الجرائم الإلكترونية والتحديات القانونية في الإثبات والعقوبة

Cybercrimes and Legal Challenges in Evidence and Punishment.

المدرس الدكتور محمد سعد حمادة الخزاعي

جامعة القادسية/ كلية التربية

Assistant Professor Dr. Mohammed Saad Hamada Al-Khuza'i
University of Al-Qadisiyah / College of Education
Mohammad.Saad.hamada@qu.edu.iq

الملخص:

إن استغلال الجناة للتقدم التقني أدى لظهور الجرائم الإلكترونية التي لا تتقيد بالحدود الجغرافية ويتم اقترافها من خلال شبكة الإنترنت لتلحق الضرر بالمجني عليه أنيما كان، وهذه الجرائم المعقدة أثارت صعوبة إثباتها استناداً لخاصية الدليل الرقمي المترتب عنها وصعوبة اجراءات التحقيق فيها بالإضافة لعدم ناسب العقوبات المفروضة عليها، وقد حاولنا في هذا البحث توضيح الأحكام الناظمة لهذه الجرائم من خلال شرح مفهومها وخصائصها وأنواعها ودوافع اقترافها، ثم تطرقنا إلى الصعوبات التي تثور عند القيام بالتحري عنها وإثباتها، وخلصنا إلى فتقار القانون العراقي إلى أحكام خاصة تنظم هذه الجرائم.

الكلمات المفتاحية: الجريمة الإلكترونية، دليل رقمي، طبيعة قانونية، إثبات، العقوبة.

Abstract:

The exploitation of technological progress by perpetrators has led to the emergence of cybercrimes that are not bound by geographical borders and are committed over the Internet, harming the victim, regardless of their identity, These complex crimes are difficult to prove based on the resulting digital evidence, the difficulty of investigation procedures, and the inappropriateness of the penalties imposed on them. In this research, we have attempted to clarify the provisions regulating these crimes by explaining their concept, characteristics, types, and motives for committing them, we then addressed the difficulties that arise when investigating and proving them, and concluded that Iraqi law lacks specific provisions regulating these crimes.

Keyword: Cybercrime, digital evidence, legal nature, proof. Punishment.

المقدمة:

إن تقدم الجريمة مسايراً لتقدم الإنسان في عصره، ذلك أنه كلما تقدم الزمن ودواته المختلفة كلما تقدم الفعل الجرمي المرتكب ، فالمجرمون في سباق مع الفعل الجرمي، وقد قاد التطور التقني المذهل في هذا العصر إلى نشوء الجرائم الإلكترونية ذا الطبيعة المميزة والعابرة للحدود الدولية التي تذيب الفواصل الدولية وتنقل مسرح الجريمة بين عدة دول لحقيق الآثار المربة على الجريمة بشكل يثير دهشة رجال الحقيق فيقفون عاجزين أمام ذكاء وحنكة مجرم الفعل الإلكتروني الذي يتحلى بالإبداع التقني والمعرفة والدراية الكافية عن التقنية المعلوماتية والذي يتيح له فرصة مجرم الفعل الإلكتروني الذي يتحلى بالإبداع التقني والمعرفة والدراية الكافية عن التقنية المعلوماتية الذي يتيح له فرصة اقتراف فعل جرمي إلكتروني ذو آثار غير مرئية أو صريحة وواضحة وكأنه ينفذ جريمة دون أي آثار مادية تقود لصعوبة إثباتها حتى يتم إلقاء القبض عليه بموجبها وفرص عقوبة مناسبة له، ولهذا كان لا بد أمام مخاطر هذه الجريمة الكبيرة من الوقوف على الأحكام الناظمة لها.

إشكالية البحث:

إن طبيعة الجغرافية على الإنترنت والإمكانيات الكبيرة التي تتيحها الشبكة تؤدي لاقتراف جرائم إلكترونية تحلق الضرر بالعديد من المجني عليهم ولو كانوا موزعين بأكثر من دولة، هذا ما يستتبع نشوء العديد من الصعوبات في مواجهة هذه الجرائم، وهنا يثور التساؤل عن:

-ما العقبات التي تعترض رجال التحقيق في إثبات الجرائم الإلكترونية؟ وها استطاع المشرع العراقي مواجهتها بالعقوبات المناسبة؟

ويتفرع عن هذا التساؤل الأسئلة التالية:

-ما ماهية الجرائم الإلكترونية وخصائصها؟

-ما أنواع هذه الجرائم والدوافع التي تؤدي لارتكابها؟

-ما المعوقات التي تقف في سبيل إثبات الجرائم الإلكترونية والجزاء المفروض عليها؟

أهمية البحث:

يحظى هذا البحث بأهمية كبيرة كون إمكانية توضيح الإجراءات التي بموجبها يتم إثبات هذه الجريمة يحظى بأهمية كبيرة استناداً لخطورتها الجسيمة ذا الآثار المتعددة في العددي من الدول، وأمام قوة آثارها كان لا بد من معرفة الأسلوب المتبع في إثبات هذه الجرائم.

كما وأن العقاب على الجريمة الإلكترونية العالمية يتمتع بأهمية كبيرة في العصر الحديث الذي يشهد تطور متسارعاً في أساليب ارتكاب الجريمة والتفوق على أجهزة العدالة مما يستلزم تحديد العقوبة المناسبة بشكل يكرس قوة الردع.

أهداف البحث:

يهدف هذا البحث إلى:

-تسليط الضوء على ماهية الجرائم الإلكترونية وخصائصها.

-تحديد دوافع ارتكاب هذه الجرائم وأنواعها.

-توضيح الصعوبات التي تعترض طريق إثبات هذه الجرائم والعقوبة المفروضة عليها.

منهج البحث:

تم اتباع المنهج الوصفي لتوضيح الجانب المفاهيمي لهذه الجرائم من حيث تعريفها وخصائصها وأنواعها، كما وتم الاستعانة بالمنهج التحليلي من أجل تحليل الأحكام القانونية التي تنظم البحث.

هيكلية البحث:

من أجل معالجة البحث تم تقسيمه إلى مبحثين خصصنا المبحث الأول منه إلى الطبيعة القانونية للجرائم الإلكترونية، والمبحث الثاني وضحنا فيه التحديات الإجرائية المتعلقة بالجرائم الإلكترونية.

المبحث الأول: الطبيعة القانونية للجرائم الإلكترونية.

تعد الجرائم الإلكترونية صورة حديثة من الجرائم ذات الصبغة العالمية التي تتجاوز الحدود وينعكس أثرها بشكل مباشر على الكثير من المجني عليهم وفي أماكن متفرقة، ويتصف جناتها بصفات مخلفة ومتفردة عن مجرمي الجرائم التقليدية وقد ألغت المسافات بين الدول فتم ارتداء ثوب جديد لصورة الجرائم تفردت بكل مكوناتها وآثارها وخصائصها، يستند ارتكابها بشكل أساسي على شبكة الإنترنت وعلى شخص على خبرة كافية في التعامل معه، وهذا ما يفرض علينا ضرورة الغوص في أحكام هذه الجرائم وهذا ما سنوضحه من خلال تقسيم هذا المبحث لمطلبين نوضح في المطلب الأول ماهية الجرائم الإلكترونية وفي المطلب الثاني أنواع هذه الجرائم ودوافع ارتكابها وفق الآتي.

المطلب الأول: ماهية الجرائم الإلكترونية.

إن الجرائم الإلكترونية هي عبارة عن أفعال جريمة تقليدية بحلة جديدة لها وجود حقيقي ولكنه غير معين في المكان حيث تعد مثالاً واضحاً للعولمة كونها تنفذ كفعل جرمي عن بعد تم فيه إلغاء الحدود الجغرافية وانصهرت كافة الدول في بوقة واحدة جعل منها جريمة عالمية ذا آثار دولية، فطليعته وخصائصها تستلزم أن يتم التطرق إلى تعريفها في الفرع الأول ثن توضيح خصائصها المميزة في الفرع الثاني وفق الآتي:

الفرع الأول: تعريف الجريمة الإلكترونية.

باعتبار الجرائم الإلكترونية جرائم مستجدة بشكل عام نظراً لارتباطها الوثيق مع التطور التقني فقد كانت فعالة ووضع تعريف شامل لها مسألة يحوطها الشك والغموض ولم يتم الاتفاق على تعريف واحد، وقد تعددت تعريفات الفقه القانوني التي قدمها للفعل الجرمي الإلكتروني المرتكب، حيث تم تصنيفها لخمسة آراء فذهب البعض إلى تعريفها بكونها صورة من صور النشاط غير الشرعي المقترف عن طريق الحاسوب، معتمداً على أداة اقتراف الفعل الإلكتروني وهو الحاسب حتى يتم اعتبارها إلكترونية[1]، كما وعرف بكونها سلوك غير قانوني يتم توجيهه لنسخ أو تبديل أو حذف أو الوصول للمعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه مستنداً على كون محل الجريمة الإلكترونية يتمثل بالحاسب الآلي[2].

بينما ذهب البعض الآخر إلى تعريفها بكونها فعل غير شرعي يعتمد على معرفة الجاني التقنية بالمعلومات من أجل اقترافه والتحقيق فيه وملاحقة بشكل قضائي، أي أن هذا التعريف على معرفة الجاني بالتقنية بشك لعميق حتى يتم اقتراف الفعل الجرمي[3].

أما الرأي الراجح فقد استند على الأفعال ذات الطابع القانوني التي يتم اقترافها عن طريق الأدوات الإلكتروني من أجل الوصول للربح والمتعة، وهذا التعريف اعتمد على تحقيق الفاعل للربح.

بينما ذهب الاتجاه الخامس إلى كونها فعل أو امتناع عن فعل يمثل من مسألة العدول على الأموال المعنوية ينتج بشكل مباشر أو غير مباشر بناءً على تدخل التقنية الإلكترونية[4].

وقد ذهبت المنظمة الأوبية للتعاون والتنمية الاقتصادية إلى عريفها بأنها كل فعل أو امتناع يؤدي لعدوان على الأموال ذات الطابع المادي أو المعنوي ينتج بأسلوب مباشر أو غير مباشر عن استعمال التقنية الإلكترونية[5]، وهناك إجماع لدى معظم الفقهاء الفرنسيون على كون فكرة الغش الإلكتروني التي تساوي جريمة الحاسب الآلي مختلفة وليس الهدف مجرد وصف ولكنها بشكل عام يتم النظر لهذا المصلح بكونه مفهوم يتصل بعلم الإجرام، وهذا المفهوم يعد غامضاً نسبياً حيث يضم الكثير من المعاني حتى يتم تعيين مجموعة قانونية بشكل مباشر تطبق على صعيد القانون الجزائي[6].

وبالعودة للتعاريف السابقة يتبين لنا أن معظمها اتجه نحو وضع نطاق واسع لمفهوم الجرمية الإلكترونية لاسيما وأن هذا النطاق في حركة مستمرة دائمة من التقدم وبشكل سريع ويصعب اللحاق به ففي ظل فترة زمنية قصيرة ينشأ أنواع جديدة من الجرائم الإلكترونية المختلفة في النوع والفعل[7]، وإن وضع تعريف معين بالإطار الضيق من خلال تعيين أركان وعناصر الجريمة وتعيينها ثم ظهور أفعال بعد هذا يترتب عليها ضرر ولا تتوافر كافة أركان الفعل فسيكون هذا فرصة لإفلات الكثير من المرجمين من العقاب وسيتم تأطير سلطة القاضي وصلاحياته في نظر الفعل الجرمي والقيام بالأصول اللازمة لمواجهتها والكشف عنها والقبض على فاعليها، ولاسيما في ظل عدم إمكانية تطبيق نصوص ثانية كون هذا يخل بمبدأ شرعية الأفعال الجرمية والعقاب[8].

وبعد هذا العرض يمكننا أن نعرف الجريمة الإلكترونية بكونها كل سلوك إجرامي يركب بأسلوب إيجابي أو سلبي يم فيه استعمال التقنية المطورة بشكل مباشر أو غير مباشر كأداة أو هدف من أجل تنفيذ الفعل الإجرامي العمدي في التقنية الإلكترونية، أي أن الجريمة الإلكترونية كون أحد سببين إما تكون المعلومات أداة للتحايل والخداع والعدوان، وأن تكون محل من أجل العدوان وبالتالي فاقتراف الأفعال الجرمية الإلكترونية يتطلب من الجاني استعمال أداة إلكترونية من أجل اقتراف الفعل الجرمي من خلالها، وقد تنوع هذه الأدوات الي تعمل على قراءة شيفرات وبيانات الشبكة الإلكترونية لجعلها لغة صريحة لمستعملي هذه الأجهزة[9].

الفرع الثاني: خصائص الجرائم الإلكترونية.

تتميز الجريمة الإلكترونية بالعديد من الصفات الي تفردها عن الكثير من الجرائم الأخرى، ولعل السمة المميزة لها هو:

– كونها جريمة عابرة للحدود : ذلك أن الصلة المستلزمة بين ضرورة اتصال الشبكة الإنترنت بالحواسيب حتى نشأ الجريمة المعلوماتية قاد بشكل طبيعي إلى أن يكون الجاني في بلد والمجني عليه في بلد آخر في غالبية الجرائم، وهذه السمة المتفردة لها تتطلب أن يتوفر تنظيم قانوني لدى كافة الدول يقضي بضرورة التعاون الدولي حتى يتم إيقاف انتشار مثل هذه الجرائم ولاسيما أن هذه الصفة سوف يتبعها إشكالية تحديد الدولة المختصة في عقاب مركب الفعل، ذلك أن طبيعة الجغرافية على الإنترنت مع المقومات المتاحة للشبكة تقود ليتم اقتراف النشاط الجرمي لدى أكثر من دولة وقد تكون أدلة الإثبات على هذا النشاط الجرمي مشتتة بين عدة دول ، فالإنترنت لا يعد ملكاً لدولة معينة ولا خاضع لسيطرتها وبالتالي

سوف تتنوع القوانين الجزائية التي قد تحكم هذه الشبكة بتنوع الدول المتصلة بها [10].

-صعوبة اكتشاف وإثبات الفعل الإلكتروني المرتكب: فهذه الأفعال الجرمية تتميز بكونها لا تخلف آثار مادية واضحة من السهل ضبطه كما هو الحال في الجرائم التقليدية بل على العكس من ذلك فإنها آثارها تكون غير مرئية ومن الصعوبة حتى اكتشافها[11]، ويم استعمال النبضة الإلكترونية في اقترافها حيث تتم خلال ثانية واحدة والجاني يعمل على تشتيت وتخريب الدليل باستخدامه فقط وبكل هدوء ودون أن ينتج عن هذا أي فوضى خلافاً للكثير من الجرائم المعروفة[12].

-خصوصية مجرم المعلومات: غالباً ما يكون مرتكب الفعل الإلكتروني ذو خصائص مميزة حيث يكون ذو مستوى علمي متقدم ومختص ولديه خبرة كافية في إطار تقنية المعلومات، حيث يصنف مجرمو الأفعال الجرمية الإلكترونية بالمخترقون كالهاكرز الذي يسعى جاهداً لاستعمال حسابات الآخرين بشكل غير مشروع ويكون شخص فضولي وذو خبرة عميقة في الحاسب الآلي[13]، أو المحترفون وهم المجرمون الأكثر خطورة حيث يكون هدفهم تحقيق الربح بأسلوب غير قانوني أو مادي، وإنما تنحصر أهدافهم بالناقم والثأر كالأمور الطائفية، فمجرمي الإنترنت يعدون أشخاص أذكياء يقرفون جرمهم بكل هدوء وبرودة دون أي قطرة دم وهم مندمجين بالمجتمع حيث لا يناصبون العدوان للمجتمع لديهم معرفة إلكترونية[14].

-عدم توفر مفهوم موحد للفعل الجرمي الإلكتروني: حيث لا توجد دلالة قانونية مشتركة يتم تداولها من أجل توضيح الأفعال الجرمية الإلكترونية حيث تتنوع تسميتها بين الاحتيال المعلوماتي أو الاختلاس المعلوماتي أو بالجريمة المعلوماتية أو الغش المعلوماتي، إضافة لكونها أحكام هذه الجريمة تستجد مع التقدم التقني وتخلف أنواع جديدة من الجرائم وبهذا تختلف عن الجرائم العادية كون مكانها صعب التعيين فملفات الحاسوب والرسائل تنتقل من نظام معلوماتي لآخر خلال وقت قصير لا يذكر دون وجود حدود دولية تقطع طريقها هذا، أضف إلى ذلك كله أن النماذج القانونية في كل تشريع دولة مختلف عن الآخر استناداً لاختلاف البيئة والعادات والتقاليد والثقافة والديانات والسياسة التشريعية المتبعة من مجتمع لآخر، وهذا ما يشكل ثغرة في منظومة مواجهة هذه الجرائم وإضعاف فعاليته[15].

-قيام لفعل الجرمي الإلكتروني خلال المعالجة الآلية للبيانات، وهذه الخاصية متميزة للجريمة الإلكترونية حيث يعد هذا شرط مستلزم حتى تكون أركان هذه الجريمة متوفرة ، فقيام الجريمة الإلكترونية بأركانها الأساسية ذات صلة وثيقة بوقوعها خلال المعالجة الآلية للبيانات ترتبط به وجوداً وعدماً، وقد تتم هذه الجريمة خلال عملية المعالجة في كافة مراحلها عند إدخال البيانات أو أثناء معالجتها أو خروجها، ولقد تم المحاولة من قبل مجلس الشيوخ الفرنسي بوضع تعريف معين لعملية المعالجة الآلية للبيانات ولكنه فشل وتم حذفه استناداً لكونه يمثل عملية ذات طابع فني يخضع بشكل مستمر للتقدم التقني وبالتالي من الصعوبة وضع تعريف جامع مانع لها[16].

-الجريمة الإلكترونية جريمة مستحدثة: حيث عد هذه الأفعال الجرمية أفعالاً جديدة تحمل خطورة جسيمة في إطار العولمة، وهذا أمر بديهي فالتقدم التقني المتطور الذي جعل من العالم قرية صغيرة تذوب فيها كافة الحدود والفواصل الجغرافية والسياسية تطلب نشوء مثل هذه الأفعال المتطورة التي تتجاوز التطور بإمكاناته وأدواته المتاحة، مما خلق تهديد واضح وماس بالأمن وسلامة المواطنين، وهذا ما يخلف هديد واضح لأعضاء التحقيق في قدرتهم على تعقب المرجمين وكشف جرائمهم وإلقاء القبض على الفاعلين[17].

-احتمالية تنوع الأوصاف التي يطلقها القانون على محل الجريمة الإلكترونية: فمحل الجريمة الإلكترونية يأخذ شكلين حيث يتمثل الشكل الأول بالمادي والثاني بالمعنوي، فقد يكون الفعل الجرمي الإلكتروني مخزن على أقراص إلكترونية وهذه المعلومات ذات الطبيعة غير المادية يخضع لأكثر من نص قانوني سواء كانت مادية أم غير مادية أو قد تشكل حالة انتقال أو تواجد في ذاكرة النظام الإلكتروني فتكون في حالة غير مادية من الصعب ضبطها وتخزينها[18].

-مضار الجريمة الإلكترونية حيث يتم اقتراف هذه الجرائم ضمن إطار تقني وتكنولوجي متطور يزيد استعمالها يوماً بعد آخر في إدارة المعاملات المتنوعة سواء ذات الطابع المالي أو الاقتصادي والي قد تنتهك الوضع الحسابي والإداري وتنقلات الأموال والاستثمار ولا تتميز بين كونها المنشآت العامة أو الخاصة حيث تلحق ضرراً بالاثنين، كما وقد تستهدف البيانات الخاصة بالأشخاص والتي يتم تخزينها على ذاكرة الحواسيب المقدمة للبنوك أو شركة التأمين ومراكز الشرطة وغيرها من الأفعال العدوانية بشكل غير مباشر يتم فيه انتهاك الحياة الخاصة والحرية الفردية ويزداد الأمر سوءاً بحال اتصلت هذه الخطورة بالجوانب التي تتعلق بإدارة الدولة عمل الحكومات في

نطاق الأمن والدفاع والمشروعات النووية وتصنيع الأسلحة الحديثة[19].

المطلب الثاني: أنواع الجرائم الإلكترونية ودوافع ارتكابها.

تعد الجريمة الإلكترونية نتاج التقدم العلمي المطور لها خصائص متفردة عن غيرها، وبناءً على هذا كان من الطبيعي أن يكون لها أنواع مختلفة عن الجرائم التقليدية وحتى لتمتد بهذا الاختلاف إلى الدوافع التي تقود لاقترافها ولاسيما في ظل الصفات المميزة لفاعليها والتي تنحصر بهذا النوع من الجرائم هذا ما يدفعنا لتوضيحها وذلك من خلال تقسيم هذا المطلب لفرعين نتطرق في الفرع الأول إلى أنواع الجرائم الإلكترونية وفي الفرع الثاني إلى دوافع ارتكابها وفق التالي.

الفرع الأول: أنواع الجرائم الإلكترونية.

إن صور الجرائم الإلكترونية متنوعة ومختلف ولكنها في المجمل لا تنأى أن تنحصر في إطار الحاسب ومكوناته حيث تتخذ شكلين إما يكون العدوان فيها أنظمة الحاسوب مما ينجم عنه أن تكون هذه الأنظمة محلاً للجريمة أو هدف يسعى إليه الجاني، أما الشكل الثاني فيتصل بالاستخدام غير القانوني للنظم المعالجة الآلية للمعلومات[20]، وما تجدر ملاحظته أن الفاعل في الشكل الأول من الأفعال الجرمية يعتمد على الحاسب لاقتراف الفعل الجرمي الإلكتروني ويتم هذا طريق فعل يقود لتعطيل نظام المعالجة الآلية عن أن يتولى المهام الملقاة على عاتقه، وهذا ما يحصل بموجب أفعال الاختراق أو الدخول غير القانوني في جزء من منظومة المعالجة الآلية للبيانات وهذا ما يتم بالعديد من الأساليب الاحتيالية، كاستخدام رمز الدخول بشكل غير عادي أو باستخدام أنظمة ثانية كبرنامج حصان طروادة مثلاً[21].

وحتى البرامج ذات الطابع الخبيث تأخذ العديد من الأصناف وتهدف لتحقيق عدة غايات فقد يكون غايتها الاحتيال والسيطرة عن طريق الكمبيوتر على الأموال وتحصيل البيانات بالسرقة أو تدمير المعلومات، وفضلاً عن حصان طروادة يوجد القنابل المنطقية وبرنامج الدودة وهي عبارة عن برنامج الدودة وهي عبارة عن برنامج تشغيل يتم إدماجه في أنظمة التشغيل[22].

أما الصنف الثاني من الجرائم الذي يصل بالاستخدام غير القانوني لأنظمة المعالجة الآلية للبيانات فيمثل بإحدى شكلين منها الدخول أو الابقاء غير القانوني ونام المعالجة الآلية والتي تمثل سرقة فائدة المال المعلوماتي أو الحاسب الآلي ، كما في حالة الدخول لنظام الحاسوب ومعرفة مضمونه والبقاء بشكل غير قانوني دون السماح من صاحبه كما هو الحال في العامل الذي يسمح له بموجب القانون بأن يدخل إلى المنظومة المعلوماتية ضمن إطار عمله ثم يستعمل رموز الدخول المزينة يهدف معرفة البيانات الغير متصلة بعمله، كمثال آخر عندا يقوم فريق يتألف من خمسة أشخاص في مديمة شيكاغو بأمريكا تابعين لإحدى المراكز ذات الطابع التعليمي باستغلال الحاسب الآلي الي يبع للمركز من أجل برمجة أعمال عملائهم التي تخص شركة خاصة ثانية لهم، كما وقد تم الكشف عن استعمال الحاسب الآلي في أكبر معامل إنتاج الصواريخ النووية في الولايات المتحدة من خلال مئتي مستخدم من أجل القيام بغاياتهم الشخصية[23].

وقد ازدادت الجرائم الإلكترونية بشكل ملحوظ استناداً لزيادة مساحة انتشار البيانات وعولمتها وهذا ما قاد لانتشار جرائم سرقة المعلومات التي تعد أموال منقولة ويمكن أن يم تقويمها بالمال نظراً لقيمها الاقتصادية، حيث من السهولة للمجرمين الإلكترونيين الأذكياء أن يقوموا بتحويلات لهذه الاموال من أي تبعة في العالم عن طريق الدخول للملفات المذكورة ضمن أنظمة الحاسب بعد أن يتم الحصول على كلمة السر[24].

وبالطبع فإن الجرائم الإلكترونية لم تعد مقتصرة على الإطار ذ الصبغة المالية بل إنها ازدادت لتشمل إطارات أخرى كالاحتيال المعلوماتي في البرامج، وأكثر من ذلك فقد استغل المجرمون هذه التقنية وتطويعها إلى مصلحتهم بما يخدم أفعالهم وتم تكوين العديد من الجماعات الإرهابية عن طريقها مما يشكل خطراً كبيراً جداً اسناداً لحالة عدم الاستقرار الأمني التي ستسود فيما إذا تم توسعها على كافة أنحاء العالم، وهذا ما يجسد مشهداً من مشاهد حرب جديدة إلكترونية، وتشير الإحصائيات المجراة من قبل الجمعية الفرنسية أن الأضرار التي تنتج عن الجرائم ذات الطابع الإلكتروني فوق 104مليارات فرنك فرنسي[25].

الفرع الثاني: دوافع ارتكاب الجرائم الإلكترونية.

تتعدد الدوافع التي تقود لاقتراف الأفعال الجرمية فالرغبة الإجرامية هي المنبع الأساسي للدافع لهذا الإجرام، وهذا الدافع يكون تميزاً عن الدوافع التي تقود لاقتراف الجرائم التقليدية[26]، وفيما يخص الجرائم الإلكترونية هناك نوعين من

الدوافع لاقترافها تنطوي تحتها العديد من الدوافع المتنوعة وهي:

-أولاً: الدوافع الشخصية لاقتراف الأفعال الجرمية الإلكترونية: وتتمثل هذه الدوافع بالدوافع المادية والذهنية والي يكون لها تأثير جلي على هذه الجرائم:

-فالدوافع المادية تعد من أكثر الدوافع التي تدفع الفاعل لارتكاب الأفعال الجرمية الإلكترونية كون الربح الكبير والذي يمكن الوصول له عن طريقها هو الذي يؤدي بالمجرم الإلكتروني لتطوير نفسه حتى يستطيع مواكبة كل تقدم يطرأ على هذه التقني الإلكترونية فيعمل على استغلال الفرص وللاحتراف من خلال التعمق بتفاصيل هذه الأفعال الجرمية من أجل تحقيق أكبر قدر ممكن من الربح وبأقل مجهود دون ترك آثار مادية خلفه، ويعمل على التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية في حال كان الفاعل موظف لها أو قد يقوم باختراق نظم المعالجة الآلية عن طريق اكتشافه لثغراتها الأمنية[27]، فيقوم باستغلالها وتحويلها لمبالغ مالية كبيرة لحسابه أو لحساب غيره يعمل لمصلحة من خارج المؤسسات، وكذلك لا بد من الحصول من المكاسب المالية بطرق أخرى كالمفاوضة على البرامج أو البيانات التي يتم الحصول عليها بأسلوب الخداع من جهاز الحاسب[28].

ذلك أنه في حال نجح المجرم الإلكتروني في اقتراف فعله الجرمي فهذا سوف يحقق له الكثير من الأحوال بوقت قصير فيحصل على أرباح طائلة من ارتكابها[29]، أو قد تكون الدوافع ذهنية والتي تتجلى في التحدي والرغبة في فهم النظام ذا الطابع الإلكتروني وإثبات الذات، فهنا الدوافع هذه قد تجسد مثلاً لحب وهو عالم الإلكترونات وإرادة قهر وظلم النظام والتفوق على أدوات التقنية، فمتعة هؤلاء المرجمين وإمضاء وقت فراغهم تتمثل في كشر النظام المعلوماتي واختراق الحواجز الأمنية التي تحيط بهذه الأنظمة أو قد يرغب المجرم من ارتكاب أفعاله هذه في إبراز تفوقه وكذكائه على أدوات التقدم الحديثة حيث لا يكون لهم في غالبية الأوقات ودافع تخريبية أو تدميرية وإنما تنحصر هذه الأنواع من الدوافع بالتحدي والرغبة في إثبات الذات[30].

أما النوع الثاني من الدوافع فيتمثل بالدوافع الموضوعية لاقتراف الفعل الإلكتروني وتتمثل هذه الأنواع من الدوافع في دافع الانتقام وإيقاع الأذى بصاحب العمل وغالباً ما يتم قيام هذا الدافع وتكونه عند العامل الذي يفصل من عمله أو عدم منحه الترقية والحوافز وعدم مساواته مع غيره من الموظفين، فمثل هذه الدوافع تقود المرجم لاقتراف الفعل الجرمي، وهذا من الدوافع الخطيرة التي تعود الفرد لاقتراف الفعل الجرمي، ويكون من عامل على درجة من الأهمية يمتلك الكثير من المعلومات عن الشركة أو المؤسسة التي يعمل في نطاقها، حيث تكون هذه الدوافع تتصل بالحياة العملية حيث تشكل لدى المرجم الإلكتروني الإرادة في الانتقام من صاحب العمل بعد شعوره بالحرمان من العديد من الحقوق المهنية أو الطرد من العمل[31]، بالإضافة إلى دافع التعاون والتواطؤ والخداع وهو النوع الأكثر انتشاراً في الجرائم الإلكترونية ويحصل بالتعاون بين مختصين وعاملين في النظام المعلوماتي بشكل متعمق حيث يقومون بالجانب الفني بالمشروع الإجرائي و قد يكون الجاني من خارج المؤسسة التي تقع عليها الجريمة ويعمل على إخفاء عمليات لخداع والغش التي تحصل لانتقال المكاسب المادية[32].

المبحث الثاني: التحديات الإجرائية المتصلة بالجرائم الإلكترونية.

إن الطبيعة المتميزة التي تحظى بهذه الجرائم الإلكترونية والتي جعلت مسرحها عالمياً بعد أن كان محلياً، بالإضافة إلى ارتكابها بمجرد نقرة بسيط على لوحة المفاتيح دون الحاجة لأي أداة ثانية، ليتم تدمير حتى أدلتها الرقمية من دون أن تخلف ورائها أثراً يذكر فر أن يكون هناك الكثير من الصعوبات التي تتعلق بها ضمن الإطار الإجرائي، وهذا ما انعكس بدوره على سلطة رجال التحقيق وقدرتهم على ضبطها لاسيما في ظل ضعف الإمكانيات المتاحة لهم وعدم توفر الخبرة الكافية للفهم العميق لهذا النوع من الجرائم بشكل يسمح لهم بمكافحتها بشكل محكم، ولتوضيح الأشكال التي تواجه الجرائم الإلكترونية في الجانب الإجرائي سنقسم هذا المبحث لمطلبين نتطرق في الأول إلى صعوبة إثبات الجرائم الإلكترونية وفي الفرع الثاني إلى صعوبة اجراءات التحقيق ومدى كفاية العقة المقررة لها.

المطلب الأول: صعوبة إثبات الجرائم الإلكترونية.

إن الخصائص التي يتمتع بها الدليل الرقمي تعكس خصوصيته على طبيعة الجريمة الإلكترونية نفسها، وبالتالي تبرز إشكالية صعوبة إثبات هذه الجرائم في ظل الصفات الخاصة التي يحظى بها هذا الدليل مما يشكل عقبة أمام رجال التحقيق، ولتوضيح هذه الصعوبات سنقسم هذا المطلب لفرعين نوضح في الفرع الأول خاصية عدم ظهور الدليل الإلكتروني وسهولة تدميره، أما في الفرع الثاني نبحث صعوبة الوصول للدليل الإلكتروني.

الفرع الأول: عدم ظهور الدليل الإلكتروني وسهولة تدميره.

ينتسب الدليل الرقمي إلى بيئة تتألف من ذبذبات ذات طابع إلكتروني تقني يتم علاجها باستعمال لغات برمجة تقنية حيث يتم التحويل لأصناف متعددة من المعلومات يتم عرضها في صورة صور ونصوص وجداول وغير ذلك، بالإضافة إلى كونها تعطي الفرصة للمستخدم من اختيار إحدى اللغات الأساسية خلال تصرفه مع الجهاز الرقمي، وتنتقل هذه الصور المبرمجة عن طريق أداوت الاتصال الرقمي لشبكات النظم الرقمية[33].

فالوسط الذ يتم اقتراف الفعل الجرمي ذو الصبغة التقنية في إطاره مختلف عن وسط الجرائم التقليدية حيث يعد وسطاً افتراضياً معنوياً غير تقليدي، وبالتالي فالأدلة المتحصلة من هذا الوسط لا بد وتنسجم مع الطبيعة الخاصة لهذه الجرائم وأدوات اقترافها، فالطبيعة الخاصة لهذه الأفعال الجرمية خلقت نوعاً جديداً من الأدلة متناسبة مع الوسط الذي يتم فيه اقتراف جرائم المعلوماتية أي الأدلة الرقمية، وهذا ما سنعكس بدوره على اجراءات التحقيق التصرفات التي يقوم بها رجال التحقيق حيث يتوجب عليهم الاستعداد الكامل للتعامل مع هذا النوع المستحدث من الأدلة[34].

والصعوبة الأساسية التي تواجه رجال التحقيق فيما يتعلق بالدليل الرقمي أن هذا النوع من الجرائم يتم اقترافه في وسط متنوع عن بيئة الجريمة التقليدية، فالأدلة تكون عبارة عن ذبذبا ذات صبغة مغناطيسية أو كهربائية تتشكل معلومات وبيانات لها خاصية رقمية في العلم الإلكتروني، وبالتالي فعدم وضوح الدليل الرقمي ورؤيته يكون الكثير من الإشكالات عن طريق تجميعه وتحليله وهذا ما يستلزم أن يكون رجال التحقيق ذوات خبرة ودراية كافية في أسلوب التعامل مع هذا النوع من الأدلة[35].

وما يزيد الأمور تعقيداً أن هذه الأدلة من السهل أن يتم تخزينها وتدمير كل ما يتعلق بها فهذا ما يجسد العقبة الكبرى التي تقف في طريق استخلاص استناداً للسهولة التي يتميز بها العملية والي لا تتجاوز إلا فترة قصيرة جداً، ولاسيما أن مقترفي الجرائم الإلكترونية يتمتعون بالإبداع والتفوق التقني في مجال العمل الذي يتولونه ولهذا فهم يسعون بشكل ائم لتدمير وتخريب كل دليل من الممكن أن يقود لإدانتهم من خلال التلاعب الغير واضح في أنظمة الحاسوب الآلي ومضمونه[36].

الفرع الثاني: صعوبة الوصول للدليل الإلكتروني.

إن التقدم التقني في مجالا الحياة يرافقه تقدم مرتكبي لجرائم في تنفيذ جرائمهم فيعملون وبشكل مسمر على مسايرة عذا القدم وتطويعه بما يخدم مفاهيمهم وقدرهم على اقتراف الأفعال الجرمية، ولعل هذا ما يتجسد بشكل واضح في الجرائم الإلكترونية حيث يعمد فاعلوها على أحدث الأساليب في اقتراف جرائمهم وهذا ما يضع عراقيل أمام رجال التحقيق خلال ممارسهم اجراءاتهم بجمع الأدلة من أجل إثبات ارتكاب هذه الأفعال، حيث غالباً ما يعمدون لاستعمال تقنية التشفير[37]، أو فرض تدابير أمنية من أجل منع القيام بعملية التفتيش بشكل سليم أو الوصول إلى الأدلة بشكل بسيط وبالتالي صعوبة ضبطها وهذا ما يتم عن طريق استعمال كلمات ورموز سرية يتم من خلالها إخفاء هوية المستخدم خلال دخولها على شبكة الإنترنت باستخدام عدة برامج وتطبيقات والتي تعمل على إخفاء هويته في هذا العالم الافتراضي[38]، فالبيانات والمعطيات التي تم تخزينها بشكل إلكتروني يتم إحاطتها بسياج من الحماية الفنية من أجل منع الوصول غير القانوني لاستنساخها ومعرفتها، بل وقد يلجأ المجرم الإلكتروني لاستعمال أسلوب وسن تعليمات سرية أو ترميزها، فاستعمال مثل هذه الرموز والشيفرات بشكل عام يعتبر إشكالية واقعية تعترض طريق ممارسة ورقابة على المعلومات التي يتم تخزينها ونقلها عن طريق حدوج الدولة والتي تخفض من إمكانية سلطات رجال التحقيق، وهذا ما يخلق صعوبة توفير حماية كافية لمعلوماتها الشخصية التي يتم تخزينها في مراكز الشبكات[39].

يضاف إلى هذا أن التعامل عند قيامه بالتشفير لهذه المعلومات ذات الطابع المعلوماتي والي تحتوي على مضمون غير قانوني لمنع الغير من مشاهدتها يشكل عقبة في إمكانية الوصول إلى الدليل إثبات الجرائم الإلكترونية[40].

كما وتتم إعاقة الوصول للدليل الرقمي من خلال امتناع لمجني عليه عن الإبلاغ عن هذه الأفعال الجرمية، وهذا ما يتضح من خلال توضيح أن نسبة ما يتم كشفه هو فقط واحد بالمئة وأن الإبلاغ عنها لم يتجاوز 5% لاسيما بحال كانت المجني عليه مؤسسة كبيرة كالبنوك والذي قد يلحق به الإبلاغ عن الجريمة أفدح الأضرار فيلجؤون إلى كتمان الموضوع حتى لا يفقد المتعاملون ثقتهم بهم ويعمدون إلى سحب ودائعهم أو رغبة في عدم تنبيه باقي المرجمين بوجود نقاط ضعف في أنظمها[40]، ولقد أثبتت الدراسات أن غالبية جرائم الإنترنت ولتي يتم كشفها لا يتم الإبلاغ عنها للشرطة وحوالي 70% من هذه الجرائم لا يتم الإبلاغ عنها[41].

والقاضي ليس له صلاحية الموافقة على دليل وإدانة الفاعل في حال تم الحصول عليها بشكل غير قانوني لتناقض ذلك مع حق المتهم في الدفاع، بالإضافة لمخالفته لقواعد الأخلاق والعدالة، وبالتالي فإن أي سلوك يقوم به الفاعل الإلكتروني أو المجني عليه يكون له أثر في صعوبة الوصول للدليل الرقمي[42].

يضاف إل هذا أن هناك كمية ضخمة جداً من البيانات والمعطيات التي يجب على رجال التحقيق العمل على تدقيقها ومن ثم تحليلها بشكل فني، وهذا ما يتطلب ضرورة وجود خبرة ودراية كافية للمحقق في إطار الحاسوب الإلكتروني وملحقاته وهذا بدوره ينعكس في ضرورة وفر دعائم من الأقراص الجاهزة للتخزين الإلكتروني وهذا ما يستلزم توفر الخبراء الفنيين في نطاق التعامل مع آلة الحاسب من أجل معرفتهم بأسلوب اقتراف الجريمة والمكان الذي من الممكن وجود البيانات فيه والتي تفيد رجال التحقيق[43].

المطلب الثاني: صعوبة اجراءات التحقيق وتناسب العقوبة في الجريمة الإلكترونية.

إن خصائص هذه الجريمة الإلكترونية وطابعها المتفرد انعكس وبشكل واضح على إمكانية تطبيق اجراءات التحقيق التقليدية عليها بل على العكس من ذلك تشكلت العديد من الصعوبات التي اتصلت بإجراءات التحقيق مع عدم قدرة المشرع العراقي على مواجهتها بالعقوبة المناسبة، ولتوضيح ذلك سنقسم هذا المطلب لفرعين نبحث في الفرع الأول صعوبة اجراء التحقيق وفي الفرع الثاني صعوبة تناسب العقوبة المقررة لمثل هذه الجرائم.

الفرع الأول: صعوبة اجراءات التحقيق.

يتم الاستعانة بالإجراءات التقليدية ذاتها المتبعة في التحقيق بالجرائم العادية من أجل كشف الجرائم الإلكترونية ولكن لا بد من أن يتم الأمر ضمن متطلبات خاصة تراعي طبيعتها الخاصة[44]، وأول اجراء تحقيقي يتم القيام به بعد أن يتم ارتكاب الفعل الجرمي هو المعاينة حيث لا بد لقاضي التحقيق بعد سماعه بارتكاب الجريمة من الانتقال والمعاينة لمعرفة طريقة اقترافها وكشف ظروفها ونسبتها إلى فاعلها[45]، وغالبية التشريعات لم تحدد المقصود بالانتقال والمعاينة بشكل دقيق فتم ترك هذا الموضوع للفقه، الذي عرفها بكونها اجراء يقوم من خلاله قاضي التحقيق بالانتقال إلى محل ارتكاب الفعل الجرمي حتى يشاهد بذاته ما يحصل ويجمع النتائج، وتهدف المعاينة إلى جمع البراهين التي تترتب على الفعل الجرمي وإفساح المجال للمحقق حتى يرى محل ارتكاب الفعل الجرمي ويكون فكرة صحيحة واضحة لا غموض فيها عن أسلوب اقتراف الفعل الجرمي[46]، وفي إطار الجرائم الإلكترونية تنصب المعاينة على الآثار التي تترتب من قبل مستخدم الشبكة المعلوماتية أو الإنترنت وتضمن جميع الرسائل التي تم إرسالها منه أو تم استقبالها وجميع الاتصالات التي تتم عن طريق الكمبيوتر والإنترنت، وتقع المعاينة على المسرح التقليدي[47]، والمسرح الافتراضي[48]، وتتنوع صور المعاينة استناداً لنوع الجرم المقترف على الرغم من وجود أساليب عامة تتناسب مع طبيعة الاتصال بالإنترنت كوسيلة تصوير شاشة الكمبيوتر التي تتم عن طريق آلة تصوير تقليدية بموجب استعمال برمجة حاسوب متخصصة في أخذ صورة لما يظهر على الشاة، وهو ما يسمى تجميد مخرجات الشاشة[49].

وتحظى اجراءات المعاينة في الجرائم الإلكترونية بطابع متميز عن الجرائم التقليدية استناداً لصبغتها الخاصة المتفردة، ويعمل قاضي التحقيق بالتقيد بالأصول الفنية خلال ممارسة عمله حيث يجب عليه عدم العبث بالأجهزة الموجودة بمسرح الجريمة والمحافظة على حالها كما هي وذكر ذلك في المحضر، كما ولا بد من تحرير الأوراق التي تم طباعتها على الحاسب الآلي وتم العثور عليها بمسرح الجريمة ووضعها في أكياس استناداً لحالتها حيث يجوز عادة طباعتها بحال كان الجهاز مشغل وتفقد الجهاز ثم تدوين ما إذا كان هناك برامج تم استعمالها لحظة دخول مسرح الجريمة، ثم يتم ترقيم دعائم التخزين التي يتم العثور عليها، وتوضع في أكياس خاصة لحمايتها من الكسر، وغالباً ما يتم الاستعانة بخبير بمثل هذه المسائل[50].

وهناك العديد من الإشكاليات التي تواجه اجراء المعاينة وأهمها:

ضعف أو انخفاض الأدلة ذات الأثر المادي التي تنتج عن الجريمة الإلكترونية، وإمكانية الإخلال بهذه الأدلة وتدميرها وحتى تبديلها استناداً إلى ارتياد العديد من الأفراد لمسرح الجريمة خلال المدة الزمنية بين وقوع الفعل الجرمي والكشف عنها والتي تعد فترة طويلة نسبياً، وهذا ما يثير الشك وعدم المصداقية في الأدلة التي يتم تحصيلها من المعاينة[51]، ويضاف إلى هذا أن فاعل الجريمة له قدة على إتلاف المعطيات والمعلومات ولو كان بعيداً عنها من خلال التدخل عن طريق وحدة طرفية خارجية، لوضع حد بمثل هذا الإجراء لا ب من تدخل المشرع في وضع عقوبات جزائية على القيام بمثل هذه التحريفات الي يتم تخزينها في الآلة الإلكترونية المستخدمة في ارتكاب الجريمة، يضاف إلى هذه الصعوبة هناك معوقة فقدان الأدلة ذات الطابع الإلكتروني التي يتم تبديلها أو محوها خلال وقت قيصر لا يتجاوز الثواني، واستناداً لهذا عمل العديد من المشرعين إلى فرض العجلة على اجراء المعاينة عند وقوع جريمة إلكترونية من أجل فقدان الأدلة

وهذا عن طريق إرسال رسالة لمزود الخدمة ليلاً من السجلات المطلوبة حتى يتم إصدار أمر من المحكمة للقيام بهذا الإجراء أو غيره[52].

ولا بد من حصر معاينة المسرح الإلكتروني بالباحثين والمحققين أصحاب الكفاءة والخبرة ذات الطابع الفني والعلمي حيث إن قلة معرفتهم التقنية قد تعود لكارثة إذا ما تم المساس بالأجهزة بشكل عشوائي وتمير الدليل الرقمي وبالتالي استبعاد احتمال كشف الفاعل والوصول للحقيقة، فالأدلة الموجودة ضمن مسرح الجريمة تتطلب عاملة خاصة.

أما الإجراء الثاني فهو التفتيش الذي يعد من أهم اجراءات التحقيقي التي تساعد في الوصول للحقيقة وتعد من الإجراءات الخطيرة على الحياة الخاصة، وغالباً ما نص دساتير الدول على ضمان حرمة المنازل وعدم إباحة تفتيشها إلا بموجب القانون وبنطاق احترامه حيث لا يتم التفتيش إلا بموجب أمر مكتوب يصدر عن السلطة القضائية المختصة[53].

ويتمثل التفتيش بكونه بحث في مكان ما من أجل إيجاد أشياء تتصل بالجريمة التي تم جمع الأدلة عنها أو حدوث التحقيق فيها، فهو اجراء تحقيقي تتولاه سلطة أعطاها القانون إمكانية البحث التفصيلي عن براهين الفعل الجرمي الذي وقع وكل ما يساعد على كشف الحقيقة ولكن هذا يتناقض مع الطبيعة المادية وأدلة الجنائية الرقمية، وتتجلى ضوابط التفتيش للجرائم لإلكترونية بفرعين هما: ضوابط ذات طابع شكلي حيث تتخذ أسلوب آلي من أجل تنفيذ التفتيش والقائمين بالتفتيش[54]، أما النوع الثاني فيتمثل بضوابط ذات طابع موضوعي وتحتوي على وقوع الأفعال الجرمية ذو الصبغة الإلكترونية من أجل تحقيق أهداف غير قانونية ووجود دلائل على توفر أشياء أو أجهزة الكترونية من أجل اكتشاف الحقيقة ولا يتم القيام بالتفتيش إلا بحال وجود أسباب تثبت وجود رسائل استعملت بهذه الجريمة لدى المحققين في مكان الشخص الذي يطلب تفتيشه[55].

ويثير اجراء التفتيش صعوبة بحال كان جهاز المتهم الذي اقترف الجرم بواسطته مرتبطاً مع جهاز آخر، وفي هذه الحالة إذا كان الجهاز المرتبط به موجود في ذات ابلد داخل إقليم الدولة فهذا لا يثير أي صعوبة حيث يمتد التفتيش لهذا الجهاز، أما بحال كان الحاسوب موجود بمكان آخر خارج الإقليم وهنا تواجه صعوبة بالقيام بالتفتيش في شبكة الاصال التي تجمع بين الجهازين خارج البلد، كون القيام بإجراء التفتيش يصطدم بعقبة السيادة للدول وعدم إمكانية القيام بهذا الإجراء نظراً لعدم قانونيته[56].

بل وحتى الدليل المتحصل منها بالضبط يتجرد من شرعيته ويستتبع هذا تجريده من حجيته في الإثبات أمام المحاكم المحلية كون الأداة التي تم الحصول عليه منها لا يتعد قانونية، يضاف إلى هذا أن مقترفي الأفعال الجريمة يعملون على تخزين المعلومات اليت تتصل بجرائمهم خارج حدود الدولة من خلال شبكا الإنترنت وهذا ما يختلق معضلة في الكشف عنها ووضع عقبة أمام رجال التحقيق، وإن الدخول إلى نظام معلوماتي بوجود خارج الدولة لا يسمح به بموجب إذن المحقق المحلي، ولكن يسمح بالقيام بمثل هذه الإجراءات بحال الحصول على الموافقة القانونية من الشخص الذي له الصلاحية في كشف البيانات لذلك الطرف[57].

ويرى الفقه أنه بحال تطلب الأمر بالتفتيش في دولة ثانية خلال ارتكاب جريمة الكترونية فإنه يتطلب وجود اتفاقية دولية ذات طابع خاص يجيز هذا التوسع وإلا فإنه لا مجال لتطبيق التفتيش العابر للحدود إلا بموجب رخصة من الدولة التي يتم القيام بالتفتيش فيها، وفيما يخص المشرع العراقي فإنه لم ينص على اجراءات تفتيش خاصة بالنظم الإلكترونية ولهذا فلا بد من إضافته لإمكانية القيام بالتفتيش سواء كانت الجريمة ادية أو تتعلق بالأنظمة المعلوماتية ولكن قانون الاتصال والمعلومات العراقي قد نص على إمكانية التفتيش للشبكات خلال القيام بالتحقيق[58].

وبحال تم الحصول على الدليل بشكل غير شرعي فإنه سيتيح أن الدليل يبطل لأن ما بني على باطل فهو باطل، كما ولا بد من كون إذن التفتيش معين من حيث الوقت، حيث يفرض على المحقق القيام به خلال المدة المعينة بحيث يجب على المحقق مراعاة عدم كون المدة المعينة غير مجتازة أي أنه يتم مراعاة هذا الوقت عند إصدار الإذن فلا تكون مدة طويلة حتى لا يكون الشخص الصادر بحقه الإذن قد لحقه تهديد في حرمة مسكنه مدة طويلة[59].

أما فيما يخص اجراءات الضبط في الجرائم الإلكترونية فإن الأشياء التي يتم ضبطها وتكون ذات صلة بالجرائم تتصف بكونها ذات صبغة معنوية، فضبط الأشياء غالباً ما يتم على عناصر الكترونية منفصلة كالأسطوانات الممغنطة وهذا الأمر من السهولة حيث لا يثور أي مشكلة، ولكن الإشكالية تكمن بحال تطلبت الحاجة في الجريمة الإلكترونية أن يتم ضبط كل النظام أو الشبكة لاحتوائها على عناصر من الصعب فصلها، بينما ضبط المكونات المادية للحاسوب فل يثير صعوبة حيث

يتم ضبطها بشكل مباشر، وبعد أن يتم ضبط كافة البيانات يتم تحريزها ثم تأمينها بشكل تقني[60].

أي أن هناك صنفين من أصناف الضبط في هذا الجانب أصول مبدئية تحفظية من أجل توفير الحماية للبيانات التي تم تخزينها وتكون هامة في التحقيق بحال بقيت في موقعها من النظام الإلكتروني للحاسب أو في دعامة التخزين ومنع الوصول لها أو التصرف بها أو إلغائها، من أجل كشف فاعل الجرم وسهولة الإثبات ، أما الصنف الثاني هو اجراءات تلحق عملية الضبط حيث يتم تفريغ كافة المعلومات المخزنة في الحاسوب وتحويلها إل أوراق ولا يتم فتح هذه الملفات المحرزة إلا بحضور المتهم مع محامية على أن يم استدعائهم وفق القانون من أجل المحافظة على حقوق الدفاع واحترام مبدأ السرية[61].

والإجراء الأكثر أهمية في إطار الجرائم الإلكترونية هو الخبرة ذلك أن الخصوصية التي تتمتع بها الجرائم المعلوماتية كونها يتم اقترافها بأدوات تقنية متطورة وصعبة تجعل رجال التحقيق أمام حيرة في أمرهم في إطار عدم تمتعهم بالكفاءة المطلوبة في هذا الجانب، فهي تمثل كتلة بيانات معقدة وشيفرة من الصعب على رجال التحقيق العاديين فكها ومعرفة الحقيقية الحصول على الدليل، ولهذا يتم اللجوء لهل الخبرة وتكريساً لمبدأ التخصص، وتمثل تقييماً لهذا الدليل الغير المرئي[62].

ويعمد الخبير إلى جميع البيانات من الأدلة الجنائية وتحصيلها في خوادم المقع والجهاز الذي تم الاعتداء عليه بعد أن يتم تحديده، ثم يتم القيام بعملية تحليل من قب الخبير وتحديد عناصر حركتها للوصول إلى أسلوب إعدادها وإسنادها لمسارها الذي اعدت فيه ووصلاً إلى برتوكول الإنترنت للجهاز الذي صدر منه الذبذبات الإلكترونية[63]، فدور الخبير جوهرياً لجرائم المعلوماتية كمساع رافد للقضاة والمحققين فهو يساعدهم على تكوين قناعتهم عن المسائل التي تحتاج لمعرفة فنية متخصصة، وغالباً ما يتوقف نجاح قضاة التحقيق في ملهم على عمل الخير وكفاءته في إطار تعمقه في الجرائم الإلكترونية، ويتحدد عمل الخبير بأسلوبين يقوم بجمع واستخلاص كافة المواقع المشكلة للفعل الجرمي كالتهديد والنصب ثم يقوم بتحليل رقمي لها من أجل الوصول لأسلوب إعدادها البرمجي وإسنادها للطريق الذي جهزت له وتعيين عناصر حركتها وكيف تم الوصول لمعرفتها ومن ثم الوصول لمعرفة برتوكول الإنترنت الذي يسند إلى جهاز الحاسوب الذي صدرت عن هذه المواقع[X]، أما الأسلوب الثاني فهو يتجلى بجمع واستخلاص كافة المواقع التي لا تشكل جرم قائم بذاته ولكن الجرائم تنصب عن طريق متابعة موضوعات هذه المواقع[64].

الفرع الثاني: عدم تناسب العقوبة المقررة في التشريع العراقي.

تتنوع الجرائم الإلكترونية وهي على اختلاف أنواعها وتطورها الدائم لم يواجهها المشرع العراقي بالمواجهة الكافية، حيث لم يصدر قانون خاصاً حتى الآن بالجرائم الإلكترونية في العراق من أجل فرض عقوبة مناسبة لهذه الأفعال المستجدة، وإنما يتم التعامل بالقواعد التقليدية ذاتها المطبقة على الجرائم العادية، وفيما يتعلق بالجرائم التقليدية التي م اقترافها باستعمال المعلوماتية فهناك نوعين منها :وفيما يخص النوع الأول الذي يتمثل بالجرائم التي يتم فيها العدوان على الأشخاص كجريمة التشهير عبر الإنترنت الذي يمثل باستعمال الإنترنت من أجل نشر مواضيع تلحق الضرر والأذى بسمعة وكرامة الناس باستخدام بريد إلكتروني أو أحد صحف إلكترونية أو أي أداة الكترونية ثانية[65]، وبالعودة للمشرع العراقي نجد أن النصوص الخاصة بجريمتي السب والقذف هي التي يمكن تطبيقها على جريمة التشهير عبر الإنترنت كونها تؤدي لذات النتيجة الجرمية، وهذا ما قضت به المحكمة العراقية[66]. وجريمة التزوير الإلكتروني حيث يتم تجريم كل أفعال العدوان على الأموال كالشرقة والاحتيال والتزوير، وبعد تقدم التكنولوجيا ظهر أصناف جديدة من الوثائق وألصق بها طابع الإلكترونية فأصبحت تمثل محررات إلكترونية، وفيما يخص المشرع العراقي فإنه لم يتعرض لتعريف التزوير الإلكتروني وإنما عرف التزوير بشكله العام وعامله كالتزوير المعلوماتي وفرض ذات العقوبة حيث لم يتطلب وقوع التزوير على كامل المعلومات وإنما يكتفي بجزء منه وأن يكون واضحاً أو مخفياً[67].

أما بالنسبة للجرائم المستحدثة فإن القانون العراقي جاء قاصراً على إمكانية احتواء مثل هذه الأفعال وهذا ما يشكل صعوبة واقعية أمام المحاكم في القدرة على التعامل مع مثل هذه الجرائم، وكمثال عن هذه الجرائم جرائم الدخول للأنظمة المعلوماتية التي تتطلب قيام الفاعل بسلوك خارجي ملموس أو نشاط مادي يتم فيه التعبير عن الإرادة في امساس في أنظمة الحماية الأمنية التي يتم وضعها من قبل مؤسسات الدولة أو الشركة الخاصة أو الأفراد من أجل حماية نظمها المعلوماتية من أفعال النصب والإتلاف ويتم تعبير الجاني عن إرادته في البقاء بهذا النظام بشكل غير مشروع من أجل تحقيق هدف إجرامي[68].

وبالرجوع للقانون العراقي الذي لم يتعرض لهذا النوع من الجرائم مما يشكل ثغرة قانونية ومن الصعوبة مواجهة هذه الجريمة استناداً على نصوص التجريم التي تقع في القانون العراقي كون هذا الفعل الجرمي يشكل نشاط مستحدث[69].

الخاتمة:

بعد أن انتهينا من دراسة أحكام الصعوبات التي تواجه الجرائم الإلكترونية على الصعيد الإجرائي من حيث الإثبات والعقوبة، توصلنا لجملة من النتائج والاقتراحات:

النتائج:

1. تعد الجرائم الإلكترونية من الجرائم المتطورة ترتبط بوجود الإنترنت وتطوره الدائم لها خصائص متفردة عن كافة الجرائم التقليدية سواء من حيث وسيلتها أو مرتكبها أو أدلتها وغيرها من الميزات.
2. تأخذ الجرائم الإلكترونية صنفين إما تقليدية تقع على الأشخاص والأموال، أو مستحدثة ذات طبيعة تقنية تتصل بالأنظمة والبيانات الإلكترونية وقد استطاع المشرع العراقي مواجهة التقليدية منها بذات القواعد التقليدية للجرائم العادية، ولكنه عانى من ثغرة واضحة في قانونه للتعامل مع الجرائم المستحدثة ويشكل صعوبة كبيرة في هذا.
3. يوجد العديد من لصعوبات التي تتعلق بالجرائم الإلكترونية أبرزها صعوبة التعامل مع مسرح الجريمة الإلكترونية خلال المعاينة نظراً لطبيعتها العابرة للحدود واختراقها لكافة الحدود الجغرافية، بالإضافة إلى صعوبة اجراء التفتيش بمثل هذه الجرائم التي لا تترك دليل غير مادي وغير مرئي فضلاً عن ضرورة توفر الخبرة اللازمة أمام رجال التحقيق حتى يمكن السيطرة على مثل هذه الأنواع.
4. يوجد إشكالية واضحة في عدم قدرة القانون العراقي على التعامل مع الجرائم المستجدة، استناداً لعدم وجود قانون ينظم مثل هذه الأنواع من الجرائم.

الاقتراحات:

1. العمل على تأهيل رجال التحقيق وإعادة تدريبهم بشكل دوري من أجل متابعة تطور هذه الجرائم الإلكترونية والقدرة على كشفها في الوقت المناسب كمحاولة منهم لضبطها بشكل محكم.
2. العمل على تكريس التعاون بين المؤسسات الدولية التي تختص بمواجهة هذه الجرائم العابرة للحدود من أجل متابعة المستجدات على الساحة العالمية.
3. نوصي المشرع العراقي بإصدار قانون بمكافحة الجرائم الإلكترونية ووضع نظرية متكاملة عن أحكامها تضمن الوقوف في سبيل انتشارها وازديادها مع صياغة قواعد قانونية كفيلة بذلك.
4. تكريس دور المجتمع بالتوعية بمخاطر الجرائم وآثارها السلبية على المجتمع وخطر المواقع التي تعمل على نشر الأفكار الإرهابية أو التي تزرع الفتنة أو تنشر عن المخدرات.
5. نوصي المشرع العراقي بفرض جزاءات خاصة تناسب هذا النوع من الإجرام والتخلي عن القواعد القانونية التقليدية في التعامل معها.

قائمة المراجع:

أولاً: الكتب.

1. أحمد أبو القاسم ، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، ج1، المركز العربي للدراسات الأمنية، السعودية، 1993.
2. أحمد حسام الدين طه، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2001.
3. أسامة أحمد المناعسة، جلال محمد الزعبي، صابل فاضل الهواشة، جرائم الحاسب الآلي والإنترنت، دار وائل للنشر والتوزيع، عمان، دون سنة نشر.
4. جعفر حسن جاسم الطائي، رائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البلدية، عمان، 2007، ص131.
5. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.
6. حسن أو سقيعة، التحقيق القضائي، دار هومة، الجزائر، 2013.
7. حسين محمود ابراهيم، التحقيق الجنائي في مواجهة التقنيات والمتغيرات، دار النهضة العربية، القاهرة، 1975.
8. خالد الحلبي، اجراءات التحري التحقيق في جرائم الحاسب والإنترنت، دار الثقافة، الأردن، 2011.
9. خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2011.
10. دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتي، ط1، دار الفكر الجامعي، الاسكندرية، 2016.
11. راشد محمد المري، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2018.
12. طه أحمد الرشيدي، مدى المواجهة التشريعية لجزاء المعلومات في النظام الجزائي المصري والسعودي، ط1، دار الكتب والدراسات العربية، الاسكندرية، 2016.

13. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر ولإنترنت، دار الكتب القانونية، 2002.
14. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت،،، 2011.
15. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت.
16. علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الاسكندرية، 1997.
17. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، ط2، دار النهضة العربية، مصر، 1995.
18. عمر محمد بن يونس، الدليل الرقمي، دون دار نشر، مصر، 2006.
19. فراح مناتي، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر، الجزائر، 2008.
20. مأمون سلامة، الإجراءات الجنائية في التشريع المصري، ج1، دار النهضة العربية، القاهرة، 2000.
21. محمد أحمد عباية، جرائم الحاسب وأبعادها الدولية، دار الثقافة، عمان، 2005.
22. محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2004.
23. محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج، عمان، 2006.
24. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات ، مطابع الهيئة المصرية العامة للكتاب، 2003.
25. محمد عبد الله لأبو بكر سلامة، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الاسكندرية، 2006.
26. محمد علي العريان، الجرائم المعلوماتية، ط2، دار الجامعة الجديدة، الاسكندرية، 2009.
27. مسرة خالد محمد، الدليل الرقمي ومعايير جودته، ط1، مركز الكتاب، عمان، 2012.
28. مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دار الكتب القانونية مصر، 2005.
29. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، در الكتب القانونية، مصر، 2006.
30. نائلة عادل محمد فريد قورة، رائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2004.
31. نبيلة هروال، الجوانب الإجرائية لجوانب الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2013، ص212.
32. هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع النقارن،ط1، دار النهضة العربية، القاهرة، 1992.
33. هشام محمد رستم، جرائم الحاسب المستحدثة، ط1، دار الكب القانونية، مصر، 1999.
34. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر، 1995.
35. وضاح محمود الحمود ونشأت مقضي المجالي، جرائم الإنترنت، دار المنار للنشر، 2005.

الرسائل الجامعية:

1. بن لاغة عقيلة، حجية أدلة الإثبات الحديثة، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، 2012.
2. سعيداني نعيم، آليات البحث التحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج خضر، باتنة، 2012.
3. سوزان نوري، الإثبات في جرائم الإنترنت في القانون العراقي المقارن، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2015.
4. سوير سفيان، جرائم المعلوماتية، رسالة ماجستير، جامعة أبو بكر بلقايد، تلمسان، 2011.
5. صغير يوسف، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، الجزائر، 2023.

الأبحاث:

1. أبو بكر سليمان، جرائم الحاسوب وأساليب مواجهتها، مجلة الأمن والحياة، ع21، سنة 13، 2017.
2. ثابت دينازاد، مراقبة الاتصالات الإلكترونية والحق في رمة الحياة الخاصة، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، ع6، 2026.

الهوامش

[1] هشام محمد رستم، جرائم الحاسب المستحدثة، ط1، دار الكب القانونية، مصر، 1999، ص.180

[2] محمد علي العريان، الجرائم المعلوماتية، ط2، دار الجامعة الجديدة، الاسكندرية، 2009، ص177.

[3] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت،،، 2011، ص.15

[4] محمد أحمد عباية، جرائم الحاسب وأبعادها الدولية، دار الثقافة، عمان، 2005، ص.17

[5] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر، 19995، ص.34

[6] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، .35

[7] أسامة أحمد المناعسة، جلال محمد الزعبي، صابل فاضل الهواشة، جرائم الحاسب الآلي والإنترنت، دار وائل للنشر والتوزيع، عمان، دون سنة نشر، ص.31

[8] عبد الله حسين علي محمود، بحث بعنوان اجراءات جمع الأدلة في مجال سرقة المعلومات، مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، دبي، 2003، ص.86

[9] وتتعدد الأجهزة المعلوماتية المستخدمة في الجرائم الإلكترونية فقد يستخدم جهاز الحاسب الآلي أو الهواتف النقالة الذكية وكذلك الأقمار الصناعية تضاف كوسيط إلكتروني.

[10] علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الاسكندرية، 1997، ص12.

[11] حيث تشير الدراسات أن ما يتم اكتشافه من جرائم المعلومات يصل إلى نسبة 1% والذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل إلى 5% فقط.

[12] هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع النقارن، ط1، دار النهضة العربية، القاهرة، 1992، ص20.

[(1)] تشير الدراسات أن هؤلاء الصنف من المجرمين يعتبرون أشخاص متطفلون وغير مرحب بهم لدى الغير وأغلبهم ما يكون جانبهم تحدي الشباب للدخول إلى المواقع الرسمية وبعض الأحيان الدخول إلى مواقع حسابات من أجل إثبات الذات وغالباً تكون أعمارهم في سن المراهقة.

[13] بنظرة متأني للأنظمة القانونية القائمة في الكثير من الدول يتضح عدم وجود اتفاق عام ومشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحاً في أحد الأنظمة قد يكون مجرماً وغير مباح في نظام آخر والنشاط الذي يشكل جنحة يعاقب عليها بالحبس في تشريع قد يشكل مخالفة يعاقب غليها بغرامة في تشريع آخر، موجود لدى أبو بكر سليمان، جرائم الحاسوب وأساليب مواجهتها، مجلة الأمن والحياة، ع21، سنة 13، 2017، ص38.

[14] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة المصرية العامة للكتاب، 2003، ص59.

[15] كان هذا التعريف ينص على أنها (كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط التي يربط بينها مجموعة من العلاقات والتي عن طريقها يتم تحقيق نتيجة معينة وهي المعالجة المعطيات على أن يكون هذا المركب خاضعاً لنظام الحماية، موجود لدة علي عبد الاقدر قهوجي، الحماية الجنائي للبيانات إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، 2000، ص.43

[16] يرجع البعض أن السبب في عولمة هذه الجرائم إلى أنه من حيث المكان تختلف المواقيت بين الدول فيصعب تعيين أماكن ارتكاب الجريمة بين أكثر من دولة، ومن حيث الزمان تختلف المواقيت بين الدول فيصعب تعيين وقت ارتكاب الجريمة، موجود لدى عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر ولإنترنت، دار الكتب القانونية، 2002، ص102.

[17] محمد عبد الله لأبو بكر سلامة، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الاسكندرية، 2006، ص97؟

[18] نائلة عادل محمد فريد قورة، رائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2004، ص.136

[19] فراح مناتي، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر، الجزائر، 2008، ص49.

[20] وهو برنامج خادع يخفي ظاهرة غرضها غير مشروع ويهر كبرنامج عادي يؤمن بعض المهام المفيدة والمألوفة لمستخدميه بينما يكون بداخله وبطريقة خفية بعض الأوامر أو التعليمات الي تؤدي عند تشغيله مهاماً ضارة غير موقعة تمثل أغراضه الحقيقية المضرة وقد بدأ هذا البرامج في أمريكا في أواخر السبعينات نتيجة انتشار استخدام اللوحات الإلكترونية للبيانات التي تنتج تخفيف أو زيادة تحميل البرنامج وهذا النوع من البرامج يبدو عند تشغيله كحد ألعاب التسلية ثم يقوم بعد ذلك بمحو أقراص النظام.

[21] وتعرف الفيروسات المتنقلة أو الدودة بأنها أكثر أنواع البرمجيات الخبيثة شيوعاً، وهي تنشر عبر شبكات الكمبيوتر من خلال استغلال الثغرات في نظام التشغيل وهي عبارة عن برنامج قائم بذاته يستنسخ نفسه من أجل إصابة أجهزة كمبيوتر أخرى دون الحاجة إلى اتخاذ اجراء من أي شخص وبما أن هذه الفيروسات تنتشر بسرعة فغنه غالباً ما يتم استخدامه في نفيذ كود برمجي ضار يسعى لإحداث ضرر في النظام.

[22] وفي نفس السياق أكدت احصائيات قام بها مكتب التحقيق الفيدرالي بأن خسائر الشركات من الهجمات الفيروسية وغيرها من الخروقات غير القانونية يبلغ ما يقارب 68.2 مليون دولار سنوياً وقد شملت هذه الإحصائيات أكثر من 2066 مؤسسة أو شركة متضررة من هذه الهجمات.

[23] عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، ط2، دار النهضة العربية، مصر، 1995، ص102.

[24] أما في الولايات المتحدة الأمريكية فإن احصائيات مكتب التحقيقات الفيدرالية أكدت بأن الخسائر المترتبة عن الجرية الإلكترونية تفوق 150 مرة الجريمة العادية، وبشكل عام فإنه يصعب تقدير حجم الخسائر الناجمة عن الجرائم المعلوماتية كما تشير إليه الأبحاث التي أجري بشأنها في معظم الدول الغربية، سيما فرنسا والولايات المتحدة الأمريكية وإنكلترا كما أصدر مكتب الجنائي الاتحادي في ألمانيا في السنوات الأخيرة تقريراً يحذر فيه من خطورة استعمال الوسائل المعلوماتية من طرف الإرهابيين لأنها أصبحت أهم وسيلة لهم.

[25] يعرف الدافع بكونه العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام وهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى.

[26] سوير سفيان، جرائم المعلوماتية، رسالة ماجستير، جامعة أبو بكر بلقايد، تلمسان، 2011، ص14.

[27] وقد أشارت في هذا الإطار مجلة Securite informatique وهي مجلة متخصصة في الأمن المعلوماتي وأن 43% من حالت الغش المعلن عنها قد تمت من أجل اختلاس أمال و23% من جل سرقة معلومات، و19% أفعال إلاف 15% الاستعمال غير المشروع للحاسوب لأجل حقيق منافع شخصية.

[28] ويمكن توضيح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر أين أجري هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة لأنظمة المعلوماتية وأن 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات.

[29] وضاح محمود الحمود ونشأت مقضي المجالي، جرائم الإنترنت، دار المنار للنشر، 2005، ص.31

[30] مثال ذلك أن الانتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بدويون الشركة التي يعمل فيها بعد رحيله بستة أشهر وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

[31] جعفر حسن جاسم الطائي، رائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البلدية، عمان، 2007، ص131.

[32] نبيل جاد، جرائم الحاسب الآلي، بحث منشور في ندوة المواجهة الأمنية للجرائم المعلوماتية، مطبعة بن سمان، دبي، 2015، ص28.

[33] سوزان نوري، الإثبات في جرائم الإنترنت في القانون العراقي المقارن، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2015، ص145.

[34] عمر محمد بن يونس، الدليل الرقمي، دون دار نشر، مصر، 2006، ص91.

[35] أحمد أبو القاسم ، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، ج1، المركز العربي للدراسات الأمنية، السعودية، 1993، ص89.

[36] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، در الكتب القانونية، مصر، 2006، ص64.

[37] مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دار الكتب القانونية مصر، 2005، ص83.

[38] مسرة خالد محمد، الدليل الرقمي ومعايير جودته، ط1، مركز الكتاب، عمان، 2012، ص.149

[39] كما في حالة نقل البيانات المتعلقة بجرائم غسيل الأموال عبر الإنترنت بعد تشفيرها حيث عمل الفاعل بعد ارتكابه هذه الجريمة على محو آثارها التي تدل على وقوعها كما وذلك من خلال التوسل بتقنيات معدة لهذا الغرض مع الأخذ بعين الاعتبار وسهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي مكن القيام بها في أرقام قياسية متناهية القصر تقاس باللحظات والثواني.

[40] والمثال على ذلك أن بنك marchant bankcity في إنكلترا لنقل 8 مليون جنيه استرليني من إحدى الأرصدة إلى رقم حساب في سويسرا وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور ولكن بدلاص من أن يقوم البنك بتحريك الدعوى الجنائية ضده فقد قام بدفع مبلغ 1 مليون جنيه استرليني له بشرط عدم إعلام الآخرين عن جريمته وإخطار البنك بالآلية التي تمكن من خلالها باختراق نظام الأمن الخاص بالحاسب للبنك الرئيسي.

[41] ومن هذه الدراسات دراسة المعهد الأمريكي للعدالة التابع لوزارة العدل الأمريكية شمات 127 من العاملين في مجال التحقيق في جرائم الحاسب الإلكتروني والإنترنت يمثلون 11 وكالة رسمية.

[42] بن لاغة عقيلة، حجية أدلة الإثبات الحديثة، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، 2012، ص116.\

[43] خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص75.

[1] فراح مناتي، أدلة الإثبات الحديثة في القانون، مرجع سابق، ص35.

[44] محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج، عمان، 2006، ص256.

[45] مأمون سلامة، الإجراءات الجنائية في التشريع المصري، ج1، دار النهضة العربية، القاهرة، 2000، ص640.

[46] وهو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية الذي وقعت فيه الجريمة، مثل الجرائم الواقعة على أشرطة الحاسب والكابلات الخاصة به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس.

[47] ويع عادة داخل البيئة الافتراضية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله، وفي مقدمتها الجرائم الواقعة على برامج الحاسب الآلي أو بيانات اليت تتم بموجبها وكذلك الجرائم التي تتم بطريق الإنترنت.

[48] نبيلة هروال، الجوانب الإجرائية لجوانب الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2013، ص212.

[49] محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2004، ص122.

[50] لعل أبرز الأماكن التي يحتمل تواجد الأدلة الجنائية فيها والمتعلقة بالجرائم الإلكترونية فيها ما يلي: –الورق ويتم الحصول عليها من خلال البحث في سلة المهملات عن أوراق مطبوعة لها علاقة بالحاسب الآلي، والمكونات المادية كأجهزة الحاسب الآلي بأنواعها المختلفة، والبرامج ووسائط التخزين المتحركة، ودليل الاستخدام الخاص بالمكونات المادية والتقنية للجهاز الإلكتروني.

[51] أحمد حسام الدين طه، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2001، ص.77.

[52] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، .2002

[53] وقد نظم المشرع الأمريكي أسلوب تنفيذ التفتيش في أنظمة الحاسب الآلي وتكون في اقتحام قوات الشرطة المكان بطريقة سريعة وذلك لتقليل احتمال حدوث أي إصابة في المهمة، وبعد ذلك يتم إبعاد جميع المشتبه فيهم عن كل الأنظمة في مكان بعيد عن أجهزة الكمبيوتر وتكونوا تحت حراسة ويقدم إذن التفتيش ويتم تحذيرهم بأن أقوالهم ستكون دليل إدانة ضدهم وأنه سيتم التفتيش وفقاً لإذن الصادر من القاضي أو النيابة وإذا عثر على النقطة الساخنة وهي جهاز الكمبيوتر يقم فريق مكون من اثنين من العملاء للكشف والبحث عن الملفات ويقوم المسجل بتصوير جميع الأجهزة.

[54] وقد أجازت المادة 32 من الاتفاقية الأوربية بشأن مكافحة الجرائم المعلوماتية التي يتم التوقيع عليها قفي بودابست عام 2001 ، إمكانية الدخول تفرض التفتيش والضبط في أجهزة حاسب أو شبات لدولة أخرى بدون إذن في الدخول وذلك للتفتيش في أجهزة حاسب وشبكات تابعة لهذه الدولة الأخرى بتوفير ما لديها بتوفر حالتين إذا رضي المالك والحائز على هذه البيانات بهذا التفتيش، إذا تعلق التفتيش بمعلومات أو بيانات متاحة للعامة.

[55] راشد محمد المري، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2018، ص.84.

[56] نصت المادة 32 من اتفاقية بودابست على أن (الدخول عبر الحدد على بيانات مخزنة عن طريق الموافقة أو حيثما تكون متاحة علنا يجوز لأي طرف دون تفويض من أي طرف آخر :–الدخول على بيانات حاسوب مخزنة علنا بغض النظر عن مكان تواجد البيانات جغرافيا، الدخول على بيانات حاسوب مخزنة موجودة في طرف آخر أو أن يتلقاها عن طريق نظام حاسوب في إقليمه وذلك في حالة حصول ذلك الطرف على الموافقة القانونية والطوعية من الشخص الذي له السلطة القانونية في الكشف عن لبيانات لذلك الطرف من خلال نظام الحاسوب المذكور).

[57] حسين محمود ابراهيم، التحقيق الجنائي في مواجهة التقنيات والمتغيرات، دار النهضة العربية، القاهرة، 1975، ص77.

[58] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، الجزائر، 2023، ص28.

[59] كوحدات الإدخال (لوحة المفاتيح والفارة ونظام القلم الضوئي) أما ضبط وحدات الإخراج (كالشاشة الطابعة الرسام المصغرات الفيلمية).

[60] خالد الحلبي، اجراءات التحري التحقيق في جرائم الحاسب والإنترنت، دار الثقافة، الأردن، 2011، ص159.

[61] سعيداني نعيم، آليات البحث التحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج خضر، باتنة، 2012، ص171.

[62] حسن أو سقيعة، التحقيق القضائي، دار هومة، الجزائر، 2013، ص110.

[63] ثابت دينازاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، ع6، 2026، ص87.

[64] مثل المواقع التي تساعد الغير على معرفة جرعات المخدرات والمؤثرات العقلية حسب وزن الإنسان بإيهامه أنه إذا تم تتبع المعلومات الواردة فيها لن يصل الشخص إلى حالة إدمان، كذلك الشأن بالنسبة لكيفية إعداد القنابل وتخزينها أو كيفية التعامل مع القنابل الزمنية.

[65] طه أحمد الرشيدي، مدى المواجهة التشريعية لجزاء المعلومات في النظام الجزائي المصري والسعودي، ط1، دار الكتب والدراسات العربية، الاسكندرية، 2016، ص15.

[66] قضت محكمة استئناف بغداد 0الرصافة بصفتها التمييزية بأنه(إن الأدلة المتحصلة في وقائع الدعوى تكفي لإدانة المتهم على وفق أحكام المادة 433 عقوبات والمتمثلة بثبوت قيامه بنشر عبارات تشكل قذفاً وعليه يمكننا تعريف جريمة التشهير عبر الإنترنت بأنها تشويه شرف أو سمعة الإنسان عبر نشر كل ما من شأنه أن يؤدي لذلك سواء تعلق الأمر بسب أو بقذف أم بإفشاء سر من خلال استخدام الإنترنت)، موجود على الموقع الإلكتروني www.iraqia.iq. تاريخ الدخول 2025./4/7

[67] محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية وجرائم الكمبيوتر، مرجع سابق، ص.113

[68] دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتي، ط1، دار الفكر الجامعي، الاسكندرية، 2016، ص.49

[69] لا بد أن نشير أن مشروع قانون الجرائم المعلوماتية العراقي لسنة 2011 تضمن مجموعة من النصوص لتجريم الدخول أو البقاء غير المشروع داخل النظم المعلوماتية، حيث ورد أنه (يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن مليون دينار ولا تزيد على خمسة ملايين دينار كل من دخل عمداً بدون تصريح موقعاً أو ناماً معلوماتياً أو اتصل مع نظام الحاسب أو جزء منه، أو استخدم أو تسبب دون تصريح في استخدام الحاسوب للغير بشكل غير مباشر أو انتفع بدون وجه حق بخدمات الاتصالات من خلال شبكة المعلومات أو أحد أجهزة الحاسوب).