاضي او المحقق، واذا امتنع المتهم عن التوقيع فيثبت ذلك في المحضر"، وقد اكد المشرع العراقي صراحة على اعتبار محاضر التحقيق ضمن الادلة الجزائية التي يمكن للمحكمة ان تستند اليها في اصدار حكمها وذلك في المادة (٢١٣/أ) من قانون اصول المحاكمات الجزائية[٨]، في حين بينت المادة (٢٢٠/أ) من القانون اعلاه القيمة القانونية لمحاضر التحقيق، إذ نصت على ان: "تعتبر محاضر التحقيق ومحاضر جمع الادلة ما تحويه من اجراءات الكشف والتفتيش والمحاضر الرسمية الاخرى من عناصر الاثبات التي تخضع لتقدير المحكمة والخصوم أن يناقشوها أو يثبتوا عكس ما ورد فيها"، ونظرًا لاهمية تدوين اجراءات التحقيق الجنائي سواء فيما يتعلق بسماع الشاهدة ام الاستجواب ام التفتيش ام غيرها من الاجراءات الاخرى والقواعد المتعلقة بها، فقد ورد النص صراحة على وجوب التدوين في مواد كثيرة ومتفرقة، وترجع تلك الاهمية بعدّ التدوين حجة على الكافة[٩].

الفرع الثالث

سرية اجراءات التحقيق

يثير مصطلح سرية اجراءات التحقيق الجنائي غموضًا أو التباسًا في أذهان الجمهور على وجه العموم، وقد يؤدي استعماله إلى الإيحاء لبعض القانونيين حصوصًا، تحت تأثير الخصائص النمطية للنظام الإجرائي المعروف بنظام الاستقصاء والتنقيب، بأن هذه السرية تعني مباشرة إجراءات التحقيق الجنائي في سرية تامة بالنسبة للمتهم بحيث لا يتم ابلاغه بالاتهامات المنسوبة إليه ولا اطلاعه على ما يجري من تحقيقات أو ما تتم مباشرته من إجراءات أو اتخاذه من قرارات خلال مرحلة التحقيق الجنائي، ولغرض توضيح ذلك الغموض في سرية اجراءات التحقيق انقسم الفقه على اتجاهين:

الاتجاه الاول: يرى أن مصطلح سرية اجراءات التحقيق الجنائي يحمل في طياته شقين، ينصرف الشق الأول إلى مباشرة إجراءات التحقيق الجنائي في غيبة الخصوم أنفسهم أي دون مواجهتهم بها، وأطلقوا على ذلك مصطلح (السرية الداخلية للتحقيق الابتدائي)، في حين ينصرف الشق الثاني إلى مباشرة إجراءات التحقيق الجنائي في حضور الخصوم اي علانية اجراءات التحقيق بالنسبة للخصوم (العلانية النسبية) وتكون سرية بالنسبة

للجمهور، وأطلقوا على ذلك مصطلح (السرية الخارجية للتحقيق الابتدائي)، ووفقا لهذا الرأي فإن الاصل في التحقيق الجنائي العلانية النسبية بالنسبة للفرقاء (الخصوم) التي يجب مراعاتها مراعاة تامة، بينما الاستثناء يتمثل في سريته الداخلية (السرية المطلقة) للخصوم والجمهور التي انحصرت بدرجة كبيرة نتيجة لتصاعد حقوق الدفاع ومبدأ المواجهة خلال مرحلة التحقيق الجنائي، بحيث أصبحت القاعدة أن تتم إجراءات التحقيق الجنائي في مواجهة الخصوم أي في حضورهم[١٠].

الاتجاه الثاني: فيرى أن سرية اجراءات التحقيق الجنائي تعني عدم السماح للجمهور بحضور أي من إجراءاته أو التواجد في المكان الذي يجري فيه التحقيق أيا كان هذا المكان، وعدم اطلاع الغير على هذه الإجراءات وعدم كشف أو إذاعة معلومات ملف التحقيق للجمهور عن طريق المخاطبين بالمحافظة على سريته سواء في ذلك إجراءات التحقيق ذاتها أو ما تسفر عنه هذه الإجراءات من نتائج، وأيا كانت الجهة التي تباشر إجراءات التحقيق الجنائي، بمعنى أن التحقيق الجنائي يظل كقاعدة عامة سريًا بالنسبة للجمهور[١١].

ومن جانبنا نؤيد هذا الاتجاه الذي يجعل نقطة الارتكاز في تحديد معنى سرية التحقيق الجنائي متمثلة في الجمهور وليس في خصوم الدعوى الجزائية ووكلائهم، إذ يتعين ان ينصرف مصطلح سرية التحقيق الجنائي إلى الجمهور وليس إلى الخصوم بأي حال من الأحوال، وذلك لان هذه العلانية بالنسبية للفرقاء تعد من اهم الضمانات الخاصة بإجراءات التحقيق الجنائي، كونها تمنح لقاضي التحقيق قدرًا من الحرية والاستقلال في مباشرته لعمله بعيدًا عن ضغوطات الرأي العام، وتجنب المدعى عليه من التشهير والاساءة ومن ثم الحاق الاذى المعنوي به حتى لو افرج عنه فيما بعد.

وبالرجوع الى موقف المشرع العراقي، نجد أن المادة (٥٧/أ) أصولية نصت على ان: "للمتهم وللمشتكي وللمدعي بالحق المدني والمسؤول مدنيا عن فعل المتهم ووكلائهم أن يحضروا اجراءات التحقيق وللقاضي او المحقق ان يمنع أيا منهم من الحضور اذا اقتضى الأمر ذلك لأسباب يدونها في المحضر على ان يبيح لهم الاطلاع على التحقيق بمجرد زوال هذه الضرورة ولا يجوز لهم الكلام الا اذا اذن لهم، واذا لم يأذن وجب تدوين ذلك في المحضر".

يتضح من نص المادة اعلاه ان المشرع العراقي على الرغم من انه جعل التحقيق الجنائي علني بالنسبة للخصوم، الا انه لا يمنع من ان يكون سريًا بالنسبة للكافة، الخصوم والجمهور وذلك في حالة الضرورة بغية المحافظة على الادلة ومجريات التحقيق، على ان يحق للخصوم الاطلاع على ما جرى بغيابهم عند انتهاء حالة الضرورة.

المطلب الثاني

الوسائل والمهارات الفنية للتحقيق الجنائي في الجرائم الإلكترونية

عندما تباشر السلطة المختصة التحقيق في جريمة ما، فإنه يتوجب عليها الالتزام بالقوانين والتشريعات، والقواعد الفنية التي تحقق شرعية اجراءاتها، وحيث أن الجرائم الإلكترونية

طابعهـا الخاص المميز لها، فـإن التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل ارتكاب الجريمـة ومـن ثم حـل لغزها والوصـول إلى الجانـي، بالإضافة الـى المهـارات الفنية التي ينبغي ان تتمتع بها السـلطة المختصة بالتحقيق فـي اطـار الجرائـم الإلكترونية، لذا سـنحاول في هـذا الفرع بيان الوسـائل والمهارات الفنية اللازمة للتحقيق في الجرائم الإلكترونية، وذلك في فرعين، وعلى النحو الاتي:

الفرع الأول

وسائل التحقيق في الجرائم الإلكترونية

يوجـد العديـد مـن البرامج التـي يمكن أن تلعب دورًا كبيرًا في مساعدة السلطة المختصة بالتحقيق على جمع الأدلة بشـكل أسـرع وأكثر دقـة فـي الجرائـم الإلكترونيـة، وتنقسـم هذه البرامج على نوعين، هما:

اولاً: برامـج خاصـة بأمـن الحاسـوب والشبكات: وتكون هذه البرامج موجودة ضمن اجهزة الحواسيب والشبكات التي تمثل المسرح الافتراضـي للجريمة قبـل وقوعها، تهدف إلى حماية الشـبكات من الاعتـداء، إذ تقوم بمراقبة العديد من الأنشـطة والعمليات الحاسوبية التي تجرى فيها وتحتفظ بسجلات خاصة بها، بحيث تجد فيها سـلطة التحقيـق الكثير من المعلومات التي قد تسـاعد في كشـف غمـوض الجريمة، ومن اهم هذه البرامج هي:

١. جـدار الحمايـة Firewall)): يعمل هـذا البرنامـج علـى حمايـة اجهزة الحاسـب الآلـي والشـبكات مـن خـلال تقنيـن وضبـط الاتصالات الحاسـوبية الصادرة منها والواردة إليها، وبعبـارة اخرى يقوم علـى حماية جهاز الحاسـوب أثنـاء اتصاله بشـبكة الإنترنت من المخاطر، حيث يتولّى جدار الحماية فحص كلّ المعلومـات والبيانات الـواردة من الإنترنت أو من أي شبكة أخرى[١٢].

وقـد يتم تركيـب هذا البرنامـج على نفس الحاسـوب المطلـوب حمايتـه أو مركب على صناديق الكترونية مسـتقلة يتم ربطها بالشـبكة وجعـل جميـع الاتصالات الحاسـوبية تمر من خلالهـا، إذ يتم تطبيق شـروط معينة على حزم البيانـات جميعها بحيث يتم تحديـد الحزم التي يمكن أن تنتقل مـن إحدى جهات جدار الحماية الى الجهـة الأخرى، وتقوم هـذه البرامج أثناء توليهـا لهـذه المهمة بتوثيق عمليـات الاتصال الخارجـة والداخلة وإن شـاء سـجلات توضح مصـدر ووجهة كل اتصال منهـا، وتحفظ هذه السـجلات على شـكل ملفـات حاسـوبية يمكن الرجـوع لها وقراءتها فـي أي وقت، وبرنامج جـدار الحماية متى ما تم إعداده للعمل بالشـكل الصحيح يكون قادر على تزويد سـلطة التحقيق بالكثير مـن المعلومات الهامة التـي قد تقودها إلـى الوقوف على مصدر الاتصال الحاسـوبي الـذي يقف خلف الجريمة محل التحقيق ومن ثم يساعد في تضييق دائرة الاتهام[١٣].

٢. البروكسـي ((Proxy Server: وهو نوع خـاص من البرامـج يؤمن الاتصال بواسـطة بروتوكـول الإنترنـت بيـن الشـبكة الداخليـة المحمية والعالم الخارجي، أي شـبكة المعلومـات الدولية (الانترنـت)، ويعمل على مراقبة جميـع الاتصالات الواردة إلى الشـبكة والصادرة منها والتحكم في منع بعضها بحسب الإعدادات المسـبقة التي قام بها مدير الشـبكة،

إذ يتلقى مزود البروكسي عبر الإنترنت طلبًا من المستخدم للبحث عن صفحة ما ضمن ذاكرة تسمى الذاكرة المخبأة او ذاكرة التخزين المؤقت Cache)) المحلية المتوفرة[١٤]، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فإذا كانت كذلك بالفعل أعادها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يجد مزود البروكسي الصفحة المطلوبة ضمن ذاكرة Cache)) فإنه يعمل كمزود زبون ويرسل الطلب إلى الشبكة العالمية بحيث يستخدم أحد عناوين (IP)، وأهم مزايا مزود البروكسي أن ذاكرة التخزين المؤقت (Cache) المتوفر لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة، فقد يجد المحقق الكثير من الأدلة التي ربما تم حذفها عمداً تفيد التحقيق وتساعد في الكشف عن الجريمة[١٥].

٣. نظام كشف الاختراق (Intrusion Detection System): ويرمز له اختصارًا بالأحرف IDS))، والبرامج التي تنتمي إلى هذه الفئة تتولى مراقبة بعض العمليات[١٦]، التي يجري حدوثها في الحاسوب أو الشبكة مع تحليلها بحثاً عن أية إشارات تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة، ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة، ومراقبة بعض ملفات نظم التشغيل الخاصة بتسجيل الأحداث فور وقوعها في الحاسوب أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، وفي حال اكتشف النظام وجود أحد هذه الصفات يقوم بإنذار مدير النظام بشكل فوري وبطرق عديدة ويسجل البيانات الخاصة لهذا الاعتداء في سجلات حاسوبية خاصة، ويمكن ان تقدم هذه السجلات معلومات قيمة لسلطة التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة واسلوبها ومصادرها[١٧].

٤. نظام جرة العسل Honeypot: هو نظام حاسوبي يتم تصميمه خصيصًا لصد واعتراض مختلف الهجمات عبر الشبكة، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعًا خاطئًا بسهولة الاعتداء على هذا النظام، بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي حاسوب آخر في الشبكة، في الوقت الذي يتم فيه جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، وتحليلها ومن ثم اتخاذ إجراء وقائي فعال وهذه المعلومات التي تم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها وتمد سلطة التحقيق بالعديد من البيانات التي توضح معالم الجريمة[١٨].

ثانياً: برامج خاصة مساعدة للتحقيق في الجرائم الإلكترونية: نظرًا لان مرتكبي هذه النوعية من الجرائم المستحدثة يتمتعون بقدرات ومهارات فنية عالية فإنهم غالبًا ما يحرصون على عدم ترك اي دليل ضدهم، إذ قد يقوم مرتكب الجريمة الإلكترونية بتشفير البرامج، أو تغيير كلمات المرور، أو أخفاء المعلومات أو التلاعب بها، أو اتلاف أدوات الحفظ الخارجية، أو تدمير المعلومات بأدوات الجريمة كالفيروسات وغيرها، لذا فأن القائم بالتحقيق يحتاج إلى أدوات وبرامج مساعدة

كأدوات استرجاع المعلومات من الأقراص التالفة مثل (View Disk) وبرامج كسر كلمة المرور، وبرامج الضغط وفك الضغط ((Pkzip، وبرامج البحث عن الملفات العادية والمخفية مثل (Xtreepro Gold)، وبرامج تشغيل الحاسوب مثل (Bootable Diskette) وبرامج نسخ البيانات مثل (Lap Link)[١٩]، وقد يلجأ الجاني إلى حذف الملفات من الحاسب الآلي نهائيا ومن ثم يمكن استرجاعها، ومن الأدوات المهمة لاستعادة تلك الملفات المحذوفة هناك برامج مثل برنامج Windows For Research) وبرنامج (Rescue File Regnerud)، كما ان القائم بالتحقيق يحتاج ايضًا استخدام برامج منع الكتابة على القرص الصلب بعد ارتكاب الجريمة وذلك لحماية مسرح الجريمة[٢٠].

وهناك أيضا برامج تحرير الملفات الست عشري (Hexadecimal Editors) وهي برامج تمكن المحقق من الاطلاع على محتوى كل ملف حاسوبي بشكله الثنائي، تتيح له هذه البرامج المزيد من القدرة على تحليل الملف والتعرف على طبيعة البيانات التي يحتويها، خصوصًا وأن بعض الأنظمة قد لا تستطيع تحديد إلى أية فئة من الملفات ينتمي هذا الملف، وهناك برامج البحث عن المفردات النصية والتي تستعمل في البحث عبر البيانات عن تلك الملفات التي تحتوى على مفردات معينة عادة ما تكون لها علاقة بالقضية، كذلك توجد برامج استعراض الصور والتي تستخدم في عرض الصور الرقمية على شاشة الجهاز، تساعد المحقق من مشاهدة واستعراض الصور الرقمية المخزنة داخل أجهزة الحاسوب الآلية أو وسائط التخزين الخارجية، إذ تبرز الحاجة لهذه النوعية من البرامج في الجرائم الإباحية[٢١].

الفرع الثاني

المهارات الفنية للتحقيق في الجرائم الإلكترونية

إن ظهور الجرائم الإلكترونية الناتجة عن التطور التكنولوجي أضاف أعباء جديدة على الأجهزة المختصة بالتحقيق، كون ان التصدي لهذه الجرائم يتطلب قدرات فنية لم تألفها تلك الاجهزة ولم يتعودوا عليها، الامر الذي يستلزم ضرورة توفير الإمكانات والمهارات المطلوبة في هذا المجال، تختلف عن المهارات التقليدية التي يجب أن يتمتع بها القائم، فمهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعد من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى سلطة التحقيق، الا انه في اطار الجرائم الإلكترونية فإنه يتوجب على القائم بالتحقيق معرفة العديد من المهارات الفنية ليتمكن من القيام بعمله على احسن وجه، وعليه فإن التركيز هنا سوف ينصب على تلك المهارات الفنية المستحدثة والتي تعد إفرازًا للتطور الإنساني في مجال تقنية الاتصالات والحوسبة وأمراً مستجداً في مَن يتعامل مع هذه النوعية من الجرائم، ومن أهمها:

اولاً: التعرف على المكونات المادية للحاسب الآلي والتعامل المبدئي معها: بحيث يتمكن المحقق من معرفة الشكل المميز للحواسيب وملحقاتها ومسمى كل منها، والهدف من استخدامه وما هي احتمالات توظيفه لارتكابه اي من الجرائم الإلكترونية، إذ إن عدم تعرفه عليها قد يؤدي إلى إهمالها أو حتى إتلافها بدون قصد أو تعديل البيانات الموجودة فيها نتيجة الجهل بها[٢٢].

ثانيـاً: معرفة أساسـيات عمل شـبكات الحاسب الآلي وأهم مصطلحاتها: بما ان الجرائم الإلكترونيـة ترتكـب عبـر شـبكة الاتصالات الدولية (الإنترنت)، فالمحقق فيها يكون بحاجة إلى معرفة مبـادئ الاتصال الشـبكي وأنواعه المختلفـة وكيفية انتقال البيانـات من جهاز إلى آخر على شـكل حـزم، ومبـادئ البرتوكولات الرئيسـة الخاصـة بالاتصال بالشـبكة، وتبرز أهميـة فهـم المحقق لمبادئ عمل الشـبكات في كونهـا ضرورة لتصـور كيفية ارتـكاب الفعل الإجرامـي في الفضاء السـيبراني من اختراق للشـبكات والحواسيب واعتراض حزم البيانات أثنـاء انتقالهـا عبر الشـبكة والتجسـس عليها وتحويـل مسـارها، كما أنهـا تعطـي المحقق تصـورًا جيدًا عن مدى إمكانيـة متابعة مصدر الاعتـداء على الشـبكة والمعوقـات الفنية التي تحول دون ذلك[٢٣].

ثالثـاً: تمييز أنظمة تشـغيل الحاسـوب المختلفة: يتوجب أن يكـون لدى المحقق على الأقـل فهم مبدئـي بأنـواع الأنظمة التشـغيلية لأجهزة الحاسـب الآلـي وخصائص ومميزات كل نظـام وأبجديات أنظمـة الملفات التي يعتمد عليهـا، إذ أن معرفـة المحقـق بهـذه الأنظمـة ضروريـة لكي يشـارك فـي متابعـة وفحص وتفتيش مسرح الجريمة، وأحيانا قد يجد المحقق نفسـه أمام قرار فني صعب يجب أن يتخذ قرار بشأنه بالتشـاور مع الخبير، وبدون توافر الحد الأدنـى من المعرفة التقنية لـه فإن القرار على الأرجح سوف يكون للخبير وحده[٢٤].

رابعـاً: التعرف علـى الصيـغ المختلفة للملفات وتطبيقات الحاسـوب الرئيسية التي يتعامل معها: تعد الملفات الوعاء الحقيقي لأدلة الإدانة فـي الكثير من القضايا المتعلقة بشـبكة الإنترنت بما تحويه من معلومات، وبالتالي فإن قـدرة المحقق علـى معرفة صيغ هـذه الملفات وما يمكـن أن تحويه، ومعرفته لأهم التطبيقات التـي يمكنـه مـن خلالها قـراءة أو سـماع أو مشـاهدة محتوى هذا الملف يعـد أمرًا في غاية الأهمية[٢٥].

خامساً: إجادة التعامل مع خدمات الإنترنت الرئيسية: تعد شبكة الإنترنت أداة جمع وتحريات مناسبة للمحقق، كونها خلقت مجتمعًا افتراضيًا شـبيهًا إلى حد ما بالمجتمعات الحقيقية، ويدور في هذا المجتمع الافتراضي الكثير من الحديث الذي قد يفيد المحقق في توضيح غموض بعض الجرائم ومن الممكن أيضا أن يستعمل الإنترنت كأداة تعليمية للاطلاع على مسـتجدات الجرائم الإلكترونيـة وطـرق التصـدي لها، وكوسـيلة اتصال وتبادل المعلومـات فيما بين رجال نفاذ القانون[٢٦].

سادسـاً: معرفـة الادوات والأسـاليب المستخدمة في ارتكاب الجرائم الإلكترونية: ان معرفة السلطات التحقيقية بهذه الأساليب وكيفية اسـتخدام هـذه الأدوات يعـد امـرًا ضروريًا، خصوصًـا القائميـن علـى مناقشـة الشـهود واسـتجواب المتهمين، وبدونها لن يسـتطيعوا طـرح الأسـئلة التـي تتصـل مباشـرة بالفعل الإجرامي وأسلوب ارتكابه، كما أن فهم المحقق بهذه الادوات تمكنه من فهم تقارير الخبير الفني لأجهزة الحاسـوب ومن ثم تساعده على معرفة الأساليب المستعملة في ارتكابها[٢٧].

ومـن جانبنـا نحسـب ان مكافحـة الجرائم

الإلكترونية والكشف عنها وملاحقة مرتكبيها امراً يحتاج إلى تأهيل فني وعلمي خاص ينبغي توافره في كل من تتصل أيديهم بهذه الجرائم بدءاً من مرحلة الاستقصاء وجمع الاستدلالات ومرورًا بمرحلة التحقيق الجنائي وانتهاءً بمرحلة المحاكمة، لذا فإنه يتوجب تدريب السلطات التحقيقية الذين تتصل إعمالهم ومهامهم الوظيفية بالجرائم الإلكترونية، على كيفية تشغيل الحاسبات الآلية، والتعرف على أنواعها وأنظمتها المختلفة وعلى ملحقاتها، لاكتساب مهارات ومعارف تتعلق ببرمجة الحاسبات الإلية، والمعالجة الإلكترونية للبيانات والجرائم التي تقع على اجهزة الحاسوب والانظمة الإلكترونية، وأساليب ارتكاب هذه النوعية من الاجرام المستحدث، فضلًا عن أمن الحاسبات، ووسائل اختراقها مع دراسة حالات تطبيقية لجرائم معلوماتية ارتكبت وكيف تم مواجهتها، للاستفادة من التجارب السابقة، الامر الذي يضمن مكافحة هذه الجرائم ذات الطبيعة المختلفة عن الجرائم التقليدية، فضلا عن ذلك إعادة النظر بوسائل المكافحة التقليدية وأساليبها وطرق الوقاية منها، ووضع خطط وبرامج استراتيجية لتحديث أجهزة العدالة الجنائية وتطويرها من حيث بنيتها المؤسسية وكوادرها البشرية لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم ومواجهة مرتكبيها وضبطهم وتقديمهم للعدالة.

المبحث الثاني

إجراءات التحقيق الجنائي في الجرائم الإلكترونية

يتمتع التحقيق الجنائي في الجرائم الإلكترونية عمومًا بخصائص تميزه عن التحقيق الجنائي في الجرائم التقليدية، وذلك بالنظر لطبيعة هذه الجرائم من جهة، ولصفات المجرم المعلوماتي من جهة ثانية، مما يتطلب بالمقابل توافر صفات خاصة في الجهة القائمة بالتحقيق في هذه الجرائم، كما إن التحقيق في هذه الجرائم يتطلب إجراءات خاصة تختلف عن إجراءات التحقيق في الجرائم التقليدية، تهدف الى جمع وفحص الأدلة الرقمية التي تفيد بوقوع الجريمة ونسبتها الى مرتكبها، وهذه الاجراءات تنقسم من حيث غايتها الى نوعين، **الاول** يتمثل بالإجراءات الاحتياطية ضد المتهم كأوامر القبض والاحضار، واوامر الحبس احتياطًا، وهذا النوع من اجراءات التحقيق يستهدف المحافظة على الادلة المتحصلة ضد اي سبب من شأنه أن يضعف قوتها الاثباتية او يزيلها[٢٨]، لذا يمكن تطبيقه للتحقيق في الجرائم الإلكترونية وفقًا للقواعد العامة دون أن يثير اية صعوبات، كونه لا يحتاج الى مهارة او دراية بنظم المعلومات.

اما النوع **الثاني** فيتمثل بإجراءات جمع الادلة وتمحيصها كالاستجواب والشهادة والاستعانة بالخبراء والتي يطلق عليها ايضًا (اجراءات جمع الادلة القولية والفنية)، والتفتيش والضبط والتي يطلق عليها (اجراءات جمع الادلة المادية)، وهذا النوع يعد من اهم اجراءات التحقيق في الجرائم كافة، كونه يمثل مصدر المعلومات واداة للوصول الى الادلة وتوفير شروط صحتها، فضلًا عن تدعيم قوتها في الاثبات امام محاكم الموضوع المختصة، وتجدر الاشارة الى أن تطبيق هذه الاجراءات عند التحقيق في هذه النوعية من الجرائم المستحدثة يثير صعوبات عديدة، كونه يتطلب مهارات تقنية عالية للتعامل مع الادلة الرقمية في العالم الافتراضي[٢٩]، لذا ستكون دراستنا في هذا المبحث مقتصرة على النوع الثاني دون الاول، وهذا ما سنحاول بيانه في المطلبين الآتيين:

المطلب الأول

إجراءات جمع الأدلة القولية والفنية في الجرائم الالكترونية

تتمثل اجراءات جمع الادلة القولية في الجرائم الإلكترونية بالاستجواب والشهادة، في حين يتم جمع الأدلة الفنية من خلال الاستعانة بالخبراء، وهذا ما سنتناوله في ثلاثة افرع، وكما يأتي:

الفرع الأول

استجواب المتهم في الجرائم الإلكترونية

يقصد بالاستجواب "المناقشة التفصيلية للمتهم في الدلائل والادلة القائمة على نسبة التهمة اليه"[٣٠]، فهو بذلك يعد إجراء من إجراءات التحقيق القولية، يتم من خلاله مناقشة المتهم في التهمة المنسوبة إليه ومواجهته بالأدلة القائمة ضده لتفنيدها أو التسليم بها، وهذا يعني انه ذو طبيعة مزدوجة فهو وسيلة اتهام ودفاع في الوقت ذاته[٣١]، وخص المشرع به النيابة العامة أو قاضي التحقيق، ويقوم به مأمور الضبط القضائي في الحالات الاستثنائية، وبذلك يختلف الاستجواب عن سؤال المتهم، فإذا كاَن الاستجواب احد الاجراءات المتبعة في التحقيق الجنائي، ولا يجوز مباشرته من غير القضاة والمحققين، وأَن يكون تحريريًا، فأَن سؤال المتهم يقصد به مطالبة المتهم بالرد على الاتهام الموجهة اليه وهو أحد الاجراءات المتبعة لجمع الأدلة، الذي يكون باستطاعة كافة موظفي الضبط مباشرته بصورة شفوية[٣٢].

ولأهمية وخطورة الاستجواب كأجراء اتهام ودفاع في آن واحد، فقد نظم المشرع العراقي احكامه في المواد (١٢٣-١٢٩) من قانون اصول المحاكمات الجزائية، واحاط هذا الاجراء بعدد من الضمانات تهدف جميعها إلى تأمين افضل النتائج منه، اهمها التثبت من شخصية المتهم وإحاطته علمًا بالجريمة المنسوبة إليه، وتدوين أقوال المتهم التي يدليها أثناء استجوابه مع بيان ما يقدمه من أدلة لنفي التهم الموجهة إليه، كما يكون للمتهم عند استجوابه الامتناع عن تقديم إفادته للمحقق باعتباره غير مجبر على الإجابة على أسئلة المحقق، وبالتالي فلا يجوز استعمال أي وسيلة من وسائل الإكراه ضد المتهم، كما لا يجوز تحليفه الا في مقام الشهادة على غيره من المتهمين، كذلك لا يجوز الفصل بينه وبين محاميه الحاضر معه أثناء التحقيق، كما لا يجوز استجواب المتهم خارج مقر جهة التحقيق أو بغير حضور محاميه، إلا لضرورة يقدرها المحقق كما إذا توافرت أحدى حالات التلبس واستدعت الضرورة ذلك خشية ضياع الأدلة[٣٣].

ومن الجدير بالذكر، ان المشرّع العراقي عهد بمهمة استجواب المتهم الى قاضي التحقيق او المحقق حصرًا[٣٤]، وبخصوص ضابط التحقيق في مراكز ومديريات الشرطة، وعلى الرغم من تمتعه ايضًا بصلاحية الاستجواب في الحالات التي تمنحه سلطة محقق والواردة في المادة (٥٠/ب) اصولية، غير أَن ذلك لا يكون الا على سبيل الاستثناء[٣٥]، إذ لا يجوز له مباشرة اجراءات التحقيق، وخصوصًا اجراء الاستجواب، الا بناءً على تكليف مباشر من القاضي، او عندما يعتقد بأَن احالة الشخص

المتقدم بالإخبار الى القاضي، من شأنها تأخير الاجراءات التحقيقية على نحو يتسبب في خفاء معالم الجريمة او هروب من توجه الاتهام ضده، أو تعريض الاجراءات التحقيقية للإضرار، وفي كلا الحالتين يتوجب على ضابط الشرطة اعلام القاضي او المحقق بالإجراءات المتخذة، وتسليمه الاوراق التحقيقية بعد الانتهاء منها مباشرة[٣٦]

الفرع الثاني

الشهادة في الجرائم الإلكترونية

تعد الشهادة إجراء من إجراءات التحقيق القولية وهي المعلومات التي تتعلق بالجريمة وظروف ارتكابها التي يدلي بها الشاهد أما سلطات التحقيق، ويقصد بها على وجه العموم "إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه بطريقة مباشرة أو غير مباشرة"[٣٧]، وتنقسم الشهادة في الجرائم الإلكترونية شأنها في ذلك شأن الشهادة في الجرائم التقليدية إلى الشهادة المباشرة والشهادة غير المباشرة[٣٨]، وهي بذلك –الشهادة في الجرائم الإلكترونية- لا تختلف عن الشهادة في الجرائم التقليدية من حيث ماهيتها، فالقاعدة العامة تقضي بأن يلتزم الشاهد بالبوح بما تناهى إلى علمه من معلومات ووقائع تتعلق بالجريمة المرتكبة في أي مراحل من مراحلها والإدلاء بكل ما يفيد في كشف الحقيقة[٣٩].

اما الشاهد في الجرائم الإلكترونية فيقصد به الفني صاحب الخبرة والتخصص في تقنية الحاسوب الآلي والشبكات، والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج إلى نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي ذلك ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي تميزًا له عن الشاهد التقليدي، ويشمل عدة طوائف أهمها، القائم على تشغيل الحاسوب الآلي وهو المسؤول عن تشغيل جهاز الحاسوب والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج، والمبرمجون وهم أشخاص متخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين: كاتبوا برامج التطبيقات كاتبوا برامج النظم، والمحللون وهم الاشخاص الذين يحللون الخطوات ويقومون بتجميع بيانات نظام معين ودراستها وتحليلها وذلك بتقسيم النظام إلى وحدات، كما يقومون بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن بواسطة الحاسوب الآلي، وكذلك مهندسو الصيانة والاتصالات وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكاته[٤٠].

اما عن قيمة الشهادة ودورها في اثبات الجريمة الإلكترونية، فهي تخضع لمبدأ "الاقتناع الذاتي للقاضي الجزائي"، إذ يتمتع القاضي محققاً كان أم حاكماً حرية في تقدير قيمة الشهادة ووزنها، فله أن يأخذ بها أو يطرحها، وله أن يعتمد في تكوين قناعته على شهادة واحد أو أكثر وله أن يرجحها على شهادة الآخرين، وهو غير ملزم بإبداء الأسباب حول قناعته، ولا يخضع في تقديره للشهادة لمرجع أعلى طالما كان استخلاصه للدليل سائغاً ومقبولاً عقلاً ومنطقاً[٤١].

وبالرجوع الى موقف المشرع العراقي بشأن الشهادة في الجرائم الإلكترونية، نجد ان مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١، نص على ان: "يتولى قاضي التحقيق او المحقق المباشرة في اجراءات الضبط وجمع الادلة او اي اجراء تحقيقي نص عليه قانون اصول المحاكمات الجزائية"[٤٢]، ومن ضمن هذه الاجراءات سماع الشهود، إذ اكد المشرع العراقي في قانون اصول المحاكمات الجزائية على أن: "يشرع في التحقيق بتدوين افادة المشتكي او المخبر ثم شهادة المجني عليه وشهود الاثبات الاخرين ومن يطلب الخصوم سماع شهاداتهم، وكذلك شهادة من يتقدم من تلقاء نفسه للإدلاء بمعلوماته اذا كَانَت تفيد التحقيق وشهادة الاشخاص الذين يصل الى علم القاضي او المحقق أَن لهم معلومات تتعلق بالحادث"[٤٣].

الفرع الثالث

الاستعانة بالخبرة الفنية في الجرائم الإلكترونية

تُعرف الخبرة كإجراء من اجراءات التحقيق الجنائي بانها "تقدير مادي أو ذهني يبديه اصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها بمعلوماته الخاصة سواء كانت متعلقة بشخص المتهم ام بجسم الجريمة ام المواد المستعملة في ارتكابها ام آثارها"[٤٤]، كما تُعرف بانها "الاستشارة الفنية التي يستعين بها القاضي او المحقق لمساعدته في تكوين عقيدته في المسائل التي يحتاج تقديرها الى معرفة او دراية علمية خاصة لا تتوافر لدى السلطة التحقيقية"[٤٥].

ويقوم بإعمال الخبرة شخص يسمى الخبير، وفي اطار الجرائم الإلكترونية يسمى بالخبير المعلوماتي، وله دور مهم وكبير في كشف ادلة هذه الجرائم وتفنيدها، إذ أَن استعانة من يقوم بالتحقيق بالخبراء تكاد تكون ضرورة لا غنى عنها، نظرًا للطابع الفني والتقني الذي تتميز به هذه الجرائم، كما انها تلعب دورًا بارزًا ومهمًا في إثبات الجريمة، فالاستعانة بالخبرة الفنية سواء أكانت في مرحلة التحقيق الأولي أم الابتدائي أم أمام المحكمة تُعد من أقوى مظاهر الأدلة في هذه النوعية من الاجرام المستحدث، فقد اضحت تحتل دورًا بارزًا في إثبات الجرائم الإلكترونية، وحتى أنه اطلق عليها عبارة (الإلكترونية الشرعية)، وهي تعني عملية البحث الذي يقوم بها الخبير المعلوماتي من أجل الحصول على الدليل الرقمي بغية إعادة بناء مجريات القضية وتوضيحها للمحكمة، علمًا ان الخبراء لا يحلفون يمين الخبرة إلا إذا كانوا من خارج جدول الخبراء، إذ الخبراء المدرجون في جدول الخبراء يحلفون بعد قبولهم يمين الخبرة، اما بشأن التقرير المعد من قبل الخبير فهو من قبيل الأدلة العادية كالشهادات ولا يُلزم القاضي، كون نظام الإثبات قائماً على مبدأ القناعة الشخصية للقاضي، فله أن يقدر القيمة العلمية للخبرة[٤٦].

ومن أجل ذلك يلجأ الخبير الى بعض الوسائل التي تمكنه من تحديد الجَاني وطريقة اقترافه للجريمة، ومن أهمها الوسائل المادية والإجرائية، وتتمثل المادية بالأدوات الفنية التي يستخدمها الخبير لتنفيذ أساليب التحقيق واجراءاته التي تساعد في التعرف على حقيقة الجرم المرتكب، أما الإجرائية فهي آليات بواسطتها يمكن إعمال ثوابت التحقيق، التي تؤكد وقوع الجرم وتحدد مرتكبه[٤٧]، ويتوجب أَن تتوافر

بالخبير الامكانات والمعارف العلمية والعملية بخصوص الواقعة محل الخبرة، فالأمر لا يقتصر على مجرد امتلاك الخبير لشهادة علمية، وإنما يتطلب تحقق الممارسة العملية، كون الاخيرة تنمي الكفاءة والمقدرة الفنية، علمًا أنه لا يوجد خبير معلوماتي يمتلك الخبرة المتكاملة في البرامج الحاسوبية وشبكاتها المتنوعة[٤٨].

وفي العراق، فأن مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١ اشار بصورة مباشرة وصريحة الى امكانية القاضي في مرحلة التحقيق ومرحلة المحاكمة أن يستعين بالخبراء العراقيين والاجَانِب، وذلك بغية الاستفادة من خبرتهم في أنجاز مهام التحقيق والوصول الى الادلة، وكذلك اكدت الفقرة (٢٤/ثالثا) من مشروع القانون ذاته على تولي قاضي التحقيق والمحقق القيام بكافة الاجراءات المضمنة في قانون الاصول الجزائية، وبملاحظة نصوص هذا القانون نجده تطرق الى موضوع الاستعانة بالخبراء كأحد اجراءات التحقيق الجنائي، وذلك بموجب نص عام يتسع نطاقه ليشمل كافة صور الجرائم.

المطلب الثاني

إجراءات جمع الأدلة المادية في الجرائم الالكترونية

تتمثل اجراءات جمع الادلة المادية في الجرائم الإلكترونية بالتفتيش والضبط، وهذا ما سنتناوله في فرعين، وعلى النحو الآتي:

الفرع الأول

التفتيش في الجرائم الإلكترونية

يقصد بالتفتيش بشكل عام بأنه "عبارة عن إجراء من إجراءات التحقيق يهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة"[٤٩]، اما تفتيش النظام المعلوماتي او كما يطلق عليه (الولوج داخل النظام المعلوماتي)[٥٠]، فيقصد به "الاطلاع على محل منحة القانون حماية خاصة باعتباره مستودع سر صاحبه ويستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت"[٥١].

مما تقدم يتضح ان التفتيش كإجراء تحقيقي يهدف الى ضبط الاشياء المتعلقة بالجريمة والتي تفيد في كشف الحقيقة، والتي قد يستمد منها اهم ادلة الجريمة، الا انه وفي سبيل تحقيق ذلك الهدف في اطار الجرائم الإلكترونية من خلال الولوج داخل الانظمة الإلكترونية والبحث في البرامج المستخدمة والبيانات المخزنة في الاجهزة الحاسوبية وشبكة الانترنت، تثار عدة تساؤلات اهمها، هل يعد الولوج للنظام المعلوماتي نوعًا من التفتيش؟ وما مدى صلاحية النظام المعلوماتي او مكونات اجهزة الحاسوب الآلية المادية والمعنوية وشبكات الانترنت بأن تكون موضوعًا أو محلًا ممكنًا لتفتيشها؟ وهذا ما سنحاول الاجابة عليه في فقرتين وعلى النحو الاتي:

اولاً: مدى اعتبار الولوج في النظام المعلوماتي نوعًا من التفتيش: اختلف الفقه

الجنائي في الاجابة على هذا التساؤل، وانقسموا في سبيل ذلك على اتجاهين، الاول يسعى الى تعديل التشريعات الاجرائية القائمة واضافة نصوص اجرائية تكميلية بما يتلاءم مع متطلبات كشف الحقيقة في الجرائم الإلكترونية من بحث واستقصاء في البيئة الافتراضية، ولضمان ان يكون الحصول على هذه البيانات الإلكترونية بطرق مشروعة، لكي يمكن اعتبار الولوج في النظام المعلوماتي نوعًا من التفتيش[٥٢]، في حين يسعى الاتجاه الثاني الى التوسع في تفسير القواعد العامة للتفتيش ليمتد حكمها على الولوج في النظام المعلوماتي من دون الحاجة الى اضافة نصوص جديدة[٥٣].

وذهب رأي في الفقه الى القول بأن هذا الاتجاه الاخير قد خالف احدى القواعد الراسخة في القانون الجزائي والمتمثلة بعدم جواز القياس او التوسع في تفسير النصوص الجزائية[٥٤]، ولكن يمكن الرد على ذلك بان القياس والتفسير الواسع محضور في النصوص الجزائية الموضوعية الإيجابية، أي تلك النصوص التي تحدد الجرائم والعقوبات، أما بالنسبة للنصوص الجزائية الموضوعية السلبية، كالنصوص التي تحدد أسباب الاباحة وموانع المسؤولية والاعذار القانونية المخففة، فان القياس والتفسير الواسع جائز فيها، ففي إطار هذه الحالات لا يؤدي قياس القاضي أو تفسيره الواسع للنص إلى الاعتداء على سلطة المشرع في التجريم وفرض العقاب، لان ذلك يمثل استصحاب على الأصل العام في الأفعال وهو الإباحة، وبالتالي ليس فيه أي تجاوز أو اعتداء على مبدأ الشرعية الجزائية (لا جريمة ولا عقوبة إلا بنص).

وكذلك يجوز للقاضي القياس والتفسير الواسع للنصوص الجزائية الإجرائية، وذلك لأنها مجرد قواعد شكلية لا تقرر أحكام موضوعية تتعلق بالتجريم والعقاب، إلا إنه لابد لنا من الإشارة إلى أن القياس والتفسير الواسع إذا كان جائزاً في القواعد الإجرائية، إلا إنه لا يجوز إذا كان النص الإجرائي المراد تفسيره ينتقص من ضمانات المتهم، والعلة في ذلك أن مثل هذا النص استثنائي، والاستثناء لا يقاس عليه ولا يفسر بشكل واسع، أما إذا كان النص الاستثنائي في صالح المتهم، فانه يجوز في هذه الحالة القياس عليه والتوسع في تفسيره.

ومن جانبنا نحسب ان كلا الاتجاهين وعلى الرغم من خلاف وجهات النظر بينهم يعبران عن الاعتراف بالولوج الى النظام المعلوماتي واعتباره نوعًا من التفتيش، مع عدم التسليم بما توصل اليه أيًا منهما، اذ نرى هناك ضرورة ملحة لجمع النصوص الجزائية الموضوعية والاجرائية الخاصة بمواجهة الجرائم الإلكترونية في وثيقة قانونية واحدة، يحدد فيها المشرع الأفعال المجرمة وعقوبتها والإجراءات الواجب اتباعها بشأنها، وذلك نظرًا للطبيعة الخاصة التي تتميز بها هذه الجريمة عن غيرها من الجرائم التقليدية، فضلًا عن ضمان عدم تناثر النصوص القانونية الخاصة بمواجهة الاجرام المعلوماتي في قوانين مختلفة.

ثانياً: مدى صلاحية النظام المعلوماتي او مكونات اجهزة الحاسوب الآلية المادية والمعنوية وشبكات الحاسوب بأن تكون موضوعًا أو محلًا ممكنًا لتفتيشها: ان التفتيش او الولوج في البيئة الافتراضية قد يرد على

المكونات المادية للحاسب الآلي وملحقاته، والمتمثلة بوحدات الإدخال والإخراج والحساب والمنطق، ووحدة التحكم والذاكرة الرئيسة، فضلًا عن البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية، وذلك تبعاً للمكان أو الحيز الموجودة فيه، وهذه لا خلاف يُذكر حول خضوعها للتفتيش والضبط طبقاً للقواعد العامة المنصوص عليها في القوانين الاجرائية[٥٥]، فإذا كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن، إذ يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزاً، اما اذا وجدت في مكان عام فيحكمها ما يحكم هذا المكان من أحكام، في حين أنه إذا كان الحاسب في حوزة شخص خارج مسكنه، فإن تفتيشه عندئذٍ يخضع للقواعد ذاتها التي يخضع لها تفتيش الشخص بوصفه أحد متعلقاته، يستوي أن يكون الحائز هو مالك الجهاز أم شخص غيره، ويتوجب في ذلك التقيد بالشروط الموضوعية والشكلية للتفتيش[٥٦].

كما إنّ التفتيش قد يرد على مكونات المعنوية للحاسب، وهنا ثار خلاف فقهي حول مدى جواز تفتيش المكونات المعنوية لأجهزة للحاسب الآلي تمهيدًا لضبط الأدلة الرقمية المخزنة فيها، فقد ذهب رأي في الفقه إلى أن محل تفتيش نظم الحاسب الآلي للبحث عن أدلة تتصل بجريمة معلوماتية من الممكن أن يشمل مكونات الحاسب الآلي المادية والمعنوية على حد سواء، وشبكات الاتصال الخاصة به، والتي قد توجد في حوزة شخص أو موضوعة في مكان له حرمة المسكن[٥٧].

بينما ذهب رأي اخر في الفقه الى ان الغاية من التفتيش تتمثل بالحصول على أدلة اثبات مادية من شأنها مساعدة الجهات المعنية على كشف الحقيقة، لذا فانه لا ينطبق على الأدلة الرقمية غير المادية، ومنها المعلومات والبيانات المحفوظة داخل جهاز الحاسوب الالي، إذ أن الإشارات والنبضات الإلكترونية، لا تمثل اشياء محسوسة، مما يجعلها غير قابلة للتفتيش[٥٨].

من جانبنا نعتقد أن الرأي الأرجح هو الرأي الفقهي الأول والذي يرى أن تفتيش نظم الحاسب الآلي للبحث عن الأدلة الرقمية يتسع ليحتوي على المكونات المادية والمعنوية للحاسب الآلي على حد سواء، وذلك لأن الهدف من إجراء التفتيش بشكل عام يتمثل في الحصول على الأدلة التي تفيد في كشف الحقيقة ومن ضمنها الأدلة الإلكترونية، ومن جهة أخرى فإن هذا الاتجاه الفقهي هو الذي ايدته اتفاقية بودابست في شأن الجرائم الإلكترونية[٥٩].

اما بخصوص تفتيش شبكات الحاسوب[٦٠]، فإنه لابد من التمييز بين امرين، الاول هو اتصال حاسوب المتهم بحاسوب اخر داخل اقليم الدولة، وهذا يعني ان كافة عناصر الجريمة ترتكب في دولة واحدة، فإذا كان جهاز الحاسوب موجود في المكان المشمول به إذن التفتيش جاز تفتيشه، أما إذا كان الجهاز المشمول بإذن التفتيش متصلا بحاسوب موجود في مكان آخر فهنا يرى الفقه أن يمتد التفتيش إلى سجل البيانات الموجودة في موقع آخر شرط أن تكون البيانات ضرورية لإظهار الحقيقة مع مراعاة ضوابط وشروط التفتيش المقررة في الأماكن والمنازل الأخرى كأن تكون هذه المنازل تتمتع بالحصانة أو أماكن سكن أو أماكن شخص غير المتهم[٦١]، اما الامر الثاني فهو اتصال حاسوب

المتهم بحاسوب اخر خارج حدود الدولة، فقد تباينت الآراء حول جواز امتداد التفتيش او الولوج داخل الانظمة الإلكترونية خارج حدود الدولة، فذهب رأي –وهو ما نؤيده- الى عدم جواز امتداد التفتيش داخل النظام المعلوماتي الموجود خارج حدود الدولة إلا بموجب اتفاقية ثنائية أو دولية أو الحصول على إذن من الدولة الأخرى بذلك، للحفاظ على سيادة الدول على اقليمها وعلى حق الافراد في الخصوصية الإلكترونية[٦٢]، في حين ذهب رأي فقهي اخر الى جواز امتداد التفتيش إلى نظام معلوماتي موجود في دولة أخرى، ولا يشكل ذلك انتهاكًا لسيادة هذه الدولة، لأن الطبيعة العالمية للإنترنت تسمح بمثل هذا الإجراء، كما أن متطلبات السرعة في إجراء عملية التفتيش تقتضي عدم انتظار إذن الدولة المتواجد فيها النظام المعلوماتي المتصل بالحاسوب الوطني، مع إعلام هذه الدولة بذلك بوقت لاحق[٦٣].

وبالرجوع الى التشريع العراقي، فان المادة (٢٤/اولا) من مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١، منحت قضاة التحقيق والمحققين سلطة مباشرة لاجراء الضبط وجمع الادلة، فضلًا عن منحهم الحق للقيام بأي من الاجراءات التحقيقية الوارد ذكرها في قانون الاصول الجزائية، ومن ضمن هذه الاجراءات التفتيش، والذي نظم المشرع الاحكام الخاصة به وشروطه بالمواد (٧٢-٨٦) من قانون أصول المحاكمات الجزائية، علمًا ان المادة (٢٦) من مشروع القانون ذاته، اجازت للقاضي المختص الدخول الى اجهزة الحاسوب والى البيانات المخزنة فيها للبحث عن الادلة الرقمية، بمعنى ان هذه المادة قررت امكانية تفتيش المكونات المعنوية للحاسب الآلي في الجرائم الإلكترونية كافة.

الفرع الثاني

الضبط في الجرائم الإلكترونية

ان الغاية من التفتيش تتمثل بضبط الأشياء التي يمكن أن يستعين بها المحقق في كشف الحقيقة عن الجريمة بصفة عامة، واستهداف هذه الغاية هو عله مشروعية التفتيش[٦٤]، ويقصد بالضبط عمومًا كإجراء من إجراءات التحقيق بأنه: "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها"[٦٥]، وفي مجال الجرائم الإلكترونية يقصد به: "وضع اليد على المكونات المادية والمعنوية للأنظمة الإلكترونية، وكل شيء يفيد في كشف الحقيقة عن الجريمة الإلكترونية"[٦٦].

ويتم ضبط المعطيات الإلكترونية سواء كانت مثبته على دعامات مادية أم كانت في شكل معنوي، وبناء عليه فإن الأشياء التي ينبغي إخضاعها لأجراء الضبط في الجرائم الإلكترونية والتي تعد كيانات ذات قيمة يمكن الاستفادة منها في إثبات الجريمة أو نسبتها إلى الجاني هي[٦٧]:

اولاً: ضبط المستندات والكيانات الورقية: التي لها صلة بالجريمة أو مرتكبيها، وقد تكون محررات مزورة داخل نظام الحاسب الآلي أو في أي مكان خارجه، ويمكن أن تكون في سلة المهملات.

ثانياً: وحدة المدخلات: المكونة من لوحة المفاتيح والشاشة والفارة والخادم وكذلك برنامج معالجة النصوص وبرنامج عرض الشرائح.

ثالثاً: ضبط المراسلات الإلكترونية: التي تستعمل البريد الإلكتروني عبر شبكة الأنترنت ويتم من خلالها نقل الرسائل ومحتوى المستندات الورقية حيث تتمتع هذه الوسيلة بنظام حماية تتكون من رموز وشفرات لا يمكن الاطلاع عليها إلا إذا عرفت عليها الجهة المستقبلية، وهي تحتفظ بنسخ عن المواد المرسلة منها وإليها يمكن استرجاعها والاطلاع عليها وضبطها.

رابعاً: الشرائط المغنطة: وهي جميع الشرائط ووسائط النقل والتخزين التي يعتقد أنها تحتوي على مواد تفيد في كشف الحقيقية أو مرتكبها.

خامساً: ضبط الطابعات وأجهزة التصوير بأنواعها كافة : خصوصًا أن الأجهزة الحديثة يمكنها تخزين المستندات والمواد المطبوعة أو المنسوخة، حيث يمكن إعادة استخراجها والتعرف على محتوياتها.

سادساً: ضبط وحدة الذاكرة الرئيسية ووحدة التحكم والمودم: وهي الوسيلة التي تتمكن من خلالها أجهزة الحاسوب من الاتصال فيها بينها بواسطة خطوط الهاتف.

ويتبع في عملية ضبط الأدلة الرقمية إجراءات خاصة لحفظها وصيانتها من العبث والتلاعب، اهمها تأمين مسرح الجريمة الرقمي من التلاعب، إذ يتعين عزل الحواسيب عن الشبكة، لتجنب إجراء أي تغيير على الأدلة الرقمية من قبل الغير، كما يجب رفع البصمات عن الأجهزة لمقارنتها فيما بعد ببصمة المشتبه به، وحجز الحاسوب أو القرص الصلب، وجميع الحاويات المادية والأقراص المدمجة، فضلًا عن وضع ملصقات على المواد المضبوطة، وتوثيقها وتغليفها وتحضيرها لنقلها بالحالة التي كانت عليها إلى مكان الاختبار والفحص، وتنظيم محضر بعد إجراء عملية الضبط، يتضمن عرضًا تفصيليًا لكل الإجراءات والأعمال المتخذة، خصوصًا تلك التي تتضمن سلامة الدليل وعدم إجراء أي تغيير فيه منذ لحظة ضبطه[٦٨].

وقد نظم المشرع العراقي قواعد ضبط الادلة الإلكترونية في مشروع قانون الجرائم الإلكترونية لسنة ٢٠١١، اذ نصت المادة (٢٤/ ثالثا) منه على ان: "يتولى قاضي التحقيق أو المحقق المباشرة في إجراءات الضبط وجمع الادلة أو أي إجراء تحقيقي نص عليه قانون أصول المحاكمات الجزائية"، في حين اكدت المادة (٢٦/اولا) من ذات المشروع على الاجراءات التي يتبعها القاضي المختص عند ضبط الادلة الإلكترونية.

ومن الجدير بالذكر، انه بعد انتهاء إجراءات التحقيق الجنائي والتي هي مرحلة فحص الأدلة المتوفرة من قبل قاضي التحقيق أو المحقق، لابد من أن يتقرر مصير الدعوى الجزائية والتصرف فيها، وبالرجوع الى موقف المشرع العراقي بخصوص التصرف بالدعوى بعد انتهاء الاجراءات التحقيقية، نجد ان المشرع اكد في قانون اصول المحاكمات الجزائية على ان القرارات التي يصدرها قاضي التحقيق بعد انتهاء كافة الاجراءات التحقيقية تتمثل بقرارين، الاول: القرار بغلق التحقيق ويتمثل بصورتين فهو اما ان يكون الغلق مؤقتا اذا كانت الادلة غير كافية للإدانة، او يكون الغلق نهائيا اذا تنازل المشتكي عن شكواه او ان المتهم غير

مسؤول جزائيا او ان الفعل لا يعاقب عليه القانون، اما القرار الثاني فهو احالة المتهم الى المحكمة المختصة اذا تبين للقاضي ان الادلة المتوفرة تكفي لمحاكمته[٦٩].

فاذا كان الفعل الجرمي من نوع مخالفة فان المشرع اوجب على قاضي التحقيق اني يفصل فورًا في المخالفات التي لم يقع فيها طلب بالتعويض او برد المال دون احالته الى محكمة الجنحة، اما اذا كان الفعل الجرمي من نوع جنحة فانه يجب احالته الى محكمة الجنح بدعوى غير موجزة اذا كان الفعل معاقب عليه بالحبس مدة تزيد على ثلاث سنوات، وبدعوى موجزة او غير موجزة في الاحوال الاخرى، وفي حالة كون الفعل الجرمي يشكل جناية فانه يحال الى محكمة الجنايات بدعوى غير موجزة.

الخاتمة

بعد ان انتهينا من البحث في موضوع دراستنا الموسوم بـ (التحقيق الجنائي في الجرائم الإلكترونية)، توصلنا الى عدد من الاستنتاجات والمقترحات، والتي سنحاول اجمالها بالاتي:

اولًا: النتائج:

١. تعد الجرائم الإلكترونية من الانماط الاجرامية المستحدثة التي اوجدتها ثورة تكنولوجيا المعلومات والاتصالات، وقد باتت هذه الجرائم بأبعادها ومظاهرها الحديثة، تمثل تهديدًا للاستقرار والامن والسلام في العالم، وتشكل عائقًا يحول دون اتمام عمليات التطوير والتنمية، حيث لم تعد عواقبها قاصرة على بعض الافراد او الجماعات، بل امتدت لتهدد دولًا برمتها.

٢. إن تنامي ظاهرة الجرائم الإلكترونية عبر الوطنية، وتخطي آثارها حدود الدول، أفرز العديد من المعوقات الإجرائية التي تعيق اجراءات التحقيق في هذه الجرائم، تتجسد اولى هذه المعوقات بالصعوبات التي تكتنف كشف وإثبات الجرائم الإلكترونية، اذ انها لا تترك أثرًا ماديًا ملموسًا، كما هو الحال في الجرائم التقليدية.

٣. اتضح لنا من خلال الدراسة ان ابرز معوقات التحقيق التي تثيرها الجرائم الإلكترونية، القصور التشريعي الذي يعتري النصوص الجزائية الاجرائية القائمة في مواجهة هذا النوع من الجرائم، خصوصًا ان هذه النصوص صيغت ووضعت لتحكم الاجراءات المتصلة بالتحقيق في جرائم تقليدية لا تثير اية صعوبات في اكتشافها والتحقيق فيها.

ثانيًا: المقترحات:

١. نقترح على المشرع العراقي العمل على تعديل وترشيد القوانين الجزائية القائمة على نحو يجعلها تسري على الجرائم الإلكترونية، وذلك بهدف تفادي القصور التشريعي، وتخطي العقبات القانونية في هذا المجال، والتي قد يستفيد منها المجرم المعلوماتي للإفلات من العقاب، خصوصًا ان الاعتماد على التشريعات الجزائية القائمة، لا يكفي لتجاوز معوقات التحقيق في الجرائم الإلكترونية، وانما لابد من تدعيمها بنصوص اجرائية خاصة تتضمن اجراءات تحقيق ملائمة لطبيعة هذا الشكل الجديد من الاجرام الإلكتروني، ومسايرة للتطورات الحاصلة في تقنيات واساليب ارتكابه.

٢. نقترح على الدول العربية كافة تكثيف التعاون والتنسيق التشريعي والقضائي في مجال مكافحة الجرائم الإلكترونية، من اجل تطوير وتوحيد التشريعات الجزائية المعنية بمكافحة هذه الجرائم، فضلًا عن ضرورة التعاون في مجال تبادل المعلومات والخبرات، والتعاون في المجال الامني والقضائي بصوره المختلفة.

الهوامش

(١) د. خالد ممدوح ابراهيم: فن التحقيق الجنائي في الجرائم الالكترونية (دراسة مقارنة)، ط١، دار الفكر الجامعي، الاسكندرية، ٢٠١٨، ص٥٢.

(٢) د. عادل عبد ابراهيم العاني: شرح قانون الجزاء العماني (القسم العام)، ط١، دار الأجيال، عمان، ٢٠٠٨، ص٤٣.

(٣) د. محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٤٠.

(٤) د. عمار عباس الحسيني: التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥، ص١٠٠.

(٥) د. خالد ممدوح ابراهيم: مرجع سابق، ص٢٧.

(٦) د. سليمان عبدالمنعم: اصول الاجراءات الجنائية (دراسة مقارنة)، الكتاب الثاني، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥، ص٦٦٦.

(٧) للمزيد ينظر: د. محمد كمال شاهين: الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، دار الجامعة الجديدة، الاسكندرية، ٢٠١٨، ص٢٤٨.

(٨) نصت المادة (٢١٣/أ) من قانون اصول المحاكمات الجزائية العراقي، على ان: ((تحكم المحكمة في الدعوى بناء على اقتناعها الذي تكون لديها من الادلة المقدمة في اي دور من ادوار التحقيق او المحاكمة وهي الاقرار وشهادة الشهود ومحاضر التحقيق والمحاضر والكشوف الرسمية الاخرى وتقارير الخبراء والفنيين والقرائن والادلة الاخرى المقررة قانونا)).

(٩) ومن تلك المواد التي اوجب المشرع العراقي من خلالها تدوين التحقيق هي: (٦١، ٦٣، ٦٧، ٨٢، ٩٦، ١٠٩، ١٢١، ١٢٣، ١٢٥) من قانون اصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل.

(١٠) د. مأمون سلامة: قانون الاجراءات الجنائية معلقًا عليه بالفقه واحكام النقض، ج١، ط٣، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٤٠٠-٤٠١.

(١١) د. عبد الحميد الشواربي: ضمانات المتهم في مرحلة التحقيق الابتدائي، منشأة المعارف، الاسكندرية، ١٩٨٨، ص١٧٥.

(١٢) د. زياد محمد عبود ود. غسان حميد عبد المجيد واخرون: اساسيات الحاسوب وتطبيقاته المكتبية، ج١، الدار الجامعية للطباعة والنشر والتأليف والترجمة، وزارة التعليم العالي والبحث العلمي العراقية، بغداد، ٢٠١٤، ص٩٥.

(١٣) محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت (دراسة مسحية على ضباط الشرطة في المنطقة الشرقية)، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الامنية، الرياض، ٢٠٠٤، ص٨٣.

(١٤) تستعمل هذه الذاكرة لحفظ البيانات بشكل يسمح باسترجاعها بشكل أسرع في الطلبات اللاحقة، وقد تكون هذه البيانات نسخًا من بيانات أصلية مخزنة في مكان آخر، أو قيم تم حسابها مسبقا، فإذا كانت البيانات المطلوبة موجودة في الذاكرة المخبأة فإنه يمكّن الاستجابة للطلب بقراءة البيانات من الذاكرة المخبأة، والتي تكون القراءة منها أسرع بالمقارنة مع محاولة قراءتها من مخزنها الأصلي أو إعادة حسابها. ينظر: مقال بعنوان ذاكرة مخبئة منشور على شبكة المعلومات الدولية (الانترنت)، الموقع الالكتروني: ويكيبيديا الموسوعة الحرة، الرابط الالكتروني: https://ar.wikipedia.org، تاريخ الزيارة 10/9/2024.

(١٥) د. ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٦، ص٢١٩.

(١٦) ومـن الأمثلة على تلك البرامـج، برنامج Hack Tracer v١٢ وهـو مصمـم للعمـل فـي الأجهزة المكتبيـة Web وسـاكناً في خلفية سـطح المكتب، وعندمـا يرصـد أي محاولـة للقرصنـة أو اختراق جهاز الحاسـب الآلي يسـارع بإغلاق منافذ الدخول أمـام المخترق ثـم يبدأ في عملية مطاردة تسـتهدف اقتفـاء اثر مرتكب عمليـة الاختراق حتى يصل إلى الجهـاز الذي حدثـت العملية من خلالـه، وقد تمت إجراء تجربة عملية على البرنامج محليا، وتم التأكد من أنـه برنامج فعال، وذكر صاحـب التجربة، أنه خلال اختبـار البرنامج تعرض جهـازه، لأكثر من (١٧) محاولـة اختراق في فترة قصيرة، وبعد اقتفاء الأثـر قـاد البرنامج صاحب التجربـة إلى أفراد من مدن. للمزيد ينظر: سـليمان مهجع العنزي: وسـائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، اكاديمية نايـف العربية للعلـوم الامنية، الريـاض، ٢٠٠٣، ص١٠٠.

(١٧) عزالديـن عثمانـي: إجراءات التحقيـق والتفتيش في الجرائم الماسـة بأنظمة الاتصال والإلكترونية، مجلـة البحـوث والدراسـات القانونية والسياسـية، العدد الرابع، كلية الحقوق والعلوم السياسية، جامعة البليدة، الجزائر، ٢٠١٨، ص٥٥.

(١٨) حسـين بـن سـعيد بن سـيف الغافري: السياسـة الجنائيـة فـي مواجهـة جرائـم الانترنت (دراسـة مقارنـة)، اطروحة دكتوراه، كليـة الحقوق، جامعة عين شمس، القاهرة، ٢٠٠٩، ص٤٠١.

(١٩) حسـن طاهـر داود: جرائم نظم المعلومات، ط١، مركز الدراسـات والبحوث، اكاديمية نايف العربية للعلوم الامنية، الرياض، ٢٠٠٠، ص٢٢٨-٢٢٩.

(٢٠) سليمان مهجع العنزي: مرجع سابق، ص١٠٢.

(٢١) محمد بن نصير محمد السـرحاني: مرجع سابق، ص٨٥ وما بعدها.

(٢٢) د. جميـل عبد الباقي الصغير: الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص١١٥.

(٢٣) حسـين بن سعيد بن سيف الغافري: مرجع سابق، ص٣٩٥.

(٢٤) عبـدالله بـن حسـين القحطاني: تطويـر مهارات التحقيـق الجنائي في مواجهـة الجرائم الإلكترونية، رسـالة ماجسـتير، قسـم العلـوم الشـرطية، كليـة الدراسـات العليـا، جامعـة نايـف العربيـة للعلـوم الامنية، الرياض، ٢٠١٤، ص٦١.

(٢٥) محمد بن نصير محمد السـرحاني: مرجع سابق، ص٩٧.

(٢٦) حسـين بن سعيد بن سيف الغافري: مرجع سابق، ص٣٩٦.

(٢٧) محمد بن نصير محمد السـرحاني: مرجع سابق، ص٩٩.

(٢٨)د. محمد عيد الغريب: مبادئ الاجراءات الجنائية، بلا دار نشر، ٢٠٠٤، ص٣٧٣.

(٢٩) د. سعيد عبداللطيف حسن: اثبات جرائم الكمبيوتر والجرائم المرتكبة عبـر الأنترنت (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، ط١، دار النهضة العربية، القاهرة، ١٩٩٩، ص١٣٤.

(٣٠) د. محمـود مصطفـى: شـرح قانـون الاجراءات الجنائيـة، ط١٢، دار النهضـة العربيـة، القاهـرة، ١٩٨٣، ص٣٠٠.

(٣١) د. عمـار عبـاس الحسـيني: التحقيـق الجنائـي والوسـائل الحديثـة فـي كشـف الجريمـة، ط١، منشـورات الحلبـي الحقوقيـة، بيـروت، ٢٠١٥، ص٢٩٣.

(٣٢) جـلال حماد عرميط الدليمي: ضَمَانات المتهم في إجـراءات التحقيق الجنائي المقيدة لحريته والماسـة بشخصه (دراسـة مقارنة)، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥، ص١٢٦.

(٣٣) المواد (١٢٣-١٢٩) من قانون اصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل.

(٣٤) المـادة (١٢٣) مـن قانـون اصـول المحاكمـات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل.

(٣٥) نصـت المـادة (٥٠/ ب) مـن قانـون اصـول المحاكمـات الجزائيـة العراقـي رقـم (٢٣) لسـنة ١٩٧١ المعدل، على أن ((يكون للمسؤول في مركز الشـرطة في الاحوال المبينة فـي هذه المادة والمادة ٤٩ سلطة محقق)).

(٣٦) المـادة (٥٠/أ) مـن قانـون اصـول المحاكمـات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل.

(٣٧) د. حسن جوخدار: شرح قانون اصول المحاكمات الجزائية الاردني، ج١، دار الثقافة للنشر والتوزيع، عمان، ١٩٩٣، ص٣١٦.

(٣٨) يقصـد بالشـهادة المباشـرة هـي المعلومات التي يدلي بها الشـخص، والتي وصلت إلى حواسـه عن طريق مباشـر ودون وساطة شخص كأن يكون هذا الشـاهد قد رأى أو سـمع أو شـم... الخ، أي أن يقوم الشـاهد بالإدلاء بما شاهده من قيام مرتكب الجريمة بأيـة ترتيبات برمجية تتعلق بمرتكـب الجريمة، أو من خلال ما شـاهده من قيام مرتكب الجريمة بعملية الاختـراق لأي ملفـات الكترونيـة، أو القيـام بـأي من أنـواع التزويـر الالكتروني، أما الشـهادة غير المباشـرة فالشـاهد هنا لم يرى الجريمـة ترتكب أو لم يسـمع الجاني يتهدد ويتوعد المجني عليه، ولكنه سـمع عن طريق شـخص آخر وهي تفترض رواية الشـاهد عن غيـره، فهو لـم يعاين الواقعة بنفسـه، وإنما سـمع غيـره يذكـر معلومات بشـأن ارتكاب جريمـة معلوماتيـة. ينظـر: د. احمـد سـعد محمد الحسـيني: الجوانب الاجرائية للجرائم الناشـئة عن استخدام الشبكات الالكترونية، دار الجامعة الجديدة، الاسكندرية، ٢٠١٩، ص٢١٠-٢١١.

(٣٩) سعود على عبدالله: الدليل الالكتروني وحجيته في الإثبات الجنائي (دراسـة مقارنة)، رسالة ماجستير، كلية القانون، جامعة الشـارقة، الامارات، ٢٠١١، ص١٤٧.

(٤٠) د. هلالي عبد اللاه أحمد: التزام الشـاهد بالإعلام في الجرائم الإلكترونية (دراسـة مقارنة)، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٨، ص ٣٥.

(٤١) د. سـمير عالية: الجرائـم الالكترونية في القانون الجديـد رقم ٢٠١٨/٨١ والمقـارن (حرية التواصل الالكترونـي والقواعـد العقابيـة والاجرائية)، ط١، منشـورات الحلبـي الحقوقيـة، بيـروت، ٢٠٢٠، ص٤٣٦.

(٤٢) المـادة (٢٤/ثالثـا) من مشـروع قانـون الجرائم الإلكترونية العراقي لسنة ٢٠١١.

(٤٣) المادة (٥٨) من قانون اصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل.

(٤٤) د. سـعيد حسـب الله عبدالله: شـرح قانون اصول المحاكمات الجزائية، دار الحكمة للطباعة والنشـر، الموصل، ١٩٩٠، ص ١٨٤.

(٤٥) د. عمار عباس الحسيني: مرجع سابق، ص١٨٤.

(٤٦) د. سمير عالية: مرجع سابق، ص٤٣٤.

(٤٧) للمزيد بشـأن الوسائل المادية والوسائل الإجرائية التي يسـتعين بها الخبيـر المعلوماتي في اكتشـاف الدليـل الإلكتروني، ينظـر: د. أحمد عاصم عجيلة: الحمايـة الجنائيـة للمحررات الالكترونية (دراسـة مقارنـة)، دار النهضـة العربيـة، القاهرة، ٢٠١٤، ص٤٤٤-٤٤٦.

(٤٨) د. طـه السـيد احمد الرشـيدي: الطبيعة الخاصة لجرائـم تقنيـة المعلومـات واثرها علـى اجراءات التحقيـق في النظام الجزائي المصري والسـعودي، ط١، دار الكتب والدراسـات العربية، الاسـكندرية، ٢٠١٦، ص١٢١-١٢٢.

(٤٩) د. محمود نجيب حسـني: شرح قانون الاجراءات الجنائيـة، ط٢، دار النهضـة العربيـة، القاهـرة، ١٩٨٨، ص٧٧٠.

(٥٠) يعـود اسـتخدام هـذا المصطلح إلى جهـد العديد مـن المنظمـات والمعاهـدات الدوليـة المهتمـة بمكافحـة الجرائـم الإلكترونيـة، وذلـك فـي إطار تطويـر بعض المصطلحـات القانونية المسـتخدمة في مجـال التحقيق الجنائي في هـذه الجرائم، وذلك باسـتحداث مصطلحات معلوماتية جديدة تتلاءم مع البيئة الإلكترونية التي تسـتخدم فيهـا، مع الاحتفاظ بجذورهـا التقليدية، ومن المصطلحـات التي لحقها التطويـر (التفتيش)، واسـتخدام مصطلح (الولوج) بـدلاً منه، وهو مـا نصت عليه المـادة ١٩ بفقرتيها الأولى والثانية من الاتفاقية الأوروبية بشأن الجريمة الإلكترونية. نقلًا عن: د. محمد كمال شاهين: مرجع سابق، ص٢٧١.

(٥١) د. علـي حسـن الطوابلة: التفتيـش الجنائي على نظم الحاسـوب والأنترنت، ط١، مؤسسـة فخراوي

للدراسات والنشر، مملكة البحرين، ٢٠١٠، ص٢٠. ود. هلالي عبد اللاه احمد: اتفاقية بودابست لمكافحة الجرائم الإلكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٧، ص٢٤٢ وما بعدها.

(٥٢) د. هشام محمد فريد رستم: الجوانب الاجرائية للجرائم المعلوماتية، ط١، دار النهضة العربية، القاهرة، ١٩٩٨، ص٦٦.

(٥٣) د. نبيلة هبه هروال: الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، ٢٠٠٧، ص٧٤.

(٥٤) د. محمد كمال شاهين: مرجع سابق، ص٢٧٨.

(٥٥) اسامة احمد المناعسة وجلال الزعبي وصايل فاضل: جرائم الحاسب الآلي والإنترنت (دراسة تحليلية مقارنة)، ط١، دار وائل للطباعة والنشر والتوزيع، عمان، ٢٠٠٠، ص١٠٥.

(٥٦) وتتمثل الشروط الموضوعية للتفتيش بما يلي: ١- بسببه: وقوع جريمة من نوع جناية أو جنحة، وان يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه. ٢- الغاية منه: ضبط أشياء تفيد في كشف الحقيقة. أما الشروط الشكلية فتتحدد بما يلي: ١- أن يكون الأمر بالتفتيش مسبباً. ٢- حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش -٣- تحرير محضر بالتفتيش. للمزيد ينظر: د. محمد ابو العلا عقيدة: شرح قانون الاجراءات الجنائية، ج١، دار النهضة العربية، القاهرة، ٢٠٠١، ص٤٣١ وما بعدها.

(٥٧) د. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي (دراسة مقارنة)، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٨، ص١٢٦.

(٥٨) للمزيد حول آراء هؤلاء الفقهاء ينظر: د. احمد عاصم عجيلة: مرجع سابق، ص٤١٣.

(٥٩) المادة (١/١٩) من اتفاقية بودابست الصادرة عن مجلس أوربا بتاريخ ٢٠٠١/١١/٢٣ بشأن الجرائم الإلكترونية، والتي نصت على أنه ((يجب على كل طرف أن يتبنى الإجراءات التشريعية واية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي أو لجزء منه، وكذلك للبيانات الإلكترونية المخزنة فيه، أو لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية)). مشار إليها عند د. هلالي عبد اللاه أحمد: اتفاقية بودابست لمكافحة الجرائم الإلكترونية، مرجع سابق، ص٢٣٧ وما بعدّها.

(٦٠) يقصد بشبكات الانترنت او الحاسب الآلي: بأنها مجموعة مكونة من جهازين أو أكثر من أجهزة الحاسب الآلي المتصلة ببعضها اتصالاً سلكياً أو لاسلكياً، فهناك شبكات واسعة في أماكن متفرقة ترتبط ببعضها البعض عن طريق الاجهزة الحاسوبية. ينظر: د. خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١، ص١٥٨.

(٦١) بكري يوسف بكري: التفتيش عن المعلومات في وسائل التقنية الحديثة، ط١، دار الفكر الجامعي، الاسكندرية، ٢٠١١، ص٨١ وما بعدها.

(٦٢) د. هلالي عبد اللاه احمد: تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي (دراسة مقارنة)، مرجع سابق، ص٧٩. ود. محمد كمال شاهين: مرجع سابق، ص٢٩٠.

(٦٣) د. سمير عالية: مرجع سابق، ص٤٨٨.

(٦٤) د. فوزية عبد الستار: شرح قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٦، ص٦١٥.

(٦٥) د. محمود نجيب حسني: مرجع سابق، ص٥٦١.

(٦٦) د. محمد كمال شاهين: مرجع سابق، ص٣١٩.

(٦٧) سعيد سالم المزروعي وعزمان عبدالرحمن: اجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقًا للتشريع الاماراتي، مجلة العلوم الاقتصادية والادارية والقانونية، العدد الثالث عشر، المجلد الثاني، المركز القومي للبحوث، فلسطين، ٢٠١٨، ص١٢٢.

(٦٨) د. سمير عالية: مرجع سابق، ص٤٩١.

(٦٩) المادة (١٣٤) من قانون اصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل.

قائمة المصادر والمراجع

اولًا: الكتب العربية:

١. احمد سعد محمد الحسيني: الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، دار الجامعة الجديدة، الاسكندرية، ٢٠١٩.

٢. احمد عاصم عجيلة: الحماية الجنائية للمحررات الإلكترونية (دراسة مقارنة)، دار النهضة العربية، القاهرة، ٢٠١٤.

٣. اسامة احمد المناعسة وجلال الزعبي وصايل فاضل: جرائم الحاسب الآلي والإنترنت (دراسة تحليلية مقارنة)، ط١، دار وائل للطباعة والنشر والتوزيع، عمان، ٢٠٠٠.

٤. بكري يوسف بكري: التفتيش عن المعلومات في وسائل التقنية الحديثة، ط١، دار الفكر الجامعي، الاسكندرية، ٢٠١١.

٥. جلال حماد عرميط الدليمي: ضمانات المتهم في إجراءات التحقيق الابتدائي المقيدة لحريته والماسة بشخصه (دراسة مقارنة)، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥.

٦. حسن جوخدار: شرح قانون اصول المحاكمات الجزائية الاردني، ج١، دار الثقافة للنشر والتوزيع، عمان، ١٩٩٣.

٧. حسن طاهر داود: جرائم نظم المعلومات، ط١، مركز الدراسات والبحوث، اكاديمية نايف العربية للعلوم الامنية، الرياض، ٢٠٠٠.

٨. خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١.

٩. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الاسكندرية، ٢٠١٠.

١٠. زياد محمد عبود وغسان حميد عبد المجيد واخرون: اساسيات الحاسوب وتطبيقاته المكتبية، ج١، الدار الجامعية للطباعة والنشر والتأليف والترجمة، وزارة التعليم العالي والبحث العلمي العراقية، بغداد، ٢٠١٤.

١١. سعيد حسب الله عبدالله: شرح قانون اصول المحاكمات الجزائية، دار الحكمة للطباعة والنشر، الموصل، ١٩٩٠.

١٢. سعيد عبداللطيف حسن: اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، ط١، دار النهضة العربية، القاهرة، ١٩٩٩.

١٣. سليمان عبدالمنعم: اصول الاجراءات الجنائية (دراسة مقارنة)، الكتاب الثاني، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥.

١٤. سمير عالية: الجرائم الالكترونية في القانون الجديد رقم (٢٠١٨/٨١) والمقارن (حرية التواصل الالكتروني والقواعد العقابية والاجرامية)، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٢٠.

١٥. طه السيد احمد الرشيدي: الطبيعة الخاصة لجرائم تقنية المعلومات واثرها على اجراءات التحقيق في النظام الجزائي المصري والسعودي، ط١، دار الكتب والدراسات العربية، الاسكندرية، ٢٠١٦.

١٦. عادل عبد ابراهيم العاني: شرح قانون الجزاء العماني (القسم العام)، ط١، دار الأجيال، عمان، ٢٠٠٨.

١٧. عبد الحميد الشواربي: ضمانات المتهم في مرحلة التحقيق الجنائي، منشأة المعارف، الاسكندرية، ١٩٨٨.

١٨. علي حسن الطوابلة: التفتيش الجنائي على نظم الحاسوب والأنترنت، ط١، مؤسسة فخراوي للدراسات والنشر، مملكة البحرين، ٢٠١٠.

١٩. عمار عباس الحسيني: التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥.

٢٠. فوزية عبد الستار: شرح قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٦.

٢١. مأمون سلامة: قانون الاجراءات الجنائية معلقًا عليه بالفقه واحكام النقض، ج١، ط٣، دار النهضة العربية، القاهرة، ٢٠٠٩.

٢٢. محمد ابو العلا عقيدة: شرح قانون الاجراءات الجنائية، ج١، دار النهضة العربية، القاهرة، ٢٠٠١، ص٤٣١ وما بعدها.

٢٣. محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٤٠.

٢٤. محمد عيد الغريب: مبادئ الاجراءات الجنائية، بلا دار نشر، ٢٠٠٤.

٢٥. محمد كمال شاهين: الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، دار الجامعة الجديدة، الاسكندرية، ٢٠١٨.

٢٦. محمود مصطفى: شرح قانون الاجراءات الجنائية، ط١٢، دار النهضة العربية، القاهرة، ١٩٨٣.

٢٧. محمود نجيب حسني: شرح قانون الاجراءات الجنائية، ط٢، دار النهضة العربية، القاهرة، ١٩٨٨.

٢٨. ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٦.

٢٩. نبيلة هبه هروال: الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، ٢٠٠٧.

٣٠. هشام محمد فريد رستم: الجوانب الاجرائية للجرائم المعلوماتية، ط١، دار النهضة العربية، القاهرة، ١٩٩٨.

٣١. هلالي عبد اللاه احمد: اتفاقية بودابست لمكافحة الجرائم الإلكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٧.

٣٢. هلالي عبد اللاه أحمد: التزام الشاهد بالإعلام في الجرائم الإلكترونية (دراسة مقارنة)، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٨.

٣٣. هلالي عبد اللاه أحمد: تفتيش نظم

الحاسب الآلي وضمانات المتهم المعلوماتي تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي (دراسة مقارنة)، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٨.

ثانيًا: الرسائل والاطاريح الجامعية:

١. حسين بن سعيد بن سيف الغافري: السياسة الجنائية في مواجهة جرائم الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠٠٥.

٢. سعود علي عبدالله: الدليل الالكتروني وحجيته في الإثبات الجنائي (دراسة مقارنة)، رسالة ماجستير، كلية القانون، جامعة الشارقة، الامارات، ٢٠١١.

٣. سليمان مهجع العنزي: وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، اكاديمية نايف العربية للعلوم الامنية، الرياض، ٢٠٠٣.

٤. عبدالله بن حسين القحطاني: تطوير مهارات التحقيق الجنائي في مواجهة الجرائم الإلكترونية، رسالة ماجستير، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الامنية، الرياض، ٢٠١٤.

٥. محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت (دراسة مسحية على ضباط الشرطة في المنطقة الشرقية)، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الامنية، الرياض، ٢٠٠٤.

ثالثًا: البحوث والدوريات:

١. سعيد سالم المزروعي وعزمان عبدالرحمن: اجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقًا للتشريع الاماراتي، مجلة العلوم الاقتصادية والادارية والقانونية، العدد الثالث عشر، المجلد الثاني، المركز القومي للبحوث، فلسطين، ٢٠١٨.

٢. عزالدين عثماني: إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والإلكترونية، مجلة البحوث والدراسات القانونية والسياسية، العدد الرابع، كلية الحقوق والعلوم السياسية، جامعة البليدة، الجزائر، ٢٠١٨.

رابعًا: القوانين:

١. قانون أصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل.

٢. مشروع قانون جرائم المعلوماتية العراقي لسنة ٢٠١١.

سادسًا: المواقع الالكترونية:

١. مقال بعنوان (ذاكرة مخبئة) منشور على شبكة المعلومات الدولية (الانترنت)، الموقع الالكتروني: ويكيبيديا الموسوعة الحرة، الرابط الالكتروني: https://ar.wikipedia.org.

Cybercrime Investigation Procedures

Asst.Lect. Salah Mahmood Khudair(*)

Abstract

The many positives brought about by technological development in facilitating the transfer and exchange of information and data, accompanied by some side purposes represented in the exploitation of this development by some networks, bodies, gangs and individuals to commit acts that intersect with the laws, customs, morals and morals prevailing in society, hence it was necessary for the various legislations to keep pace with this remarkable development in cybercrime, as scientific and technological progress cannot proceed, or work alone in isolation from any legal progress that preserves it and ensures its protection and puts Solutions to the obstacles that may arise due to its use, in this case technological progress can become a tool for construction and the basis for every development, provided that at the same time if it is misused, it can become a tool for crime and a means of committing it, and there is no doubt that these crimes are one of the most serious and complex crimes at all, based on their distinct and complex nature in terms of subjectivity of their pillars, the modernity of the methods of committing them, the environment to which they respond, the privacy of the perpetrators and the means of detecting and investigating them .

Keywords: Cybercrime_Hacking_Investigation_Electronic Testimony

(*)Al -Ammal College