المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثاني عشر شهر (6) / 2019
www.eimj.com

التحقيق الجنائي في الجرائم الالكترونية في القانون الدولي العام

Criminal Investigation of Cybercrime in Public International Law

دكتور موسى عبد الحافظ مناحي المهيرات

أستاذ مساعد في القانون العام/ جامعة عمان الأهلية

Mousa.alabbadi@jfda.jo

الملخص:

تعتبر الجريمة الالكترونية من الجرائم المستحدثة في عالمنا المعاصر، وبتطور الجريمة كان لزاماً على رجال البحث والتحري والتحقيق تطوير إمكانياتهم لمكافحة هذا النوع من الجرائم.

هدفت هذه الدراسة الى تحديد مهارات التحقيق الجنائي للمحققين في لجنة التحقيق والمقاضاة في الجرائم الالكترونية، وتحديد أبرز العقبات التي تعترض سبيل التنمية التي تحول دون تطوير وإتقان مهارات التحقيق الجنائي في هذا النوع من الجرائم، كما هدفت الى تحديد أهم الطرق والأساليب التي تساعد في تطوير مهارات المحقق الجنائي في مواجهة الجرائم الالكترونية، وقد إعتمدت الدراسة على عدة مناهج كالمنهج المنهج الإستقرائي (التأصيلي) والمنهج الإستنباطي. توصلت الدراسة الى أنه من الصعب إكتشاف الجريمة الالكترونية، حيث يبدو أن عدد الحالات التي إكتُشِفَت فيها هذه الجرائم قليل مقارنة بالجرائم التقليدية؛ ويمكن تفسير الأسباب الكامنة وراء صعوبة إكتشاف الجريمة السيبرانية من خلال حقيقة أن هذه الجريمة لا تترك أي تأثير خارجي مرئي، كما أنه يمكن للجاني أن يرتكب هذه الجريمة في دول وقارات أخرى نتيجة لما أحدثه التطور التكنولوجي من تلاشي لحدود الزمان والمكان، وتوصلت الدراسة إيضاً الى أن أهم التحديات التي تواجه المحققين الجنائيين هي اكتشاف الجريمة السيبرانية، فهذا الأمر صعبٌ للغاية، وإذا كان إكتشاف وقوع هذه الجريمة والإبلاغ عنها أمر سهل، الا أن الدليل على هوية مرتكبها محاط بالعديد من الصعوبات، الأمر الذي يتطلب الكثير من المعرفة والخبرة الفنية اللتان يحتاجان لوقت ومجهود كبيرين من قبل المحققين للوصول اليهما.

الكلمات المفتاحية : التحقيق الجنائي، الجرائم السيبرانية، الجرائم الالكترونية، الأدلة الجنائية، الحماية الجنائية.

Abstract:

Cyber Crime is an emerging crime in our modern world. With the development of crime, men of research, investigation and investigation have to develop their potential to combat this type of crime.

This study aims to determine the skills of criminal investigation of the investigators in the Commission of Investigation and Prosecution in cybercrime, and to identify the most important obstacles to development that prevent the development and mastering of criminal investigation skills in this type of crime. It also aimed to identify the most important methods and methods that help in developing skills Criminal Investigation in the face of cybercrime. The study was based on a number of approaches such as the inductive method of approach and the deductive approach. The study found that it is difficult to detect cybercrime, as the number of cases in which these crimes have been discovered appears to be small compared to traditional crimes; the reasons behind the difficulty of detecting cybercrime can be explained by the fact that this crime does not leave any external visual impact, This crime is committed in other countries and continents as a result of the technological deterioration of time and space. The study also concluded that the most important challenges facing criminal investigators are the discovery of cybercrime. Crime and reporting is easy, but the evidence of the perpetrator is surrounded by many difficulties, which requires a lot of knowledge and expertise that require considerable time and effort by investigators to reach them.

Keywords: Criminal Investigation, Cybercrime, Electronic Crimes, Criminal Evidence, Criminal Protection.

المقدمة:

تُعد الجريمة الالكترونية نمطاً حديثاً من الأنماط المستحدثة للجريمة التي لم تشهدها المجتمعات القديمة، فقد ظهرت في المجتمعات المعاصرة نتيجة التطور التكنولوجي الذي شمل جميع مجالات الحياة. وعلى الرغم من ظهور تلك الجريمة بثوب حديث على غير مثال سابق؛ إلا أنها كالجريمة التقليدية المعهودة تماماً تمثل عمل غير قانوني يعاقب عليه من قبل الدولة أو السلطة، والفارق هنا يكمن في أنها تتم بإستخدام التكنولوجيا الحديثة مثل الحاسب الالي والإنترنت والتطبيقات والبرامج المتعلقة به، والتي تُنَفَذ في غياب الأمن الالكتروني، ونظرًا لأن تلك الجرائم يتم تنفيذها بدرجة كبيرة من الذكاء الإنساني مصحوبًا بإستخدام تقنيات معقدة؛ فإن التحقيق فيها مهمة معقدة للغاية مقارنة بالجرائم التقليدية (Kaur, 2018). فإرتباط هذا النوع من الجرائم بالتكنولوجيا أتى نتيجةٌ لتمكين الأفراد بالقيام بأي نشاط من أي مكان بسهولة مهما بعُدت المسافات، سواء كان ذلك النشاط قانونيًّا كعمليات البيع والشراء وتبادل المعلومات والتواصل الاجتماعي، أو غير قانوني كالإحتيال والتجارة في المواد الإباحية والتعدي على الملكية الفكرية وسرقة الهويات، أو إنتهاك خصوصية البيانات الرقمية من أنظمة الكمبيوتر والأجهزة الالكترونية الأخرى (Dacey & Kenneth, 1997).

وهناك أنواع مختلفة من الجرائم الالكترونية منها ما يستهدف الأفراد و أخرى تستهدف المؤسسات العامة و الخاصة؛ فإستخدام أصحاب النفوس الضعيفة لتقنية المعلومات مع توفر أدوات القرصنة التي لا تحتاج للكثير من الخبرة والمهارة جعل العالم الالكتروني في خطرٍ كبير لا يمكن تجنبه الا بإتخاذ كافة إجراءات السلامة (Choi, et.al., 2007). ولقد شعر المسؤولون عن إنفاذ القانون بالإحباط بسبب عجز المشرعين عن إبقاء تشريعات الجرائم الالكترونية متقدماً على المنحنى التكنولوجي سريع الحركة (Jain & Vibhash, 2014).

ويعد التحقيق الجنائي وجمع الأدلة والإستنتاجات من الأنشطة الأمنية التي تتصدر محاولات مواجهة الجرائم السيبرانية من خلال تطوير الأساليب والإرتقاء بالمحققين وتزويدهم بالعلوم والتكنولوجيا الحديثة. فالتكنولوجيا ركيزة أساسية في التطور العلمي والتقني للدول ككل والتحقيق الجنائي على وجه الخصوص، فقد ساعدت على توفير آليات متقدمة وأنظمة إتصالات حديثة، بل تجاوز ذلك لتشمل طرقًا جديدة في العمل على كشف الحقيقة وانتزاعها من براثن البهتان للوقوف على الطريق الصحيح. قال تعالى " وَيُحِقُّ اللَّهُ الحَقَّ بِكَلِمَاتِهِ وَلَوْ كَرِهَ المُجْرِمُونَ" (سورة يونس، آية ٨٢)، ولن يتحقق هذا الا من خلال الإلمام بأساليب البحث الجنائي بما يتوافق مع التكنولوجيا المتقدمة، وخاصة في الجرائم المستحدثة للعلاقة بين أساليب إرتكابها للعلوم والتكنولوجيا الحديثة (البلوي، ٢٠٠٩).

مشكلة الدراسة:

لكل عصر خصائصه وسماته. فقد إمتاز العصر الحالي بدخول ثورة تكنولوجيا المعلومات والإتصالات وما تحدثه من تغيير في نمط الحياة على مستوى الأفراد والحكومات. فلا يمكن إنكار حقيقة تأثير التقدم التكنولوجي على القانون والواقع الذي يظهر به، وبالتالي فيجب عدم فصل القانون عن الواقع الذي ينتجه ويُطبق عليه، بل ويجب أن يكون متجأوبًا ومطورًا بنفس وتيرة التطور (إبراهيمي، ٢٠١٨). وفي السنوات الأخيرة، أنشأ التطور التقني الحديث نمطًا جديداً معقدًا من الجرائم يرتكبها مجرمون ذو مهارات فنية وتقنية عالية في وسائل ارتكاب الجرائم، سعى المجرم من خلالها بإستخدام التكنولوجيا لتمرير جرائمه على الجهات القانونية، كما سعت الجهات القانونية الى الحصول على أحدث التقنيات للكشف عن هذه الجرائم التي لا تتماثل مع الجرائم التقليدية التي لا بد بها أن يترك الجاني الخيط لحل لغز الجريمة من خلال ترك أثار له في مسرح الجريمة، أو أن يترك مسرح الجريمة أثاره عليه، وعليه فإن فشل الجهات القانونية والأمنية في الجرائم الالكترونية يتمثل في الحصول على أحدث التقنيات التي تكشف الحقيقة من خلال تحليل الآثار البيولوجية والمادية، وبالتالي يجب تدريب المورد البشري في هذه الجهات على التقنيات لتمكينه من مواكبة تطورات هذا المجال (البلوي، ٢٠٠٩) ، ويتطلب التحقيق في الجريمة الالكترونية مهارات ذات طبيعة خاصة يجب على المحقق أن يكون قادرًا على القيام بها، وقد قال رئيس شعبة المتابعة والتحقيق الخاصة بإدارة البحث الجنائي في مديرية الأمن العام في الأردن المقدم الدكتور رمزي الدبك أن الإحصائيات تشير الى إرتفاع نسبة الجرائم الالكترونية منذ العام ٢٠٠٨ وحتى عام ٢٠١٧، إذا كانت ١٦ جريمة لترتفع الى ٢٠٣٨ جريمة وبين الدبك خلال محاضرة عقدت في كلية القانون بجامعة عمان العربية، إن هذه النتيجة طبيعة لعوامل أبرزها أن مستخدمي الإنترنت إرتفع حتى حزيران ٢٠١٧ الى أكثر من ٨ ملايين من مستخدمي الفيس بوك (موقع جراءة نيوز-موقع إخباري أردني).

وبناءا عن المشكلة البحثية فان الدراسة تقوم بدراسة عدة تساؤلات اهمها ما يلي:

١. ما مدى توفر مهارات التحقيق الجنائي للمحققين في لجنة التحقيق والمقاضاة في الجرائم الالكترونية؟
٢. ما هي أهم الطرق والأساليب التي تساعد في تطوير مهارات التحقيق الجنائي لمواجهة الجرائم الالكترونية؟
٣. ما هي أبرز العقبات التي تعترض سبيل التنمية وتحول دون تطوير وإتقان مهارات التحقيق الجنائي في جرائم الإنترنت؟

أهداف الدراسة:

تهدف هذه الدراسة الى تحديد أهم الطرق التي تساعد في تطوير مهارات التحقيق الجنائي لمواجهة الجرائم الالكترونية من خلال تحقيق الأهداف التالية:

١. تحديد مهارات التحقيق الجنائي للمحققين في لجنة التحقيق والمقاضاة في الجرائم الالكترونية.
٢. تحديد أبرز العقبات التي تعترض سبيل التنمية والتي تحول دون تطوير وإتقان مهارات التحقيق الجنائي في الجرائم الالكترونية.
٣. تحديد أهم الطرق والأساليب التي تساعد في تطوير مهارات التحقيق الجنائي في مواجهة الجرائم الالكترونية.

منهج الدراسة:

إعتمد هذا البحث على المنهج الإستقرائي (التأصيلي) المتتبع للجزئيات التي تكشف عن المبدأ العام للتحقيق الجنائي في الجرائم الالكترونية، كما إعتمدت الدراسة على المنهج الإستنباطي الذي يعتمد على تحليل القواعد العامة والنصوص القانونية ذات الصلة ومحاولة تطبيقها على المسائل والفرعيات التي يمكن أن تندرج تحتها، وقد تم الإعتماد على كتب الفقه القانوني، والاستعانة بالمؤلفات الحديثة، والكتب القانونية، والأبحاث العالمية ذات العلاقة في جمع المادة العلمية.

هيكلة الدراسة:

قامت هذه الدراسة بالبحث في ماهية التحقيق الجنائي في الجرائم الالكترونية للارهاب في القانون الدولي العام وتضمنت مبحثين كالآتي:

المبحث الأول: الجرائم الالكترونية في القانون الدولي العام

المبحث الثاني: التحقيق الجنائي في القانون الدولي العام

المبحث الثالث: التعاون الدولي في مجال الأمن السيبراني

المبحث الأول: الجرائم الالكترونية

تختلف الجريمة المستحدثة عن الجرائم التقليدية المعهودة في المحتوى، والنطاق، والأنواع والوسائل و الطبيعة، والآثار، والأدوات. وتمتاز عنها بكثرة عدد الضحايا وإمكانية التحضر السريع، وتوافر فرص الإنتشار في ظل الإفتقار للأمن الالكتروني، وضعف التشريعات القانونية، وصعوبة فرض وتنفيذ العقوبات للحد من الآثار السلبية المترتبة على هذا النوع من الجرائم التي تستهدف البيانات والأفراد والدول بقطاعاتها المختلفة، فهي تشكل حقيقة الإستعمار الالكتروني في أسوأ أشكاله (بونعارة، ٢٠١٦)، وقد نشرت الجرائد الرسمية الأردنية بخصوص الجرائم الالكترونية القانون رقم (٢٧) لسنة ٢٠١٥ الذي ينص على أحكام الجرائم الالكترونية.

مفهوم الجرائم الالكترونية:

قبل التطرق إلى تعريف الجريمة الالكترونية لا بد من تحديد تعريف الجريمة في حد ذاتها، فمن حيث التعرف اللغوي فقد وردت كلمة المجرم في القرآن الكريم لقوله تعالى "وكَذَلِكَ نَجْزِي المُجْرِمِينَ" (سورة الأعراف، آية ٤٠).

وقد إكتفى المشرع الأردني كأغلبية التشريعات الجنائية ببيان أنواع الجريمة، وأركانها، وذكر العقوبة المترتبة على كل منها، دون أن يحدده بتعريف معين يقيد من إمكانيته في مواكبة التغيرات في ظروف وإحتياجات المجتمع الأردني في ظل التطورات الحديثة مثل الجرائم الالكترونية، خاصة قانون المعاملات الالكترونية الصادر عام ٢٠٠١، بأن المصالح العامة تتغير وفقًا للظروف الإقتصادية والإجتماعية والسياسية، وقد إكتفى المشرع الأردني بتعريف بعض أنواع الجرائم في قانون العقوبات رقم (١٦) لسنة ١٩٦٠ كجريمة السرقة التي عرفها في المادة (٣٩٩) بأنها "أخذ مال الغير المنقول دون رضاه" (الجمعات، ٢٠١٠).

وتعني الجريمة قيام الفرد بفعل محرم شرعاً ومعاقباً عليه، أو الامتناع عن القيام بفعل يأمر الشرع به ويعاقب تاركه عليه (بوالماين، ٢٠٠٨) ، وتعرف الجريمة أيضاً أنها ظاهرة سلبية إجتماعية تعبر عن خلل أو إرتباك في السلوك أو العلاقات الاجتماعية وتجسد طبيعة التناقضات في المتغيرات الموضوعية والذاتية التي تؤثر على البيئة البشرية والحياة الإجتماعية، وتشخص ماهية المشكلات الإنسانية التي يعاني منها الفرد والمجتمع على حد سواء (الحسن ١٩٩٣). أما الجريمة من الناحية القانونية فهي كل فعل يخالف أحكام قانون العقوبات، فهي فعل لا أخلاقي تنفر وتشمئز منه النفوس (عريم، ١٩٧٠).

ومع التطور المستمر في تقنية المعلومات، ظهر نوع جديد من أنواع الجرائم الا وهو الجرائم الالكترونية، حيث كان هناك العديد من وجهات النظر حول مفهوم الجريمة الالكترونية نظراً للزأوية التي تشكل هذه الجريمة، فقد تميل بعض الدراسات الى تعريفه في ضوء إعتماد منهجية تستند الى تصنيف الأنشطة المتعلقة بالكمبيوتر لفئات وأنواع (عطاي، ٢٠١٥).

فقد عرفت الجرائم الالكترونية على أنها الجرائم التي تُرتكب بإستخدام الإنترنت وأجهزة الحاسوب وتطبيقاته، والمعدات التقنية مثل الجوال (البداينة، ٢٠١٤) ، كما تعرف أيضا بأنها فعل غير مشروع صادر عن إستخدام التقنيات الحديثة يقرر لها النظام والسلطة عقوبة محددة (ال ثنيان، ٢٠١٢).

أنواع الجرائم الالكترونية:

ساهم التطور الكبير لتكنولوجيا المعلومات و الإتصالات في ظهور نوع جديد من المعاملات يسمى المعاملات الالكترونية والتي تختلف تماماً عن المعاملات التقليدية الإعتيادية، فهي تمثل جميع المعاملات التي تتم من خلال المعدات الالكترونية مثل الهواتف والفاكسات وأجهزة الكمبيوتر والإنترنت، ومؤخراً عبر الهاتف المحمول (حجازي، ٢٠٠٥)، ومن أهم أنواع الجرائم الالكترونية:

١- الإتصالات في تعزيز المؤامرات الإجرامية:

ويشمل ذلك أنشطة إجرامية تعززها أو تيسرها تكنولوجيا المعلومات، مثل تهريب الأسلحة وغسل الأموال والإتجار بالمخدرات والقمار، وإستغلال الأطفال في المواد الإباحية. وتم إكتشاف الشبكات الإجرامية لتمتد عبر الحدود الوطنية وتهدد أمنها، فهي تعمل بدرجة كبيرة من التنسيق وتستخدم وسائل متطورة للإخفاء (Longe et.al, 2009).

٢- قرصنة الإيصالات:

وهي إحدى الطرق غير القانونية لإجراء المكالمات الهاتفية الصادرة عبر الإنترنت دون المرور عبر شبكة الهاتف العامة من خلال شبكة شركة الإتصالات المرخص لها قانونياً، بتمرير هذه المكالمات بإستخدام الوسائل التقنية المعدة أصلاً لنقل البيانات والمعلومات مثل محطات الإتصال عبر الأقمار الصناعية ومحطات الميكروويف وتهريب المكالمات عبر الإنترنت وغيرها من الوسائل (بوابة باب الإخبارية)، وقد نصت المادة ٤ من قانون العقوبات الأردني رقم ٢٧ لسنة ٢٠١٥ أنه "يعاقب كل من أدخل أو نشر أو أستخدم قصداً برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لالغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو اعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليه أو تغيير موقع الكتروني أو الغائه أو اتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو إنتحال الشخصية المالكة دون تصريح أو بما يجأوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) ماتي دينار ولا تزيد على (١٠٠٠) الف دينار"، وذكرت المادة ٥ من نفس القانون على أنه "يعاقب كل من قام قصداً بالتقاط أو بإعتراض أو بالتصنت أو أعاق أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة و بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) الف دينار".

٣-نشر المواد الاباحية والمسيئة:

ويمثل محتوى يعتبره بعض الأشخاص مرفوضًا بشكل كبير في الفضاء الالكتروني. كالدعاية العنصرية، والمواد الجنسية الصريحة، وتعليمات تصنيع أجهزة متفجرة و التهابية. ويمكن أيضًا إستخدام أنظمة الإتصالات لتهديد أو مضايقة شخص ما، حيث يتم إرسال الرسائل المستمرة الى مستلم لا يرغب بإستلامها، أو تهديد أحدهم بعدة طرق بدءًا من تهديده بالمكالمة الهاتفية الفاحشة التقليدية الى مظهرها المعاصر في الملاحقة الالكترونية لصوره وملفاته ومعلوماته Calling off Cyber Crime)،

وقد نص القانون ٢٧ لعام ٢٠١٥ في الثلاث مواد التالية ٩، ١٠، ١١ عن عرض واستخدام المواد المسيئة والاباحية وبخاصة لمن هم دون ١٨ من العمر بالآتي:

المادة ٩

أ. يعاقب كل من ارسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالا إباحية وتتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٣٠٠) ثلاثمائة دينار ولا تزيد على (٥٠٠٠) خمسة الاف دينار.

ب. يعاقب كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا أو عقليا، أو توجيهه أو تحريضه على ارتكاب جريمة، بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (١٠٠٠) الف دينار ولا تزيد على (٥٠٠٠) خمسة الاف دينار.

ج. يعاقب كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا أو عقليا، في الدعارة أو الأعمال الإباحية بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (٥٠٠٠) خمسة الاف دينار ولا تزيد على (١٥٠٠٠) خمسة عشر الف دينار. المادة ١٠

يعاقب كل من استخدم الشبكة المعلوماتية أو أي نظام معلومات أو أنشأ موقعا الكترونيا للتسهيل أو الترويج للدعارة بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (٣٠٠) ثلاثمائة دينار ولا تزيد على (٥٠٠٠) خمسة الاف دينار.

المادة ١١

يعاقب كل من قام قصدا بإرسال أو إعادة إرسال أو نشر بيانات أو معلومات عن طريق الشبكة المعلوماتية أو الموقع الالكتروني أو أي نظام معلومات تنطوي على ذم أو قدح أو تحقير أي شخص بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠٠) الفي دينار.

٣- غسيل الأموال الالكترونية والتهرب الضريبي

وهي إحدى أشكال الفساد المالي، والذي يشكل بلاءً قديما وحديثاً للمجتمع، فقد وجدت في جميع العصور، وجميع المجتمعات، متعلماً وأمياً، غنياً وفقيراً، قوياً وضعيفاً. ويرتبط ظهورها وتطور مخاطرها من خلال زيادة رغبة الإنسان في الحصول على مكاسب مادية أو معنوية بطرق غير قانونية، وهي واضحة جداً في مجتمعات العالم الثالث، خاصة في منظماتهم الحكومية، لأنها السبب في مشاكلهم الاقتصادية وتخلفهم (حسين، بدون سنة نشر).

٤- التخريب الالكتروني والإرهاب والإبتزاز:

تُعد جرائم الإبتزاز شكلًا من أشكال الجرائم الالكترونية الحديثة، وهي من أخطر الجرائم؛ لأنها تهدد أمن المجتمع وسلامته، ومن الأمثلة عليها: تلك الجرائم التي تحدث من خلال مواقع التواصل الاجتماعي، فنجد أن البعض منهم يغررون بالفتيات ويسعون الى تأسيس العلاقات غير الشرعية معهن عن طريق الخداع أو التهديد أو الابتزاز العاطفي، وقد يقومون نشر صور خاصة لهن لا يصح نشرها عبر مواقع التواصل الاجتماعي؛ وهذا يعرضهن لمأساة كبيرة ويضر ببسمعتهن في المجتمع، وقد تتخذ الجريمة شكل الابتزاز المادي الذي تضطر معه الفتيات لدفع مبالغ مالية لهؤلاء المجرمين خوفًا من الفضائح التي قد يتعرضن لها إذا لم يدفعن لهم، ومنها كذلك استغلال القُصّر من الجنسين بهدف تحقيق أرباح مالية، ولعل تلك الجرائم من أشد الأخطار التي تتعرض لها المجتمعات في عصرنا الحالي (الالفي، بدون سنة نشر)، وقد نصت المادة ٣ من قانون العقوبات الأردني رقم ٢٧ لسنة ٢٠١٥ على الآتي:

أ- يعاقب كل من دخل قصداً الى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخلف أو تجأوز التصريح ، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مئة دينار ولا تزيد على (٢٠٠) مئتي دينار أو بكلتا هاتين العقوبتين.

ب- إذا كان الدخول المنصوص عليه لالغاء أو حذف أو اضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) الف دينار.

ج- يعاقب كل من دخل قصداً الى موقع الكتروني لتغييره أو الغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو إنتحال صفته أو إنتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار و لاتزيد على (١٠٠٠) الف دينار.

٥- الغش في المبيعات والإستثمار:

يُعرّف الغش بأنه أي عمل يغير من طبيعة ومكونات وخواص وفائدة المادة، والفرق بين جرائم الغش الالكترونية والتقليدية أنه من السهل في الجرائم التقليدية تحديد الإحتيال والغش لأن طبيعة الأجسام تكون بها مرئية كمثال عليها بيع اللحوم الفاسدة، وخلط البنزين، و بيع الأدوية السامة، وبيع مستحضرات التجميل منتهية الصلاحية، أما في حالات الجريمة الالكترونية فإن الطبيعة المرئية أو الفيزيائية للمادة قد لا تكون متاحة بسهولة (حجازي، ٢٠٠٤).

٦- الإحتيال في تحويل الأموال الالكتروني:

يعتبر الإحتيال في المعلومات في مجال أنظمة تحويل الأموال الالكتروني أحد أهم وأخطر جرائم الإحتيال في القطاع المصرفي، والذي يشمل أشكالاً متنوعة من الإحتيال يسهم بها الكمبيوتر الى حد كبير، مثل الإعتماد على الكمبيوتر لإنشاء ضمانات وهمية للقروض والتلاعب داخل البنك (عبدالجبوري، ٢٠١٤)، وقد ذكرت المادة ٦ من قانون ٢٧ المنشور في الجريدة الرسمية الأردنية لسنة ٢٠١٥ أنه "يعاقب كل من حصل قصداً دون تصريح عن طريق الشبكة المعلوماتية أو اي نظام معلومات على بيانات أو معلومات تتعلق بطاقات الائتمان أو بالبيانات أو بالمعلومات التى تستخدم في تقنية المعاملات المالية أو المصرفية الالكترونية بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٢٠٠٠) الفي دينار".

خصائص المجرم الالكتروني:

المجرم هو شخص طبيعي من مبدأ أن الناس تولد بيولوجياً سواسية، لديه المقدرة على تشغيل الكمبيوتر و تجربته وإستخدامه، والمقدرة نفسها أيضاً على إرتكاب الجرائم المتعلقة بإستخدامه، وبالتالي فإن خصائص المجرم الالكتروني متشابهة مع خصائص المجرم ككل، وتتمثل خصائص المجرم الالكتروني فيما يلي (لعفيفي، ٢٠١٣):

١. المجرم الالكتروني إنسان اجتماعي:

المجرم الالكتروني هو فئة نادرة من نوعها في عالم الإجرام، فهذا المجرم هو شخص غير عنيف على عكس المجرمين التقليديين. كل ما يمتلكه ذكاءٌ حاد يساعده على التكيف مع أفراد المجتمع، ويجعله يرتكب جريمته بهدوء دون أي عنف ومن ثم يرويها ويمحو آثارها بسهولة. وقد يكون المجرم الالكتروني إنساناً طبيعي للحظة ومجرم في لحظة أخرى، وربما أن أكثر الأمور التي تدفع الشخص لهذا التحول وإرتكاب جريمته هو الإنتقام من صاحب العمل لفصله من وظيفته، أو كمحأولة لإظهار قدرته ومهاراته في إختراق المواقع الالكترونية، وفي بعض الأحيان تكون الأسباب بدافع التسلية أو جمع الأموال من خلال النصب.

٢. المجرم الالكتروني مجرم ذكي ومتخصص:

مرتكب الجريمة الالكترونية هو مجرم ذكي بل هو حاد الذكاء، وذكاؤه يفوق ذكاء المجرم التقليدي بمراحل، فالمجرم التقليدي قد يترك أثرًا يؤدي الى اكتشافه، أما المجرم الالكتروني فمن النادر جدًّا أن يترك أي دليل يؤدي الى التعرف على شخصيته خاصة المتمرسون ذوي الخبرة منهم، وتختلف الجريمة حسب خبراتهم: فأصحاب الخبرات المحدودة منهم لا تتعدى جرائمهم الإتلاف أو نسخ البيانات والبرامج، أما أصحاب الخبرة منهم تكون جرائمهم أشد خطرًا من ذلك: مثل اختراق الأجهزة، أو جريمة التجسس الالكتروني، أو زرع الفيروسات، أو سرقة الأموال . وتبين من خلال الكثير من القضايا أن المجرمين الالكترونيين هم مجرمون متخصصون.

أركان الجريمة الالكترونية:

سوف نتناول في هذا الجزء الأركان الثلاثة للجريمة بصفة عامة؛ وذلك كي نتعرف أوجه توافقها وأوجه اختلافها مع الجريمة محل البحث، وهذه الأركان هي: الركن المادي، والركن المعنوي، والركن الشرعي.

١- الركن الشرعي:

ويقصد بالركن الشرعي "السند القانوني لتجريم الفعل وذلك عملًا بالمبدأ الذي ينص على أنه: "لا جريمة ولا عقوبة الا بنص"، وبناءً على هذا المبدأ فإنه من غير الممكن للقاضي الجزائي الإجتهاد بأي حال من الأحوال، فلا يجوز له القياس في التجريم، والجرائم الالكترونية أمر مستجد على المجتمعات، ولم يكن من السهل على المشرع أن يضع القوانين الخاصة بها، وعلى الرغم من ذلك قامت بعض الدول بوضع قوانين لمثل تلك الجرائم، وتعد دولة السويد أول دولة تصدت لهذا الأمر، حيث أصدرت قانون البيانات في عام ٩٧٣، ثم قامت الولايات المتحدة الأمريكية بسنِّ قانون لحماية أنظمة الحاسب الالي بين عاميْ (١٩٧٦-١٩٨٥)، ثم تبعتها فرنسا إذْ قامت في عام ١٩٨٨ بتحديث قوانينها الجنائية لتتناسب مع ما استُحدث من جرائم، أما على صعيد الدول العربية فقد قامت بعضها بسن بعض القوانين في هذا المجال: نذكر منها المملكة العربية السعودية التي أصدرت في العام ٢٠٠٧ نظامًا للتعاملات الالكترونية ونظامًا آخر لمكافحة الجرائم المعلوماتية، وكذلك دولة الإمارات العربية المتحدة التي أصدرت القانون الإتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات (المضحكي، ٢٠١٤) ، وفي الأردن فإن هناك إهتماماً كبير بقانون التجارة الالكترونية فقد تم تعديل القانون الصادر في ٢٠١٥ في سنة ،٢٠١٩ والذي ينص ضمن بنوده على ضرورة محاسبة المجرم الالكتروني.

٢- الركن المادي:

نصت المادة (٢٨) من قانون العقوبات العراقي على أن: (السلوك الإجرامي بارتكاب فعل من الأفعال الإجرامية أو الامتناع عن فعل أمر يوجبه القانون)، وبالتالي تثبت الجريمة في حالتين: الأولى ارتكاب فعل يجرمه القانون، والثانية الامتناع عن فعل يوجبه القانون، ولا ينطبق ذلك على ما يحدث في ذهن الإنسان لأنه لا يدخل في حالة التجريم، و يختلف العنصر المادي من حالة الى أخرى اعتمادًا على التصنيف الذي هو الفعل، وبالتالي لا يمكن حصره في جريمة المعلومات بموجب تعديل واحد: فقد يتخذ الحادث شكل التشهير أو التهديد أو التحريض باستخدام الوسائل الالكترونية، وهذا لا يسبب إشكالا؛ إذْ تنطبق عليه أحكام قانون العقوبات الخاص بهذه السلوكيات التقليدية، ولكن هناك أنواع من السلوك تتطلب التمييز بينها وبين سابقتها (التقليدية)، وهذا يستدعي إجراء تشريعات (غايب، ٢٠١١).

أ- السلوك الاجرامي:

السلوك الإجرامي طبقًا لما حدده القانون: هو النشاط البدني الخارجي للجاني لتحقيق النتيجة الجنائية التي يعاقب عليها القانون، وهو أمر ضروري لكل جريمة، ولا يمكن للمشرع الجنائي أن يحدد العقوبة قبل تحديد النشاط البدني الذي يشكل جرماً (المجالي، ٢٠٠٥).

فالجريمة تبدأ بفكرة في ذهن الجاني، وهذا أمر لا يعاقب عليه القانون ما دامت حبيسة في ذهن الجاني ولم يعبر عنها بأفعال مادية، أما إذا تحولت هذه الفكرة الى واقع مادي بأن نتج عنها أعمال أو أنشطة أو سلوكيات مادية ملموسة هنا يخضع الجاني للمساءلة القانونية ويستحق العقوبة (سرور، ١٩٧٤).

بشكل عام، وسيلة الجريمة هي الجريمة التي يستخدمها الجاني لتنفيذ مشروعه الإجرامي. وقد تضمن قانون منع الإرهاب الأردني الوسائل الالكترونية في المادة ٣ (هـ)، لكن قانون مكافحة الإرهاب لم ينص على هذه الوسائل المتعلقة بالجرائم السيبرانية التي يرتكبها الجاني ويقوم بتنفيذها بإستخدام الوسائل الالكترونية المنصوص عليها في المادة (٣) من الفقرة (هـ) من قانون منع الإرهاب، والتي يتم إرتكابها بهدف تعريض الأردنيين وممتلكاتهم لخطر الإرهاب والعداء أو القيام بأعمال إنتقامية ضدهم (مخلف، ٢٠١٧).

ب- النتيجة الجرمية:

النتيجة الجنائية هي التغير الذي يحدثه السلوك الإجرامي في العالم الخارجي وينال مصلحة أو حقاً قدر الشارع جدارته بالحماية الجنائية، إنه أحد عناصر الركن المادي والفقه الجنائي، الذي يقدم دليلًا على النتيجة الجنائية، وله مدلولان: مدلول مادي، ومدلول قانوني (المجالي، ٢٠٠٥).

ومن حيث الأهمية المادية فإن النتيجة الإجرامية تظهر بسبب السلوك المحظور وتؤدي الى تغير الوضع: إذْ أن الوضع قبل وقوع الفعل كان في صورة معينة، وبعد ارتكاب الجريمة تغير هذا الوضع، فالتغيير الذي حدث في الواقع المحيط لمرتكب الجريمة هو نتيجة الجريمة التي ارتكبها، على سبيل المثال: كان ضحية القتل على قيد الحياة قبل إطلاق الرصاص، ثم مات بعد إطلاق النار عليه. أو كان الضحية يمتلك مالا قبل عملية السرقة، ثم فقد ماله بعد السرقة. والنتيجة القانونية للجرم هي الاعتداء على حق الإنسان في الحياة في حالة القتل، والاعتداء على حقوق الملكية في حالة السرقة (مخلف، ٢٠١٧).

ج- علاقة السببية:

لا بد أن تكون هناك علاقة سببية بين سلوك الجاني ونتائج تصرفه: أي أن يكون سلوك الجاني هو الذي أدى الى النتيجة الجنائية على سبيل المثال: في جريمة القتل لا بد أن يكون سبب وفاة الضحية سلوك الجاني الإجرامي، ويمكن تطبيق القواعد العامة نفسها المطبقة على الجرائم العادية على الجرائم الالكترونية فيما يتعلق بالعلاقة السببية إن وجدت، على سبيل المثال: في جريمة سرقة المعلومات، يتم اختلاس المعلومات عن طريق النشاط البدني للجاني، سواء من خلال تشغيل الجهاز للحصول على المعلومات أو الحصول على البرامج أو بقصد التسبب في الحاق الضر أو إحداث التلف، أو تشغيل الجهاز لإساءة استخدام المعلومات التي تم الحصول عليها عن طريق الحصول على النتيجة دون الحاجة الى استخدام العنف لاستخراج الشيء الذي يريده، هنا تتحقق العلاقة السببية بين نشاطه البدني والنتيجة الإجرامية (قشقوش، ١٩٩٢).

٣- الركن المعنوي:

الجريمة ليست مجرد كيان مادي بحت يقوم على الفعل وتبعاته، بل هي أيضًا كيان نفسي. إن مادة الجريمة لا تخلق مسؤولية واحدة. وإذا كان هذا المبدأ ينطبق على الجرائم بشكل عام فإنه أيضًا ينطبق على جرائم المعلومات، وعملًا بهذا المبدأ فلكي يمكن تطبيق العقوبة على الجاني لا بد أن يكون شخصًا يتحمل المسؤولية. (مادة ٦٠ ومادة ٦١ من قانون العقوبات العراقي)، وبناءً على ذلك لا تنطبق العقوبة على أولئك الذين يخضعون لقوانين الإكراه (٦٢)، والضرورة (٦٣) والقصر(٦٤)، أو أولئك الذين ليسوا على علم بها. الركن المعنوي بشكل عام هو عبارة عن صلة بين الصورة المادية للجريمة وشخصية الجاني، وجوهر هذه العلاقة قوة الإرادة؛ ومن ثم هي ذات طبيعة نفسية (حسني، ١٩٨٨) ، ومن أنواع الركن المعنوي ما يلي:

أ- الجريمة المعلوماتية كجريمة عمدية:

تعتبر جريمة إتلاف المال المعلوماتي في ركنها المعنوي من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام الذي يقوم بتوافر العلم والإرادة، ويتوفر القصد الجنائي بأن يكون الجاني على علم بأن إقدامه على ارتكاب فعله يعد اعتداءً على ممتلكات الغير أو أنه يلحق الضرر بهم (الجرائم المرتبطة بتكنولوجيا المعلومات، 7o9o9.blogspot.com).

وقد نصت على ذلك المادة ٤٦٢-٤ من قانون العقوبات الفرنسي القديم، ولكن المشرع عاد ونص على مضمون ذات النص في المادة ٣/٣٢٣ من قانون العقوبات الجديد، وكذلك المواد ٠٤،٠٣، ٠٨ من الإتفاقية الدولية للإجرام المعلوماتي (بوزيدي، ٢٠١٧).

أما المشرع الجزائري فنص على ذلك في أحكام المادة ٣٩٤ من قانون العقوبات الخاصة بجرائم جرائم الإعتداء المتعمد على البيانات داخل نظام المعلومات والتي تنص على أن " تُفرض عقوبة السجن من ستة أشهر الى ثلاث سنوات وغرامة تتراوح بين (50.000 و 200.000 د.ج) المضمنة فيه". وبالنظر الى هذه الجريمة نجد أن لها صورتين: الصورة الأولى هي الهجمات المتعمدة على البيانات داخل النظام، و الصورة الثانية هي الضرر المتعمد للبيانات خارج النظام. وتنعكس الهجمات المتعمدة على البيانات داخل النظام في أحد الأعمال الثلاثة التالية: الإدخال، المحو، التعديل (سوير، ٢٠١١).

ب- الجريمة المعلوماتية كجريمة غير عمدية:

بموجب أحكام المادة ٣٥ من قانون العقوبات العراقي، لا تكون الجريمة متعمدة إذا تحققت النتيجة الجنائية بسبب خطأ مرتكبها، سواء كان هذا الخطأ هو الإهمال أو القسوة أو عدم الإهتمام أو عدم التقيد أو عدم الامتثال للقوانين واللوائح والأوامر بشكل عام؛ ففي مثل تلك الحالات إذا نتج عنها جريمة فإنه تكون غير متعمدة، ومن الممكن أن تتخيل الجريمة المعلوماتية وفقًا للمثال التالي: إذا كان المتهم يعتمد على المهارة في تجنب المتاعب والمشاكل التي تسببها الفيروسات، وهذا أدى الى تدمير الدوائر التي يعمل فيها أو تسبب في تلف بعض البرمجيات بسبب الإفراط في استخدام جهاز الكمبيوتر أو نقص المهرة في التعامل معه، فإن مسؤوليته هنا تكون غير مقصودة، وكذلك بالنسبة لأولئك الذين يستخدمون الأقراص المرنة من تلقاء أنفسهم قبل أن يتأكدوا من أنها خالية من الفيروسات في أجهزة الدائرة، فإذا تسببت هذه الأقراص في نقل الفيروسات الى هذه الأجهزة أو أدت الى تدمير بعض المكونات، أو غيرها من أوجه الضرر فإن ذلك لا يمكن وصفه بالجريمة. والواقع أن جرائم المعلوماتية قد تخرج عن نطاق التجريم لأن مرتكبها قد يكون واقعًا تحت الخوف من انتهاك قواعد القانون الإداري المحصنة ضد مبدأ الشرعية الجنائية أو الخوف من مخالفة لوائح وتعليمات المؤسسات أو الهيئات التي يعمل بها. ومع ذلك، فإن هذه الإجراءات قد تشكل جرائم جنائية وإدارية في ذلك، وهذا هو ما يثير المسؤولية المدنية إذا حققت الشروط الصحيحة واتخذت إجراءً ضارًا بالمؤسسة: مثل الإستيلاء على أموال المستثمرين وحرمان المؤسسة من الاستفادة من الأرباح التي كانت ستعود عليهم من توظيفها (غايب، ٢٠١١).

المبحث الثاني: التحقيق الجنائي في القانون الدولي العام

إن التطور الهائل لثورة الإتصالات والوسائل الالكترونية المتقدمة تركت أثرها في حياتنا، فقد نتج عنها جرائم تميزت عن الجريمة التقليدية من حيث طبيعة الجناة ومكان الجريمة والوسائل المستخدمة في تنفيذها، أُطلق عليها الجرائم الالكترونية. وبسبب عدم قدرة القوانين السابقة على التعامل مع تلك الجرائم الالكترونية كان لابد من استحداث قوانين جديدة لمواجهتها. وقد يتطلب تطبيق هذه القوانين أيضًا استخدام وسائل تكنولوجية متقدمة بحيث تبدو الجريمة وكأنها مادة ملموسة (إبراهيمي، ٢٠١٨).

مفهوم التحقيق الجنائي:

في اللغة يُقال حق الأمر يحقه حقًّا وأحقه: كان منه على يقين، ويقال إن فلانا حقق أمرًا: أي أنه أدرك حقيقة الأمر وهو تجريده من الوهم (عاشور، ٢٠١٠).

ويعرف التحقيق الجنائي بأنه مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها، ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم الى المحاكمة (ناصر، بدون سنة نشر).

صفات المحقق الجنائي:

المحقق الجنائي يبحث عن حقيقة العدالة بهدف اكتشاف الجريمة وتحديد هوية المشتبه به وتأكيده من خلال السعي لجمع الأدلة. ولا يمكن للمحقق أن يسود في هذا الصراع ما لم يكن لديه بعض الصفات منها: (عاشور، ٢٠١٠) و (البلوي، ٢٠٠٩) و (السرياني، ٢٠٠٥)

١- **الإيمان برسالته:** المحقق صاحب رسالة سامية تتمثل في الكشف عن الجريمة، وتقديم مرتكبها الى المحاكمة، وقبل كل شيء يجب أن يتخلص المحقق من أية أهواء شخصية أو أفكار مسبقة، وأن يلتزم الحياد والنزاهة، وتنص المادة ١٤٧ على أنه "يجب أن يكون المحقق مؤمناً برسالته في استظهار الحقيقة، واتخاذ كل الوسائل الكاشفة عنها، وأن يعتقد أن الوصول الى الحقيقة وتحقيق العدالة هما هدفه وغايته المنشودة".

٢- **قوة الملاحظة:** وهي معرفة سريعة ومحددة بتفاصيل الأشياء التي تندرج تحت واحدة من الحواس يمكن تطويرها على وجه اليقين، وتُجرى العديد من الاختبارات لإظهارها؛ لذلك فهو يدرك كل ما يراه ويدور حوله، ولا يترك أي شيء يمر دون أن يتوقف عنده بالتأمل والتدقيق،الأمر الذي يتطلب يقظة شديدة.

٣- **قوة الذاكرة:** هي قدرة المحقق على الاحتفاظ بالمعلومات والملاحظات واسترجاعها في ذهنه عند مراجعة ما هو مشابه لها أو مرتبط بها، وتُعد من أهم الصفات التي يجب أن يتمتع بها المحقق لأنها تسهل عمل المحقق وتضيء الطريقة التي يمكن من خلالها تحديد هوية المتهم. فالمحقق الناجح هو الذي يعتمد على قوة ذاكرته، وإذا كانت قوة الملاحظة هي وسيلة لجمع المعلومات، فإن قوة الذاكرة هي التي تضع هذه المعلومات موضع التنفيذ.

٤- **الدقة والترتيب:** يجب أن يكون عمل المحقق الجنائي مبنيًّا على الدقة الشديدة والترتيب المنطقي في جميع مراحل التحقيق، وتتطلب الدقة من المحقق أن يطلب حجز مكان الحادث ومنع أي شخص من الاقتراب منه حتى ينتهي التحقيق في الحادث؛ وذلك للحفاظ على الآثار خوفًا من إزالتها وطمسها. كما يجب أن يُراعي ترتيب وتسلسل التحقيق بحيث يكون متماسكًا وغير قابل للفصل وغير قابل للكسر.

٥- **السرعة في التصرف والإنجاز:** التصرف السريع أحد أهم مظاهر النشاط العملي للمحقق: مثل سرعة الانتقال الى مكان الحادث فور إخطاره، حيث يساعد ذلك في الحفاظ على معالم مكان وقوع الجريمة وسماع أقوال الضحية التي أصيبت بجروح خطيرة قبل وفاته وفي القبض على الجاني قبل مغادرة مسرح الجريمة. لكن عليه الا يكون متسرعًا بشكل قد تؤدي به الى ارتكاب أخطاء يصعب تجنبها وتصحيحها لاحقًا.

٦- **العدالة والحياد:** يجب أن يكون المحقق عادلاً والا يتعجل في إصدار أحكامه فالمتهم بريء حتى تثبت إدانته بأمر من المحكمة. كما يجب أن يعتذر عن التحقيق إذا وجد أن أحد أطراف القضية يرتبط به بأي علاقة من العلاقات.

٧- **الشجاعة:** غالبًا ما يتعامل المحقق مع أشخاص خطرين، الأمر الذي يتطلب منه الشجاعة كي يتمكن من أداء عمله على أكمل وجه، لكن ينبغي له التعامل مع الأمر من خلال خطة مدروسة، وأن يراعي الحذر في تصرفاته.

٨- **الهدوء والصبر:**، قد يلاحظ المحقق بعض السلوكيات غير العادية للضحية أو المتهم أو الشاهد أثناء التحقيق: مثل الاضطراب، والتأتأة، والصمت المطلق، والتوتر العصبي، الخ. وهذه السلوكيات غير المعتادة تتطلب من المحقق أن يكون قادرًا على التحكم في أعصابه، وأن يتمتع بالهدوء والصبر.

أقسام التحقيق الجنائي:

ينقسم التحقيق الجنائي الى قسمين رئيسيين (الترزي، ٢٠١٧):

أ- التحقيق الجنائي العملي:

هو جميع إجراءات التحقيق الجنائي التي يقوم بها المحقق الجنائي وقت ارتكاب الجريمة، حتى يتمكن من معرفة الحقيقة بناءً على الخبرة العملية التي توصل اليها المحققون في التحقيق في العديد من القضايا المهمة. قد يتم إجراء هذا التحقيق من قِبل المدعين العامين أو قضاة التحقيق أو أي شخص آخر مكلف به حسب القانون لبدء بعض أو كل الإجراءات المتعلقة بالتحقيق: مثل ضابط المراقبة (الذي لديه شهادة تحقيق من النيابة) (عاشور، ٢٠١٠).

فقد نصت المادة (٥٥) من قانون الإجراءات الجنائية الفلسطيني رقم (٣) لسنة ٢٠٠١ على ما يلي:

١. تختص النيابة العامة دون غيرها بالتحقيق في الجرائم والتصرف فيها.

٢. للنائب العام أو وكيل النيابة العامة المختص تفويض أحد أعضاء الضبط القضائي المختص بالقيام بأي عمل من أعمال التحقيق في دعوى محددة، وذلك عدا استجواب المتهم في مواد الجنايات.

٣. لا يجوز أن يكون التفويض عاماً.

٤. يتمتع المفوض له في حدود تفويضه بجميع السلطات المخوَّلة لوكيل النيابة.

كما نصت المادة ٩٦ من ذات القانون على أنه: "يتولى وكيل النيابة استجواب المتهم في الجنايات جميعها والجنح التي يرى استجوابه فيها".

ب- التحقيق الفني الجنائي:

إن القاضي له الحرية في تكوين عقيدته في تقدير الأدلة وقيمتها الجنائية، وبالتالي فإن المسالة هي سلطة تقديرية للقاضي فله أن يقتنع بأن شخصًا ما هو المشتبه به الفعلي أو لا، لأن شهادة الشهود تحتمل الحقيقة أو الكذب، لكثير من الاعتبارات: منها خوف الشاهد من المجرم أو الخوف من أهل المجرم والمشاكل التي يمكن حدوثها بعد ذلك؛ وبالتالي يحتاج الى إجراءات علمية: مثل رفع الآثار التي خلَّفها المجرم ووصفها وحجزها ثم فحصها (عاشور،٢٠١٠).

العناصر الأساسية للتحقيق الجرائم المعلوماتية:

تتمثل هذه العناصر في الآتي: (الترزي، ٢٠١٧)

١- تحديد وقت ومكان ارتكاب الجريمة المعلوماتية:

ينتج عن الجريمة الالكترونية العديد من المشكلات، على سبيل المثال: إذا ارتكب المتهم جريمةً في بلد ما من خلال اختراق حساب مصرفي في بلد آخر، أين ومتى يتم التحقيق الجنائي للجريمة الالكترونية؟، إن المشكلة قد تتمثل في وقت ارتكاب الجريمة: هل يتم الاعتماد على توقيت الجريمة في بلد المتهم أو توقيت البنك المسروق؟ وكذلك تظهر مشكلة أخرى من حيث مكان وقوع الجريمة.

٢- إظهار الجانب المادي للجريمة المعلوماتية:

يتطلب النشاط أو السلوك الجسدي في الجرائم الالكترونية معرفة السلوك المادي الذي يتبعه الجاني لارتكاب جريمة المعلومات، ويتم ذلك من خلال معالجة الكمبيوتر وتنزيل البرامج، وعلى الرغم من أن الإعداد يعد عملاً تحضيريًا في الجرائم التقليدية، فإن إطلاق الفيروسات وتنزيل البرامج يمثل جريمة في حد ذاتها.

٣- عرض الزاوية الأخلاقية للجريمة الالكترونية:

وهذا يرتبط بالحالة النفسية وإرادة الجاني، والتي تربط بين مدى خطورة الجريمة وإقدامه على ارتكابها ولابد من الكشف العلني عن الضمانات اللازمة لتوفير العدالة، وهذا يفيد في تحقيق الثقة في قلب المتهم من جانب، كما أنه يُعد حماية للقاضي من جانب آخر. وعلى هذا يجوز لأي فرد من الجمهور حضور المحاكمة في مرحلة التحقيق في التناسب المحدود بالخصوم في القضية الأردنية.

أهم معوقات الإثبات بالإعتماد على الأدلة الرقمية في الجرائم المعلوماتية:

من أهم المعوقات التي تواجه التحقيق الجنائي بالاعتماد على الأدلة الرقمية في الجرائم المعلوماتية (القحطاني، ٢٠١٤):

١- إخفاء الدليل: إذا كانت أنظمة التحكم ضعيفة، فإنها تمكن مرتكبي الجرائم السيبرانية من التسلل الى الدوافع والذبذبات الالكترونية التي يتم من خلالها تسجيل المعلومات والبيانات والتلاعب بها من أجل إحداث تغييرات فيها، ثم معالجة نظام الكمبيوتر بحيث يصعب إثبات حالة التسلل والدخول، وبالتالي يمكن لمرتكبي الجرائم السيبرانية إخفاء جرائمهم وطمس آثارها في وقت قياسي قبل وصولها الى سلطة التحقيق.

٢- أوجه القصور في تحديد هوية الجاني من خلال الأدلة الرقمية: الجريمة المعلوماتية نادرًا ما يقوم مرتكبوها بإستخدام العنف، ولكن يتم التعامل معها من خلال إدخال معلومات كاذبة أو محظورة داخل البرامج أو التشويه أو تعديل البيانات أو المعلومات المخزنة بالفعل في الكمبيوتر أو نقل البرامج الضارة أو التجسس على البيانات والمعلومات المخزنة، وما الى ذلك. وإذا تم اكتشاف هذه الأفعال فقد لا يوجد دليل على اتصال شخص معين بالجريمة المرتكَبَة وذلك نظرًا لصعوبة تتبع الآثار الرقمية ومراجعة وفحص البيانات والمعلومات الهائلة التي يتم إدراجها في النظم.

٣- عرقلة الوصول الى الدليل: في بعض الحالات، يضع الجاني عقباتٍ تقنيَّة لمنع اكتشاف جريمته: كاستخدام تقنيات التشفير أو كلمات المرور، فهؤلاء الجناة هم مجرمون محترفون، يستطيعون عند ارتكابهم جرائم الكترونية أن يحيطوا أنفسهم بتدابير أمنية وقائية تجعل من الصعب اكتشافهم.

٤- عدم وجود دليل مرئي لجريمة الإنترنت التي تقع على مختلف العمليات الالكترونية: من الصعب العثور على دليل مادي ضد الجناة؛ لأن معظم المعلومات والبيانات التي يتم تداولها من خلال أجهزة الكمبيوتر وشبكات الاتصال تكون في شكل رموز ونبضات مخزنة على وسائط التخزين الممغنطة بحيث لا يمكن للبشر قراءتها أو إدراكها الا من خلال أجهزة الكمبيوتر هذه.

٥- صعوبة فهم الأدلة التي تم الحصول عليها من الجريمة الالكترونية (الوسائل الالكترونية): قد يتم تضمين الدليل الرقمي بعضًا من المسائل الفنية التي لا يمكن فهمها الا من قِبل خبير متخصص، فهناك العديد من العمليات الالية للبيانات التي قد يتم إجراؤها بواسطة الكمبيوتر تلقائيًا دون أن تترك وراءها الآثار المادية الملموسة التي تكشف عنها، ويصبح فهم الأدلة لإثبات الجريمة السيبرانية للجرائم الالكترونية أكثر صعوبة في تلك الحالات التي يكون فيها الكمبيوتر متصلاً بشبكة المعلومات العالمية.

٦- مشاكل إجراءات قبول الدليل الرقمي: الصعوبة لا تتمثل فقط في إثبات الجريمة السيبرانية عندما يتعذر الحصول على أدلة كافية لإثباتها، لكن هذه الصعوبة تمتد الى إجراءات الحصول على هذا الدليل؛ لأن المجرمين الذين يرتكبون جرائمهم بالوسائل الالكترونية الحديثة يتمتعون بالذكاء الحاد ومن الصعب أن يتركوا خلفهم أدلة يمكن أن تدينهم.

المبحث الثالث: التعاون الدولي في مجال الأمن السيبراني

إن الهدف الرئيسي من إتفاقية التعاون الدولي في مجال الأمن السيبراني هو تعزيز التعاون الدول العربية في مجال مكافحة الجرائم السيبرانية، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة أرفادها ومجتمعاتها وتنص بعضاً من بنودها على ما يلي: (المركز العربي للبحوث القانونية والقضائية، ٢٠١٨).

المادة الثالثة عشرة:

"تتعاون الدول الاعضاء، مع الهيئات الدولية والإقليمية المتخصصة في قضايا حماية الفضاء السيبراني، لاسيما اللجان التابعة للامم المتحدة، والإتحاد الدولي للإتصالات، والآيكان (هيئة الإنترنت للأسماء والأرقام)، وجامعة الدول العربية، وهيئات الاتحاد الاوروبي، ومجموعة دول الكومنولث، ومنظمة التعاون والتنمية الاقتصادية، وأي هيئة دولية أخرى ذات اختصاص وصلة بمسائل الامن السيبراني".

المادة الرابعة عشرة:

"تتعاون الدول العربية الأعضاء، لحماية الفضاء السيبراني، والخدمات الالكترونية، في منع ومكافحة الجرائم السيبرانية، طبقا للقوانين والإجراءات الداخلية لكل دولة منها"، من خلال الآتي:

١. تبادل المعلومات المتعلّقة بأنشطة وجرائم الجماعات التي تنظّم الإعتداءات والهجمات على الأنظمة المعلوماتية والبُنى التحتية للإتصالات والمعلومات والمواقع الالكترونية. وتتبُّع مواقعها ووسائل إتصالاتها ودعاياتها المستخدمة.

٢. التحرّيات وتقديم المساعدة في مجال القبض على الهاربين من المتهمين أو المحكوم عليهم بجرائم سيبرانية وفقاً لقانون وأنظمة كل دولة.

٣. تبادل الخبرات والدراسات والبحوث وتوفير المساعدات الفنّية المُتاحة لإعداد برامج ودورات تدريبية مشتركة خاصة بكل دولة أو بين الدول المتعاقدة للعاملين في مجال مكافحة الجرائم السيبرانية لرفع مستوى أدائهم.

المادة الخامسة عشرة:

"على الدول الأعضاء، إنشاء هيئات خاصة، توكل اليها مهمة متابعة طوارئ الانترنت، وتبادل المعلومات، فيما يخص هذه الطوارئ، والرد عليها، ونشر المعلومات حولها، عبر مراكز الاستجابة لطوارئ الإنترنت".

نتائج الدراسة :

كشفت الدراسة أن الأجهزة الأمنية تواجه تحدياً كبيراً في إثبات الجريمة والآلة التقليدية، ويزداد صعوبة في الجريمة الالكترونية، حيث إن اكتشاف الجريمة الالكترونية أمر صعب للغاية، وحتى إن كان هناك إمكانية لاكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من التحديات، فالجريمة الالكترونية تتم في بيئة غير تقليدية، خارج إطار الواقع المادي الملموس المرئي، في متواجدة في بيئة الحاسوب والإنترنت، مما يشكل عائقٌ للسلطات الأمنية وأجهزة التحقيق والملاحقة في تحديد الأدلة الالكترونية؛ ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات غير مرئية تنساب عبر النظام والأجهزة المعلوماتية، مما يجعل أمر محو الدليل من قبل الفاعل أمرا في غاية السهولة. ومن أهم النتائج التي توصلت اليها الدراسة:

- تتسم الجريمة الالكترونية بصعوبة اكتشافها مقارنة بالجرائم التقليدية، ويكمن السبب في عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، كما إن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى لما أحدثته التكنولوجيا من تلاشي الحدود المكانية والزمنية، إذ أن الجريمة الالكترونية جريمة عابرة دولية.
- يعد إثبات هذه الجرائم من أهم التحديات التي تواجه الأجهزة الأمنية، مما يستلزم الكثير من الجهد والخبرة الفنية.
- هناك نقص في الخبرة الفنية والتقنية لدى الشرطة وجهات الإدعاء والقضاء، وهذا يشكل عائقا أساسياً أمام إثبات الجريمة الالكترونية، ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت، ونتيجة لنقص الخبرة والتدريب كثيراً ما تفشل الأجهزة الأمنية في تقدير أهمية الجريمة الالكترونية.
- قد تكون الجريمة الالكترونية جزأ من جريمة تقليدية، لا سيما في ظل ارتباط الناس بالوسائل التكنولوجية الحديثة التي بدأت تنتشر بشكل كبير وأهمها الحاسبات الآلية والهواتف الذكية، وقد تكون جريمة الكترونية مستقلة.
- تتسم الجرائم ذات الصلة بالتكنولوجيا ووسائلها، بسرعة تنفيذها، وحداثة أساليب ارتكابها، وسهولة إخفائها، ودقة وسرعة محو آثارها. لذا يجب أن يكون المحقق الجنائي على درجة كبيرة من المعرفة بالأنظمة التكنولوجية، وكيفية تشغيلها، وأساليب ارتكاب الجرائم من خلالها، مع إمكانية معرفة غموض هذه الجرائم و التصرف السريع بشأنها.

- إن علانية التحقيق في الجرائم الالكترونية من الأمور اللازمة لضمان توافر العدالة، فلا يقتصر فيها الأمر على طمأنة قلب المتهم، بل هي بذاتها حماية لأحكام القاضي من الشك أو الخضوع تحت التأثير، كما أنها تضمن الطمأنينة للجمهور على أن الإجراءات تسير في طرق صحيحة وطبيعية.

- من أهم المعوقات التي تواجه إثبات الجريمة الالكترونية هو صعوبة ظهور الدليل المادي، فالدليل المادي للجريمة الالكترونية يكون عن طريق ارتكاب الجريمة بواسطة أجهزة الحاسوب وتطبيقاته، حيث تتم الجريمة في بيئة لا علاقة لها بالأوراق أو المستندات، أو شبكة المعلومات الدولية، ويمكن للجاني العبث في بيانات الحاسب أو برامجه، في وقت قياسي قد يكون جزءا من الثانية.

المراجع:

المراجع العربية:

- ال ثنيان، ثنيان ناصر (٢٠١٢). اثبات الجريمة الالكترونية دراسة تاصيلية تطبيقية، رسالة ماجستير، قسم العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الامنية.
- إبراهيمي، جمال (٢٠١٨). التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراة، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو.
- الالفي، محمد محمد (بدون سنة نشر) الاحكام الموضوعية والانماط، ورقة عمل حول تشريعات مكافحة جرائم الارهاب الالكتروني.
- البداينة، ذياب (٢٠١٤). الجرائم الالكترونية: المفهوم والأسباب، الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية خلال الفترة من ٢-٢٠١٤/٩/٤، عمان.
- برهم، سامر، جراء نيوز، موقع إخباري أردني، https://www.garaanews.com، ٢٠٣٨ جريمة الكترونية في ٢٠١٨ في الاردن أبرزها جرائم جنسية!، تاريخ المشاهدة: ٩-٤-٢٠١٩ الساعة: ١,٠٠ .
- البلوي، سالم حامد علي (٢٠٠٩). التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، ص٢.
- بوابة باب الإخبارية، http://www.bab.com/node/22459، تاريخ المشاهدة: ٦-٩-٢٠١٩، الساعة: ٥:٠٠pm.
- بوالماين، نجيب (٢٠٠٨). الجريمة والمسالة السوسيولوجية دراسة بابعادها السوسيوثقافية والقانونية،رسالة دكتوراه، قسم علم الاجتماع والديموغرافيا، كلية العلوم الإنسانية والاجتماعية، جامعة منتوري قسنطينة.
- بوزيدي، مختارية (٢٠١٧). ماهية الجريمة الالكترونية، كتاب أعمال ملتقى اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، المنعقد في العاصمة الجزائر.
- بونعارة، ياسمينة (٢٠١٦). الجريمة الالكترونية، جامعة الأمير عبد القادر للعلوم الانسانية، قسنطينة، الجزائر، العدد <٣٨
- الترزي، نديم محمد حسن (٢٠١٧). سلطات النيابة العانة في الجرائم المعلوماتية (المعاينة – التفتيش)، مجلة الاندلس للعلوم الانسانية والاجتماعية، العدد١٣، المجلد١٥.
- الجرائم المرتبطة بتكنولوجيا المعلومات، 7o9o9.blogspot.com.
- الجمعات، أكرم محمود (٢٠١٠). العلاقة بين الجريمة التأديبية والجريمة الجنائية، دراسة مقارنة، رسالة ماجستير، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط للدراسات العليا.

- حجازي، عبد الفتاح بيومي (٢٠٠٤). حماية المستهلك من الغش التجاري والتقليد في عقود التجارة الالكترونية عبرالإنترنت، الندوة الثالثة لمكافحة الغش التجاري والتقليد في دول مجلس التعأون لدول الخليج العربية، الرياض.
- حجازي، محمد (٢٠٠٥). جرائم الحسابات والانترنت "الجرائم المعلوماتية"، المركز المصري للملكية الفكرية.
- الحسن، إحسان محمد (١٩٩٣) .علم الإجرام، دراسة تحليلية عن دور العوامل الاجتماعية في الجريمة، جامعة بغداد
- حسني، محمود نجيب (١٩٨٨). النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة دارالنهضة العربية، ط٣ .
- حسين، نادية شاكر (بدون سنة نشر). المخالفات المحاسبية وأثرها في تفشي ظاهرة الفساد المالي واالداري (دراسة محاسبية تحليلية)، مجلة النزاهة والشفافية للبحوث والدراسات، العدد السادس.
- سرور، أحمد (١٩٧٤). الوسيط في قانون العقوبات ، دار النهضة العربية، القاهرة.
- السرياني، عبد الله سعود محمد (٢٠٠٥). فعالية مهارات المحقق الجنائي في التحقيق في جرائم تزييف العملة "دراسة صحية على الضباط العاملين في اقسام مكافحة التزييف والتزوير بالامن العام، رسالة ماجستير، قيادة امنية، قسم العلوم الشرطية، كلية الدراسات العليا.
- سفيان، سوير (٢٠١١) جرائم المعلوماتية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد تلمسان.
- سورة الأعراف، الآية ٨٢.
- الشهراني، احمد سعيد مشبب (٢٠٠٨). مسرح الجريمة واهميته في كشف مرتكبها عن طريق الادلة المرفوعة منه، قسم الطبيعات الجنائية، الدبلوم العالي في علوم الادلة الجنائية، كلية علوم الادلة الجنائية، جامعة نايف العربية للعلوم الامنية.
- عاشور، محمد حمدان (٢٠١٠). أساليب التحقيق والبحث الجنائي، قسم المناهج، الشئون الاكادمية، اكادمية فلسطين للعلوم الامنية.
- عبد الجبوري، سامر سلمان (٢٠١٤). جريمة الاحتيال الالكتروني دراسة المقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين.
- عريم، عبدالجبار (١٩٧٠) نظريات علم الإجرام، دار المعارف، بغداد.
- عطاي، إبراهيم رمضان إبراهيم (٢٠١٥). الجريمة الالكترونية وسيلة مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، كلية الشريعة والقانون بطنطا، العدد ٣٠، الجزء ٢.
- العفيفي، يوسف خليل يوسف (٢٠١٣). الجرائم الالكترونية في التشريع الفلسطيني"دراسة تحليلية مقارنة"، قسم القانون العام، كلية الشريعة والقانون، الجامعة الاسلامية.
- غايب، محروس نصار (٢٠١١). الجريمة المعلوماتية، المعهد الاتقني، الانبار.

- القحطاني، عبدالله حسين ال حجراف (٢٠١٤). تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية دراسة تطبيقية على المحققين في هيئة التحقيق والإدعاء العام بمدينة الرياض، رسالة ماجستير، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية.
- قشقوش، هدى حامد (١٩٩٢). جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة.
- لجنة ملخصات الابحاث القضائية (١٤٣٦هـ) سلسلة ملخصات الابحاث القضائية من مكتبة المعهد العالي للقضاء، الجمعية العلمية القضائية السعودية، جامعة الامام محمد بن سعود الاسلامية.
- المجالي، نظام (٢٠٠٥). شرح قانون العقوبات القسم العام ،دار الثقافة للنشر و التوزيع ،عمان.
- مخلف، مصطفى سعد حمد (٢٠١٧). جريمة الارهاب عبر الوسائل الالكترونية "دراسة مقارنة بين التشريعين الاردني والعراقي"، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط.
- المركز العربي للبحوث القانونية والقضائية (٢٠١٨). الإتفاقية العربية لحماية الفضاء السيبراني بين الواقع والطموح، مجلس وزراء العدل العرب، جامعة الدول العربية.
- المضحكي، حنان ريحان مبارك، (٢٠١٤). الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط١.
- ناصر، مازن خلف (بدون سنة نشر). أصول التحقيق الجنائي، مجموعة محاضرات لطلبة المرحلة الرابعة، كلية الحقوق، الجامعة المستنصرية.

المراجع الأجنبية:

- Calling off cybercrime, https://sites.google.com/site/callingoffcybercrime/types-of-cyber-crime
- Choi, H., and Hanwoo. L., and Heejo L., and Hyogon., K (2007). Botnet Detection by Monitoring Group Activities in DNS Traffic, in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007).
- Dacey, R., & Kenneth, G (1997). Crime control and harassment of the innocent, Journal of Criminal Justice, Elsevier, vol. 25(4).
- http://www.aladalacenter.com/index.php/legal-encyclopedia/166-2009-11-13-22-00-30/1577-2009-09-30-12-34-03.
- Jain, N., and Vibhash., S (2014). Cyber Crime Changing Everything – an Empirical Study, International Journal of Computer Application, Vol.1, Issue 4.
- Kaur, N (2018). Introduction of Cyber Crime and Its Type, International Research Journal of Computer Science, Vol. 5, Issue 08.
- Longe, O., and Oneurine .N., and Frida.W and., Victor .M (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives, Journal of Information Technology Impact, Vol. 9, No. 3.