مدى توافر السلوك الاجرامي في الجريمة الالكترونية

م.د رقية فالح حسين

الجامعة العراقية - كلية القانون والعلوم السياسية

Extent of criminal behavior in cybercrime

Iraqia University- Faculty of Law and Political Science

Ruqayah Falih Hussein

Rwrwally52@gmail.com

المستخلص

تعد الجريمة الالكترونية من الجرائم المستحدثة في مجتمعاتنا العربية على الرغم من مرورها بمراحل تطور في بلدان اخرى. ففي المرحلة الاولى من شيوع استخدام الكمبيوتر في الستينات ومن ثم في السبعينات من القرن الماضي، ظهرت اول معالجات لما يسمى بجرائم الكمبيوتر. وفي الثمانينات بدأ التعامل مع الافعال غير المشروعة التي ترتكب في بيئة الحواسيب والشبكات الالكترونية بوصفها ظاهرة اجرامية جديدة وليست مجرد سلوكيات غير اخلاقية . وبسبب تزايد ارتكاب هذا النوع من الجرائم، عمدت بعض الدول الى وضع قوانين جنائية خاصة بهذه الجريمة في حين تركت بعض الدول تنظيم ذلك للقواعد العامة الواردة في قوانينها الجنائية العادية.

الكلمات المفتاحية : سلوك اجرامي – ضحايا – جريمة الكترونية – تنظيم – قوانين عقابية

Abstract

Cybercrime is one of the new crimes in our Arab societies, although it has gone through stages of development in other countries. In the first stage of the widespread use of computers in the sixties of the last century, and then in the seventies, the first treatments for so-called computer crimes appeared. In the eighties of the last century, acts committed in the environment of computers and electronic networks began to be dealt with as a new criminal phenomenon and not just immoral behaviors. Because of the increase in the commission of these crimes, some countries have tended to develop criminal laws for cybercrime, while other countries have left the regulation of these crimes to the general rules contained in their previous criminal laws.

Key Words: Criminal Behavior – Victims – Cybercrime – Regulation – Criminal Laws

المقدمة

مر مفهوم الجريمة الالكترونية بتطور تاريخي تبعاً لتطور التقنية واستخداماتها، ففي المرحلة الاولى من شيوع استخدام الكمبيوتر في الستينات ومن ثم السبعينات ظهرت أول معالجات لما يسمى جرائم الكمبيوتر وكان ذلك في الستينات، واقتصرت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتحسين الالكتروني والاستخدام غير المشروع لبيانات المخزونة في نظم الكمبيوتر وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد عابر أم أنها ظاهرة جرمية مستجدة؟ بل ثار الجدر حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة الكترونية، وبقي التعامل عليها أقرب إلى النطاق الاخلاقي منه إلى النطاق القانوني[١].وفي منتصف السبعينات وبداية الثمانيات من القرن الماضي بدأ التعامل مع الاعمال غير المشروعة التي ترتكب في بيئة الحواسيب والشبكات الالكترونية بوصفها ظاهرة إجرامية جديدة وليست مجرد سلوكيات غير أخلاقية[٢] لذا كان من الضروري التصدي لهذه الظاهرة الخطيرة على الصعيدين التقني والقانوني.فمن الناحية التقنية تركز الاهتمام على أمن البيانات عن طريق استعمال كلمة السر، ولاسيما بالنسبة إلى المستخدم لمنع أي شخص آخر من الاطلاع على البيانات، ثم انتقل الامر لحماية المعلومات من العبث أو التلاعب[٣].ولقد طفا على السطح مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وأنشطة نشر وزراعة الفيروسات التي تقوم بتدمير الملفات أو البرامج، وشاع اصطلاح الهاكرز وهو مصطلح معبر عن مقتحمي النظم الالكترونية وتختلف الجرائم الالكترونية بين دولة وأخرى فما يعتبر جريمة في دولة لا يعد كذلك في دولة أخرى، حيث يشهد العالم في هذه الفترة إزدياداً ملحوظاً لاستخدام تقنية المعلومات في المجتمع في تسيير شؤونه بالمقابل زيادة في الاجرام الالكتروني، وبالنظر لخطورة هذه الجرائم والخسائر الناجمة عنها تظهر أهمية البحث.وبناءاً على ذلك سوف نقسم البحث إلى مبحثين الاول نبين ماهية الجريمة الالكترونية والمجرم الالكتروني والثاني نبين السلوك الاجرامي في الجريمة الالكترونية.

أهمية البحث:

إن أهمية هذا البحث تكمن في حداثة هذه الظاهرة (الجرائم الالكترونية) حيث يشهد العالم في الفترة الراهنة إزدياداً مطرداً لنطاق استخدام تقنية المعلومات في المجتمع والتطور التكنولوجي سيف ذو حدين على الرغم من آثاره الايجابية إلا أن له العديد من السلبيات التي تهدد أمن واستقرار المجتمع حيث من الممكن أن يستخدم لاغراض غير مشروعة تكبد مؤسسات أو شركات كبرى خسائر مالية فادحة.

هدف البحث:

إن الغاية من البحث محاولة بيان الرابطة بين التطور التكنولوجي والجرائم الناتجة عن استخدامه وما هي الطبيعة القانونية لسلوك الجاني في هذه الجرائم الالكترونية.

إشكالية البحث:

إن إشكالية البحث تبدو في أن أغلب الجرائم الالكترونية جرائم خفية يصعب اكتشافها لطبيعة هذه الجرائم التي تتسم بالتعقيد المتزايد الامر الذي يصعب فيه ملاحقة مرتكبيها والكشف عنها ومعاقبة المجرمين لقدرتهم وخبرتهم الفائقة في مجال الالكترونية ولعدم وجود أدلة مادية على المجرمين المعلوماتيين تسهل عملية ملاحقتهم وعدم وجود تشريع خاص بالقانون العراقي يجرم السلوك الاجرائمي الالكتروني.

منهجية البحث:

إن هذا البحث يعتمد على الاسلوب الوصفي التحليلي في جمع وتحليل الحقائق المتعلقة بالجرائم الالكترونية وسلوك المجرم الالكتروني فيها.

خطة البحث:

إن الاحاطة بجميع جوانب موضوع البحث تطلب منا تقسيمه إلى مبحثين الاول بينا ماهية الجريمة الالكترونية والمجرم الالكتروني الذي قسمناه إلى مطلبين: المطلب الاول بينا مفهوم الجريمة الالكترونية وفي المطلب الثاني تكلمنا عن المجرم الالكتروني، أما المبحث الثاني تكلمنا عن السلوك الاجرامي في الجريمة الالكترونية وقسمناه إلى مطلبين: المطلب الاول بينا النشاط الايجابي في جرائم الجريمة الالكتروني والمطلب الثاني تكلمنا عن النشاط السلبي للمجرم الالكتروني في الجريمة الالكترونية.

المبحث الأول ماهية الجريمة الالكترونية والمجرم الالكتروني.

تعتبر الجريمة الالكترونية من الظواهر الحديثة وذلك لارتباطها بتقنية حديثة هي تكنولوجيا المعلومات والاتصالات والكمبيوتر، لذا لم يتفق الباحثون والمختصون في الدراسات القانونية المتعلقة بالجريمة الالكترونية على مصطلح معين فمنهم من يستخدم مصطلح (الجريمة الالكترونية)[٤] وهناك من يطلق على هذا النوع من الجرائم مصطلح جرائم الحاسب الآلي[٥] ويستخدم بعض الفقه مصطلح (الجرائم التكنولوجية) أو (جرائم إستخدام الكمبيوتر) أو (جرائم التقنية العالية) أو (الجرائم المرتبطة بالحاسوب)[٦]، وبناءاً على ذلك سوف نقسم هذا المبحث إلى مطلبين وكالتالي:

المطلب الأول مفهوم الجريمة الالكترونية

إن الجرائم الالكترونية تدخل في إطار دراسة القانون الجنائي الداخلي (الوطني) إذ تعد من الجرائم التي تتخطى حدود الدولة الواحدة، فهي تدخل ايضاً في نطاق دراسات القانون الجنائي الدولي، وتدخل كذلك في إطار الجريمة المنظمة التي تقوم على أساس تنظيم هيكلي وتدريجي له صفة الاستمرارية لتحقيق مكاسب طائلة، وبناءاً على ذلك سنقسم هذا المطلب إلى فرعين وكما يأتي:

الفرع الأول التعريف بالجريمة الالكترونية.

إن الجريمة وفق المفهوم القانوني هي كل فعل أو امتناع يمثل خروجاً على نص من نصوص التجريم يرتب له المشرع عقوبة جزائية[٧]، سواء كان النص المعتبر وارداً ضمن نصوص قانون العقوبات العام[٨]، أو ضمن نصوص القوانين الاخرى ذات الصلة، أو في أي قانون جزائي آخر[٩]، فالمهم أن تكون العقوبة جزائية سواء تمثلت بالسجن أو الحبس أو بالغرامة، وبهذا تتميز عن الجريمة التأديبية والجريمة المدنية، وفي مطلع السبعينات كانت الجريمة الالكترونية محور اهتمام فقهاء القانون الجنائي باعتبارها ظاهرة فرضت ذاتها على المجتمع، لما تنطوي هذه الجرائم على مجموعة من السمات الخاصة، إذ كان ارتباطها عليه بالحاسب الالي مميزاً لها عن غيرها من الجرائم الاخرى التقليدية.ومنذ ذلك التاريخ ونظراً لحداثة الظاهرة نسبياً من ناحية، والتطور المتلاحق الذي يطرأ عليها من ناحية أخرى، فقد بذل الفقه جهوداً في محاولة لوضع تعريف محدد لماهية الجريمة الالكترونية واختلف الباحثون في تقسيم الجرائم الالكترونية باتجاهين هما[١٠]:-

أولاً: الاتجاه الضيق للجرائم الالكترونية.من التعريفات التي وضعها انصار هذا الاتجاه في تعريف الجريمة الالكترونية هي أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً[١١].من خلال هذا التعريف يتضح أنه يقتضي وجود معرفة بتقنية المعلومات ويشترط أن تكون هذه المعرفة أساسية لكي تكون امام جريمة معلوماتية ويجب أن يكون لدى القائمين بالتحقيق والملاحقة القضائية معرفة بتقنية المعلومات، إلا أن هذا الاتجاه يضيق من مفهوم الجريمة الالكترونية، لأن المجرم الالكتروني قد لا يمتلك القدر الكبير من المعرفة والمهارة والخبرة في تقنية المعلومات عند إرتكابه لهذه الجريمة الالكترونية.ومن التعريفات ذات الاتجاه الضيق للجريمة الالكترونية (أنها جريمة ضد المال مرتبطة بالمعالجة الالية للمعلومات)[١٢] وتعرف أيضاً بأنها: (كل سلوك سلبي أو إيجابي يتم

بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأي صورة كانت)[١٣]، كما عُرفت بأنها: كل فعل إيجابي أو سلبي يهدف إلى الاعتداء على تقنية الالكترونية[١٤] وعرفت أيضاً بأنها (الفعل الذي يتم بوساطة اجهزة الكترونية معقدة من أجل إحداث الضرر بالغير)[١٥]. كما عرفها البعض على انها : (الاعمال التي تنطوي على استخدامات اجرامية للانترنت او لانظمة اخرى متصلة بشبكة الانترنت بهدف الحاق الضصرر بالاخرين)[١٦].يتبين عدم قابليتها لان تكون جامعة لذا يمكن ملاحظة أن التعريفات السابقة تقصر محل الاعتداء على المال سواء كان مادياً أو معنوياً، وتشترط أن يكون الفعل عمدياً ويحدث الضرر بالغير، بينما أنه مجرد تعريض لمصلحة قانونية للخطر قد يشكل جريمة، إذ أن محل الجريمة الالكترونية لا يشترط أن يكون مالاً فقد يكون محل الجريمة شخصاً، فقد يستخدم المجرم الالكتروني الحاسوب وشبكات الاتصال للاعتداء على حياة الاشخاص أو على حرمة حياتهم الشخصية أو قد ينتهك عرضهم أو يطال من سمعتهم، كما أنه لا يشترط أن تكون الجريمة عمدية فقد تكون غير عمدية إذا انتفى القصد الجرمي لدى الجاني كأن يهمل أو يقصر أو لا يحتاط، ولا يوجه إرادته الوجهة الصحيحة ومثالها أن يقوم شخص بحذف بيانات ومعلومات داخل ذاكرة الحاسوب لشخص آخر عن طريق عدم الانتباه أو الخطأ.

ثانياً: الاتجاه الموسع للجرائم الالكترونية.

عرف أصحاب الاتجاه الموسع الجريمة الالكترونية بأنها سلوك إجرامي يتم بمساعدة الكمبيوتر، أو هي كل جريمة تتم في محيط أجهزة الكمبيوتر كما عرفها الفقيهان (Micel) و(Credo) وهو إن سوء استخدام الحاسب أو جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته[١٧]، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية، وسواء كان هذا الاعتداء على جهاز الحاسب ذاته أو المعتدات المتصلة به[١٨]، كما عرفت أيضاً بأنها (كل جريمة تتم في محيط الحاسبات الالية)[١٩]، وقد وجه احد الكتاب هذا الاتجاه بالقول إن هذا الاتجاه يوسع كثيراً من مفهوم الجريمة الالكترونية[٢٠].فوفقاً لهذه التعريفات أن مجرد إرتكاب السلوك الاجرامي في محيط الحواسيب يضفي على هذا السلوك وصف الجريمة الالكترونية، لكن هذا لا يمكن التعويل عليه لان الحاسوب قد يكون في بعض الجرائم محلاً لارتكاب الجريمة كسرقة حاسوب مثلاً ومع ذلك تبقى الجريمة اعتيادية ولا يمكن وصفها بالجريمة الالكترونية، وكذلك إذا كانت إحدى مكونات الحاسب المادية محل للجريمة كالشاشة أو لوحة المفاتيح أو الطابعة[٢١]، ولا يمكن إطلاق وصف الجريمة الالكترونية على الجريمة التي يكون محلها حاسوب أو إحدى مكوناته المادية.ولمنطقية هذه الانتقادات نميل إلى تأييد هذا الرأي، حيث يجب أن التمييز بين الجريمة التي يكون النظام الالكتروني محلاً لها وبين الجريمة التي يكون النظام الالكتروني هو أداة الجريمة ووسيلة لتنفيذها.ففي الجريمة الاولى قد لا تكون أمام جريمة معلوماتية وإنما جريمة اعتيادية، كسرقة الحاسوب أو الطابعة، أما الجريمة الثانية عندما يكون محل الاعتداء هو أحد المكونات المعنوية للنظام الالكتروني أو كان هو أداة للجريمة أو وسيلة لتنفيذها فهنا نكون أمام جريمة معلوماتية، فالشخص الذي يتلاعب بمعلومات حاسب شخص آخر أو يهدد شخص يعد مرتكب لجريمة معلوماتية ويعد مجرم معلوماتي.

الفرع الثاني خصائص الجريمة الالكترونية.

تتميز الجريمة الالكترونية بخصائص تميزها عن الجريمة التقليدية حيث أن الجريمة الالكترونية ما هي إلا نتيجة للتطور التقني والعلمي في مجال الحاسوب وشبكات الالكترونية، لذلك فإن هذا التطور هو الذي منح هذه الجريمة بعض المميزات، ومن أبرزها ما يأتي:

أولاً: وسيلة ارتكاب الجريمة الالكترونية.تُعرف الوسيلة التي يرتكب بها النشاط الاجرامي بأنها كل شيء أو آلة تدخل أو تتوسط بين الإرادة الاجرامية وإرتكاب الجريمة أو بعبارة أخرى كل ما يمكن أن يلجأ إليه الجاني ويستعمله لتحقيق إرادته الاجرامية[٢٢].إن الجريمة الالكترونية تتميز بخاصية تميزها عن بقية الجرائم وهي ان وسيلة ارتكابها كثيراً ما تكون جهاز حاسوب[٢٣]، فهي تتطلب توافر جهاز حاسوب يستخدم كأداة لارتكاب هذه الجريمة[٢٤]، وأن جانب من الفقه يعد الحاسب الوسيلة الوحيدة لارتكاب الجريمة الالكترونية، مع أن ارتكاب الجرائم الالكترونية قد يتم عن طريق اجهزة الكترونية أخرى غير الحاسوب كالهاتف المحمول، إذ يمكن الاشتراك عن طريق المحمول بالشبكات الالكترونية، سواء كانت محلية أو دولية كالإنترنيت، وبعد ذلك يكون الهاتف المحمول وسيلة لتنفيذ الجريمة[٢٥].إذ يمكن إستخدام الحاسوب أو أي جهاز الكتروني لتنفيذ الجريمة الالكترونية، حيث أن الجريمة الالكترونية تتطلب بعض المعرفة الفنية أو التقنية البسيطة في مجال الحاسوب[٢٦].

بالاضافة إلى أنه هناك مكاتب متخصصة على شبكة الانترنيت تقوم بارتكاب جرائم معلوماتية على نطاق واسع ويساعدها القراصنة للقيام بهذه الجرائم مقابل أموال[٢٧]، ويبدو الامر أكثر صعوبة وتعقيد عندما يقوم القراصنة باختراق شبكات المعلومات في دول لا تتضمن قوانينها نصوصاً جزائية تجرم ذلك[٢٨].

ثانياً- صعوبة اكتشاف الجريمة الالكترونية واثباتها. من الخصائص التي تتميز بها الجريمة الالكترونية عن الجريمة التقليدية هو صعوبة اكتشافها واثباتها ويرى البعض[٢٩] ، ان من الاسباب التي وراء صعوبة اكتشاف هذه الجرائم يرجع الى تميزها بانه لايشوب ارتكابها اي عمل من اعمال العنف كما انها لا تترك اثارا وانما يتمثل مظهرها في تغيير او محو الارقام والبيانات الموجودة بانظمة الحاسب الالي ولا تترك اثرا خارجيا مرئيا او ملموسا. بينما هناك من يرفض هذا الرأي المتقدم على اطلاقه[٣٠] اذ لا يقتصر أثر الجرائم الالكترونية على تغيير او محو الارقام والبيانات من الملفات المخزنة في ذاكرة الحاسبة بل انه حتى في هذه الحالات مجرد التغيير او محو هذه البيانات يعد اثرا على ارتكاب الفعل فصعوبة اكتشافها يرجع الى عده اسباب من بينها وسيلة تنفيذها والتي تتسم بالطابع التقني بالاضافة الى الاحجام عن الابلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم ونحن نؤيد هذا الرأي بالاضافة الى ان هناك خاصية مميزة للجريمة الالكترونية من حيث صعوبة اثباتها هي سرعة ضياع الدليل واتلافه وصعوبة استرجاعه بالاضافة الى انها جريمة عابرة للحدود.

المطلب الثاني مفهوم المجرم الالكتروني

بعد أن بينا المقصود بالجريمة الالكترونية وخصائصها سوف نبين في هذا المطلب مفهوم المجرم الالكتروني.تتميز شخصية المجرم بمرتكب الجريمة الالكترونية بخصائص وصفات تختلف عن مرتكب الجرائم التقليدية الأخرى وهذا مرجعه تميز شخصية مرتكب الجرائم الالكترونية بالتقدم في مجال استخدام الحاسب الالي ضمن الناحية الجنائية تعني تسمية (المجرم الالكتروني) ذلك الشخص الذي يمتلك مهارات تقنية أو دراية بالتكنيك المستخدم في نظام الحاسوب الالكتروني، والقادر على هذا التكتيك لاختراق (الكود) السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحاسبات عن طريق استخدام الحاسوب ذاته[٣١].وبناءاً على ذلك سنقسم هذا المطلب إلى فرعين وكما يأتي:

الفرع الأول التعريف بالمجرم الالكتروني

إن خبراء الحاسوب والانترنيت والعديد من كتاب القانون في هذا المجال ذهبوا إلى أن المجرم الالكتروني يظهر بأحد الصورتين الاولى هي (Hacrers) وأن تسمية (الهاكرز) تعود إلى ستينات القرن الماضي، إذا أطلقت على الشخص الذي لديه قدرات متميزة في مجال الحاسوب، مستغلة برامجه أقصى استغلال، وفي مطلع الثمانينات تمت أول عملية اعتقال (هاكرز) في الولايات المتحدة الامريكية ومن ثم صدر قانون (السيطرة على الجريمة الكاملة)، والذي أتاح للشرطة الامريكية القبض على منفذي عمليات الاحتيال المتعلقة بالبطاقات الائتمانية والكمبيوتر، أما في أواخر الثمانينات، فقد صدر قانون جديد في الولايات المتحدة الامريكية عُرف بـ(قانون الاحتيال بالكمبيوتر وسوء الاستخدام) والذي زاد من سلطات الشرطة الفدرالية قياساً بالقانون الاول، غير أن هجمات (الهاكرز) باتت تتزايد مع تزايد المواقع الالكترونية[٣٢].أما الصورة الثانية فهي (Cracker) وهم ممن تعكس اعتداءاتهم ميولاً إجرامية خطيرة وهذا المعيار تعتمد عليه التشريعات الأمريكية في التمييز بين النوعين من المجرمين[٣٣]، فيما يميل البعض إلى تسمية المجرم الالكتروني بالمجرم الالكتروني الرقمي ويعرفه بأنه من لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسب الالكتروني أو الرقمي وملحقاته ووسائل الاتصال الرقمية ويتميز المجرم الالكتروني عن غيره من المجرمي التقليديين بعدة مميزات وكما يأتي:

أولاً: سمات المجرم الالكتروني.ان ارتباط الجريمة الالكترونية بالحاسب الالي ميزها عن الجريمة التقليدية لكن لم يقتصر اثر ذلك على الجريمة الالكترونية وانما كان اثره في تمييز المجرم الالكتروني عن المجرم التقليدي[٣٤] واختلف الفقه في تحديد السمات ومن ابرزها:-

١- أن المجرم الالكتروني مجرم ذكي، إذ أن الاجرام الالكتروني هو إجرام الاذكياء، فمن يستعين بالكمبيوتر من أجل سرقة مصرف أو مال شركة هو مجرم على درجة من الذكاء، حيث أن له القدرة على التغلب على الصعاب الفنية التي تواجهه في جريمته الالكترونية[٣٥]، بينما من يسرق منزلاً أو سيارة مجرم منخفض الذكاء في الكثير من الاحيان.

٢- مجرم غير عنيف: إن الاجرام الالكتروني بإتلاف المعلومات لا يتطلب عنفاً، كونه من تقنيات التدمير الناعمة التي تتمثل في التلاعب بالمعلومات أو الكيانات المنطقية والبيانات[٣٦] وما شابه من الجرائم الالكترونية التي تمثل سلوك الجاني فيها بشكل معالجة فنية هادئة

للمعطيات الالكترونية التي تتم بهدوء وبروية ومن دون أي عنف[٣٧] لكن من المتصور أن يقوم عنف عند الاعتداء على مكونات الحاسب الالي فسرقة لوحة مفاتيح أو شاشة.

٣- التخصص في الاجرام الالكتروني: أثبتت العديد من الدراسات في هذا المجال أن المجرمين في مجال الجريمة الالكترونية في الغالب لا يرتكبون سوى هذا النوع من الجرائم لتخصصهم في إرتكابها[٣٨].

٤- المجرم الالكتروني مجرم عائد: إذ غالباً ما يعود المجرم الالكتروني إلى ارتكاب الجريمة مرة أخرى من أجل سد الثغرات التي أدت إلى التعرف عليهم ومن ثم كشف جرائمهم وتقديمهم إلى القضاء.

٥- الاحتراف: المجرم الالكتروني مجرم محترف لما يتطلبه هذا النوع من الجرائم من مهارة فنية عالية لا يستطيع الشخص المبتدئ القيام بها، إذ أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر الذي يتطلب الكثير من الدقة والمهارة والاحترافية في هذا المجال للتغلب على الصعاب والعقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية[٣٩]، وهذا الاحتراف أو المهارة يكتسبها المجرم الالكتروني أما من الدراسة في مجال التكنولوجا المعلومات أو عن طريق الخبرة العملية في هذا المجال[٤٠].

٦- مجرم متكيف اجتماعياً: المجرم الالكتروني إنسان اجتماعي فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به[٤١] بل هو متكيف اجتماعياً لكونه إنسان ذكي[٤٢] فإن الكثير من الجرائم الالكترونية ما ترتكب بدافع الكبرياء كالمستخدم المطرود من عمله أو بدافع الاحتيال أو اللهو أو لاظهار مدى ما يتمتع به المجرم من مهارة واحترافية في مجال الالكترونية والتقنية[٤٣].

ثانياً: دوافع المجرم الالكتروني.

إن دوافع المجرم المعلومات لا تكاد تختلف كثيراً عن دوافع المجرم التقليدي من حيث المبدأ مع الإشارة إلى أن هذه الدوافع لا تؤثر في التكيف القانوني للجريمة في ظل العديد من التشريعات الجنائية، إذ لا عبرة بالبواعث ولاشك في أن أبرز دوافع هذا النوع من الاجرام تتجلى في السعي إلى تحقيق الارباح المالية والاحقاد الشخصية والدوافع السياسية وتحديد النظام الالكتروني والتسلية وكما يأتي:

١- السعي إلى تحقيق الارباح المالية: أن معظم الدراسات أثبتت أن سعي المجرمين المعلوماتيين يأتي في مقدمة الدوافع وراء ارتكابهم الجرائم الالكترونية هو السعي لتحقيق المال، حتى أن أبرز القطاعات المستهدفة من هذه الجرائم هي البنوك التي تعتمد على نظام التمويل الذاتي (EFT)، وشركات التأمين[٤٤].

٢- الانتقام والاحقاد الشخصية: إذ أن المجرمون المعلوماتيين في هذه الحالة ينتقمون من المؤسسة الذي يعملون فيها ويعمدون إلى اختراق انظمتها الالكترونية، أما سبب سوء المعاملة أو بسبب قلة أجورهم فيها (مجرمون معلوماتيون) الذين يكونوا خارج المؤسسة كالمطرودين من العمل فيها والمستغنين عن خدماتهم[٤٥].

٣- الدوافع السياسية: كثيراً ما تنشأ حرب سياسية الكترونية بين الدول ولاسيما في حالات الحروب والخلافات السياسية حيث تخترق المواقع الالكتروني للدول المتحاربة ويتم التجسس عبر الانترنيت الذي أصبح من الوسائل المخابراتية أو تدمير المواقع الرسمية أو إيقافها فهنا الدوافع لارتكاب هذه الجرائم الالكترونية تكون سياسية.

٤- تحدي النظام الالكتروني: كثيراً ما تعمل إدارات المواقع الالكترونية على تأمين مواقعها بشكل كبير وذلك من خلال تعقيد الارقام السرية وتغييرها باستمرار (نظام التشفير) وبالمقابل هذا يحفز المجرمين المعلوماتيين على تحدي أنظمة المواقع.

٥- اللهو والولع بالانظمة الالكترونية: إذ يعمد بعض المجرمين المعلوماتيين ممن لديهم شغف بالانظمة الالكترونية إلى محاولة إظهار تفوقهم ومهارتهم التقنية.

الفرع الثاني تصنيف اشخاص المجرمين المعلوماتيين.

تتدرج الجرائم في مجال الحاسب الالي إلى الجرائم البسيطة إلى الجرائم الارهابية وذلك تبعاً لشخصية المجرم الالكتروني وبما لديه من خبرة في مجال استخدام جهاز الحاسب الالي والغرض من ارتكاب الجريمة لذا تعددت تقسيمات المجرمين المعلوماتيين من حيث السن والخبرة، والمجرمون المحترفون، والهواة المبتدئون، ومن حيث الاستخدام والبرمجة ومن حيث أماكن العمل[٤٦] ونتناولهم بشيء من التفصيل على النحو التالي:

أولاً: من حيث السن والخبرة.لعل هذا التقسيم هو الاقدم بن تقسيمات المجرمين المعلوماتيين وهو ينقسم إلى:

١- الهواة والمبتدئون: يعتبر نمط الهواة والمبتدئين من الانماط التي تتميز بخطورتها في إرتكاب الجرائم على الرغم من سلامة القصد لديهم أي عدم ارتكاب أي من هذه الجرائم، وهذا مرجعه لأن عدم الدراية والخبرة في استخدام الحاسب الالي يترتب عليه الوقوع في الكثير من الاخطاء التي يترتب عليها حدوث تلك الجرائم ويطلق بعضهم على هذه الفئة تسمية المتلعثمين[٤٧] فيما يطلق بعضهم الاخر تسمية بالمجانين[٤٨] وسماهم آخرون الشباب حديثوا العهد بالالكترونية[٤٩] أو الهواة[٥٠] أو العابثون[٥١] أو المخترقون[٥٢].

٢- المجرمون المحترفون: تعد فئة المجرمين المحترفين من أخطر الفئات التي ترتكب الجرائم هذه الطائفة يُطلق عليهم اسم (الكاكرز) وأغلبهم ممن تجاوزت أعمارهم (٢٥) عاماً ويتميزون بالتخصيص العالي في مجال الحاسب الالي والتقنية ويتمتعون بالذكار، وتدل جرائمهم على خطورة إجرامية[٥٣].

ثانياً: تقسيم المجرمين المعلوماتيين إلى مستخدمين ومبرمجين.

ذهب البعض إلى تقسيم المجرمين المعلوماتيين على أساس معيار المعرفة بنظ الالكترونية وكالاتي:

١- المجرمون المستخدمون: تتحدد طبيعة المستخدمين بأنهم طائفة من المجرمين المعلوماتيين هم المستخدمون فقط، ممن تتوافر لديهم المعلومات الكافية عن آلية عمل الحاسوب ومكوناته ووظائفه المحاسبية والتطبيقية والتعليمية المختلفة، ولديهم معرفة بعمل الشبكات الالكترونية، كالموظفين في المؤسسات المالية والبنوك والشركات[٥٤]، ومثال ذلك الموظف الذي يعرف كيف يصل لداخل أنظمة النظام الالكتروني بالتصفح في ملفات المرتبات والاجور عن طريق معرفة كلمة السر (password) ويكون هذا الموظف قد تعرض من قبل لجزاء أو خصم من مرتبه ومن ثم يتولد لديه الرغبة في الانتقام من رب العمل ويكون رد فعله هو إرتكاب إحدى الجرائم من مهاجمة اصول الاموال الخاصة بالمنشأة[٥٥].

٢- مجرمون مبرمجون، تتمتع هذه الطائفة من المجرمين بمستوى عالي من القدرة على دخول أو اقتحام الانظمة الحاسوبية بكل سهولة وغالباً ما تكون الجرائم المرتكبة من قبل هذه الفئة ذات أهمية كبيرة، ويزيد من خطورة هذه الجرائم هو قلة العناصر القادرة على إكتشافها، والمبرمجون قادرون على القيام بتعديل وتحويل ونسخ وإضافة أي معلومات على البرامج، وقدرتهم على إتلاف المعلومات وتغيير محتواها، كل ذلك يتم من خلال استغلال المساحات الخالية بين أوامر برامج الحاسب الالي مع الاستفادة من الاوامر الاخرى لتحقيق مبتغاهم[٥٦].

ثالثاً: من حيث أماكن العمل.

ذهب البعض إلى تقسيم المجرمين المعلوماتيين إلى مجرمين داخل المؤسسة وإلى مجرمين خارج المؤسسة[٥٧] وكالاتي:

١- مجرمون من داخل المؤسسة: إن هذه الفئة هي الاخطر لمعرفتها بنظام المؤسسة والعبث بها ومعرفة نقاط الضعف والقوة بذلك النظام ويتزايد هذا النوع في الولايات المتحدة الامريكية وأوربا مع إزدياد ظاهرة تسريح الموظفين في قطاع تقنية المعلومات والانترنيت بسبب تدهور السوق، مما يؤدي إلى سعي هؤلاء إلى الانتقام من المؤسسة وتحقيق أرباح مالية، ومن أمثلة ذلك قيام مدير لأنظمة الكمبيوتر كان يعمل في إحدى المؤسسات باختراق نظام المؤسسة وتغيير حساب الزبائن وإزالة قواعد بيانات مهمة بحذفها أو إتلافها كل ذلك لانه مستاء من تعامل الشركة معه مما كبد الشركة التي كان يعمل لديها خسائر فادحة أوصلتها إلى الافلاس[٥٨].

٢- مجرمون معلوماتيون من خارج المؤسسة: وهم ثلاث اصناف كما يأتي[٥٩]:

أ- مخترقوا الشبكات (الهاكرز): ويطلق لفظ الهاكرز على المقتحم التقليدي الذي يقوم بالتلصص على الغير ويتاجر في قطاع المعلومات[٦٠]، وهم من يخترقون شبكات الحاسوب مستعينين في ذلك بما لديهم في قدرات متميزة ورغبات جامحة في الاختراق وينقسمون إلى قسمين: الاول هم المخترقون الذين يعملون في إطار منظم لتحقيق اختراق حسابات البنوك أو الشركات التجارية، أما القسم الثاني فهم المجرمون المعتمدون على قدراتهم لاشباع الفضول وإثبات الذات وهؤلاء عندما يصلون إلى غايتهم فإنهم يتركون الشبكة دون العبث ببياناتها وملفاتها ولا يعودون لاختراقها ثانية، إلا بعد تطوير طرق الحماية فيما يبعث فيهم روح التحدي للاختراق هذه الانظمة.

ب- الكراكرز: أما لفظ الكراكرز فيطلق على الشخص المقتحم الخبير في مجال المعلومات واستخدام الحاسب الالي وجرت العادة على أن يطلق على هؤلاء تسمية القراصنة وهؤلاء من نوع الهاكرز[٦١] المتخصصين بفك شفرات البرامج وليس تخريب الشبكة، وهم يقومون بخرق مقاييس الحماية التي تمنع من استنساخ البرامج، فعادة عند شراء أي برنام فإنه يتطلب رقم تسلسلي (serial number) لإتمام عملية تثبيته في الجهاز الشخصي، ومن هنا يقوم هؤلاء بتشغيل برنامج يقوم بتجربة الملايين من الارقام حتى يحصل على الرقم الصحيح ومن ثم استخدامه في تثبيت البرامج المنسوخة، ومن الطرق الاخرى لهذه الفئة من المجرمين المعلوماتيين، خرق الصيغة المكتوبة للبرنامج، إذ يقوم بتغييرها،

ومجرموا هذه الطائفة يقومون بأحد الصورتين الاولى هم من يقومون بهذه الافعال بدوافع تحقيق غايات مالية وأرباح تجارية أو لغرض الشهرة، والثانية تقوم بهذه الافعال بدوافع الاستخدامات الشخصية فقط.

ت- صانعوا الفايروسات: يتمتع هؤلاء المجرمين بمهارات عالية في البرمجة بحيث يستطيعون اختراق الانظمة والقيام بعمليات حسابية لا تنتهي، فيستمر الحاسب الالي في التنفيذ والحساب حتى يستنفذ كل مصادره من ذاكرة رئيسية وثانوية حتى ينهار النظام[٦٢].

المبحث الثاني السلوك الاجرامي للمجرم الالكتروني

إن الركن المادي لأي جريمة يتكون من سلوك أو فعل جرمي والنتيجة المترتبة عليه والعلاقة السببية بين الفعل والنتيجة فالركن المادي للجريمة الالكترونية يتمثل بالسلوك الذي ينهجه المجرم الالكتروني يطلق عليه اسم السلوك الالكتروني ويقصد به ذلك السلوك أو النشاط الذي يقوم به مجرم محترف في مجال التقنية الالكترونية لإرتكابه جريمة الكترونية[٦٣].وعلى هذا الأساس فإن النظام الالكتروني يلعب دوراً رئيسياً ومهماً في أحداث السلوك الالكتروني الذي يتحقق من خلال إرتكاب الجريمة الالكترونية، ولذلك لا يمكن تصور وقوع الجريمة الالكترونية دون هذا النظام، حتى ولو كان هذا النظام هاتفاً محمولاً أو أي جهاز تقني أخر يمكن من خلاله الدخول إلى شبكة الانترنيت، والسلوك المكون للامن المادي أما أن يكون إيجابياً أو سلبياً، ويقصد بالسلوك الاجرامي الالكتروني بمعناه الدقيق الذي يتأتى بحركة جسيمة واضحة في العالم الخارجي بطريق مادي ملموس، وهذا السلوك هو السلوك العام في جميع الجرائم، وما السلوك السلبي إلا استثناء عليه لقصور على بعض الجرائم[٦٤].وهذا ما يسمى بالمفهوم الطبيعي للفعل، والمتمثل في الحركة العضوية، يستلزم جانب نفسي هو إرادة هذه الحركة ومن ثم إرادة الفعل ذاته بعيداً عن النتيجة[٦٥]، إذ أن الفعل الاجرامي يتمثل في مخالفة نصاً قانونياً ينهي ذلك الفعل، أو يأمر بالاتيان به، ولم يات به الفاعل[٦٦] ويتطلب التفرقة فيما إذا كان موضوع الجريمة هو الحاسب الالي وأدواته وما يتصل به من شبكات للربط والطباعة، حيث أن المشرع أضفى عليها الحماية القانونية بنصوص عقابية متعلقة بالسرقة، لانها وقعت على مال مادي منقول مملوك للغير، وبين إتلاف النظم الالكترونية، إذ عالج المشرع العراقي اتلاف الاموال في م(٤٧٧) ق (٤١) كما عالجها المشرع الفرنسي في م(٣٣٤) في قانون العقوبات الفرنسي، وسنقسم المبحث إلى مطلبين:

المطلب الأول السلوك الاجرامي الايجابي.

إن الجرائم الايجابية هي تلك الجرائم التي يكون السلوك المكون لركنها المادي إيجابياً، أي ارتكاب، وتحقق عندما يأتي الجاني عملاً من الاعمال المحرمة قانوناً، مثل جريمة السرقة والقتل...الخ وبناءاً على ذلك سنقسم هذا المطلب إلى فرعين كالاتي:

الفرع الأول الجرائم الماسة بالحياة الخاصة.

إن الحق في الحياة من أهم الحقوق التي حماها المشرع بالنصوص القانونية، سواء في تجريم القتل أو التهديد، أو الضرب، ولكن هناك تبدو الصعوبة في إمكانية وقوعها عبر الانترنت، إذ يصعب وقوع الفعل الاجرامي، ولكن يمكن التهديد بهذا الفعل من خلال الانترنيت، ويمكن الاعتداء على الحياة الخاصة في تصوير أو تسجيل أو بالسب وبالقذف، ويتم ذلك إما في المواجهة المباشرة أو عن طريق الكتابة أو الصور، والجاني هنا هو مستخدم الانترنيت مستخدماً الانترنيت وسيلة لتنفيذ إجرامه، والاعتداء على الغير[٦٧]، فمثلاً جريمة التهديد يتحقق الفعل الاجرامي الالكتروني فيها عندما يكتب المجرم الالكتروني عبارات التهديد وإرسالها إلى الشخص المعني، أو قد يقوم بإرسال صورة توضح نوع التهديد[٦٨] او ابتزاز المجني عليه بصورة عائدة اليه او لغيره مقابل حصوله على المال.

الفرع الثاني الجرائم المتعلقة بالاموال.

إن المشرع لم يقصد الحماية على حياة الاشخاص فحسب، وإنما طالت الحماية القانونية أموالهم، حيث تكفلت النصوص التقليدية العامة بما فيها من الاعتداء، سواء كانت أموال مادية أو معنوية، إذ حمى المشرع الاموال من خلال تجريم السرقة، وقد تحدث السرقة في القضاء الالكتروني، كما هو الحال في سرقة بعض البرامج المصممة أو الاستيلاء على الوسائل العادية الموجودة في البريد الالكتروني للشخص بعد الحصول على كلمة السر أو الحصول على الصور العائلية، إذ أن الجاني في جريمة السرقة يزيل حيازة الشيء بمقتضى نشاط إيجابي يصدر عنه، فيجب أن يكون فعل الجاني هو الذي أنهى الحيازة السابقة وانشأ حيازة جديدة، حيث أن محل الاختلاس يكون مالاً منقولاً، وبالتالي يخرج من هذه الجريمة كل مال غير منقول، والمال وفقاً للقانون هو لكل ما يصلح لان يكون محلاً بحق من الحقوق المالية[٦٩].ولا يشترط في المنقول فضلاً عن قابليته للنقل من مكان لآخر أن يكون ملموساً أو مادياً، فقد استقرت احكام القضاء المصري على إدخال الكهرباء في عداد المنقولات باعتبار أنه من الممكن نقلها من مكان إلى آخر خلال أسلاك مغطاة بمادة عازلة[٧٠].

أما بالنسبة للاشياء المعنوية وتشمل الأفكار والحقوق والمنافع فلا تقع عليها جريمة السرقة لأنها لا تتجسد في كيان مادي فلا يتصور انتزاع حيازتها ومن ثم لا يتصور أن تكون محلاً لجريمة السرقة، لكن يجب التمييز بين الافكار والحقوق والمنافع وهذه لا تقع عليها جريمة السرقة وبين السندات المثبتة لهذه الحقوق التي تسجل أو تحفظ عليها فتعتبر هذه السندات أموال مادية منقولة تصلح لان تكون محل للسرقة، ولكن يثار مشكلة حول مدى تحقق السلوك الاجرامي الايجابي في السرقة على المكونات المعنوية (المال المعنوي) لجهاز الحاسب الالي.إن الرأي المستقر في الفقه متفق في أن كل الاشياء المادية القابلة للانتقال من يد إلى يد تصلح لان تكون محلاً للاختلاس أياً كانت حالتها صلبة أو سائلة أو غازية متى ما تم احرازها[٧١].وفعل الاختلاس يحقق بانتزاع المال من يد الغير بغير رضاه أو علمه، بمعنى إذا لم يتحقق نقل للشيء فلا يتحقق فعل الاختلاس، ولا يتحقق إذا كان الشيء موجود أصلاً في حيازة الجاني، بالمقابل ظهر جانب من الفقه يرى بأن معنى الاختلاس لا يعبر عنه فعل أخذ الشيء أو نزعه أو تقبله وإنما الحيازة في فعل الاختلاس هي الحالة الواقعية التي تخول الشخص سلطة استعمال الشيء أو إتلافه أو التصرف فيه، وهذا يتحقق بسلب الحيازة المادية والمعنوية بدون رضا الحائز أو المالك، فلا عبرة بالحركة المادية.وعليه يمكن القول أن فعل الاختلاس ممكن أن ينطبق على المكونات المعنوية للجهاز الالكتروني وخير مثال سرقة الطاقة الكهربائية، وعليه يمكن القول بإمكانية وقوع فعل الاختلاس على الاشياء المادية والمعنوية[٧٢] إذ أن المكونات المعنوية للحاسب الالي لا تعدو عن كونها بالاساس ذبذبات كهربائية تنتقل عبر الكابلات المعدة لذلك وتترجم من قبل الاقسام المادية الموجودة في الجهاز الالكتروني بمساعدة البرامج لترجم بصورة مفهومة للبشر من خلال وحدات الاخراج، إذ تعد المكونات المعنوية عبارة عن طاقة، وهذه الطاقة يمكن إحرازها وتوجيهها ونقلها من حيز إلى آخر بالإضافة إلى أنها ذات قيمة اقتصادية، فعلى الرغم من احتفاظ صاحب البرامج أو المعلومة بالحيازة إلا أن مسؤولية الجاني تحقق، فالجاني استخدم نشاطه الذهني للاستيلاء على البرامج أو المعلومات، فقد يستخدم حاسة السمع أو النظر، سواء بقراءة المعلومات أو الاستماع إلى برامج صوتية وقام بالاستيلاء على هذه المعلومات وتثبيتها على دعامات وعرضها للبيع أو تداولها على نحو يخالف إرادة مالك المعلومات أو البرام مما يلحق ضرراً به، لانه أصبح هناك من يزاحم مالك البرامج أو المعلومات في حق ملكيته واستغلال المعلومات هذه أو البرامج للحصول على الاموال، بينما هناك من يرى ان اختلاس المعلومات منفصل عن اطارها المادي سواء عن طريق تخزينها او طباعتها لايحقق السرقة لان مالكها لا يتجرد من حيازتها ولا من جميع السلطات التي له عليها فكل ما يقصده هو سرية هذه المعلومات ولهذا فان المعلومات لا يمكن ان تكون محلا للسرقة[٧٣]، ونحن نؤيد القول أن البرامج والمعلومات تصلح أن تكون محلاً لجريمة السرقة كون السرقة تحقق بنشاط الجاني والنشاط الايجابي في هذه الجريمة يتمثل في نسخ البرامج والمعلومات أو تصويرها.

المطلب الثاني السلوك الاجرامي الالكتروني السلبي.

إن مخالفة القواعد القانونية الامرة تعد جريمة، إذ تتصف القاعدة الجنائية بالامر أو النهي، فإذا خالفها الفاعل ولم يمتثل لها، اعتبر مرتكباً لسلوك سلبي في حالة الامر، وسلوك الجاني في حالة النهي، وسنقسم هذا المطلب إلى فرعين:

الفرع الأول السلوك السلبي في الجريمة الالكترونية التي تقع على الانترنيت.

يعد الفعل جريمة إذا امتنع الفاعل عن أداء واجب فرضه القانون، وبصفة خاصة في الجرائم ذات النتائج، أما الجرائم الشكلية التي تقع بالسلوك فقط، بمجرد الامتناع عن اتيان السلوك تقع الجريمة، وإذا امتنع عن اداء السلوك، أو قام بسلوك يخالف بذلك القاعدة القانونية في الجرائم ذات النتائج، إن الجرائم غير العمدية التي تقع بالخطأ أو الاهمال يعاقب المشرع عليها دون تفرقة بين السلوك السلبي أو السلوك الايجابي، وهذا ما جاءت به المادة (٣٥) من قانون العقوبات العراقي التي حددت السبب في إتيان فعل أو الامتناع عنه، وأن الجرائم التي تقع على الانترنيت ومادتيها، أغلبها من الجرائم ذات السلوك الايجابي وهي اغلبها من جرائم النتائج، وإن كانت النتائج محدودة ويصعب كشفها بسهولة، وهذا السلوك الايجابي يمكن أن يقع بالترك، وأن كان البعض يرى أنه يختلف عن الامتناع، إذ أن الترك مرادف للامتناع، فمن يترك سلوكاً أمر به المشرع كمن امتنع بإرادته عن الفعل، ومن جانب آخر أن السلوك الايجابي المحقق بالامتناع أو الترك يقتضي الا يكون الفاعل قد قام بفعل ما يقصد به تحقيق النتيجة التي أرادها، ولولا ذلك لاعتبرت جريمة ايجابية، وهذا ما قصده المشرع في المادة (٣٦٤) من قانون العقوبات بتشديد العقاب على من يتسبب في جرح شخص إذا كان ناشئاً عن إهماله أو عونته أو عدم احترازه، أو امتنع وقت الحادث عن مساعدة المجني عليه أو من وقعت عليه الجريمة أو لم يطلب المساعدة له، وهناك آراء فقهية حول هذا الامر منها:

١- إتجاه يذهب إلى عدم العقاب إذا وقعت النتيجة إثر امتناع يقرره نص فمن يمتنع عن فعل لا يمكن الجزم بقصد ذلك لان الامتناع عدم أو العدم لا يقضي إلا الى عدم.وهذا الاتجاه في الفقه الفرنسي ويستند على أن المشرع لم يجرم بصراحة الفعل إذا قصد الجاني بامتناعه عن

تحقيق نتيجة إجرامية، إلا في المواد (١٥) و(١٦) و(٢٢٧) من قانون العقوبات الفرنسي التي تعاقب من يلحق الأذى بالصغير الذي لم يبلغ (١٥) سنة بالامتناع عن بذل العناية الواجبة، وينتقد بعض الفقه الفرنسي ذلك بأنه لم يكن بحاجة إلى النص لو أنه يعتد بالامتناع إلى جانب الايجاب في وقوع الجرائم وهذا ما أشار عليه القضاء الفرنسي.

٢- إتجاه يذهب إلى امكان وقوع الجرائم الايجابية بطريق الترك، ويرى أنصار هذا الاتجاه أن السبب شأنه شأن الايجاب في التعبير عن الإرادة رغم صعوبة إثبات السببية بين الامتناع أو النتيجة المتحققة، ويشترطون لقيام هذه الرابطة وجود التزام قانوني أو تعاقدي يمنع وقوع النتيجة[٧٤].

٣- أتجاه لا يشترط لوقوع الجرائم الايجابية بالترك أو الامتناع، وجود التزام قانوني بموجب اتفاق لمنع وقوع الجريمة ويرى أنصار هذا الاتجاه أنه لا فرق بين وقوع الفعل عن عمد فتحققت النتيجة وبين الامتناع عن عمل يؤدي إلى تحقق النتيجة ذاتها، فما هوالا صور لنشاط رتب أثراً في العالم الخارجي، كما يرى هذا الاتجاه عدم النظر في توافر القصد كالاتجاه الاول، أو توافرت السببية كالاتجاه الثاني، لعدم الخلط بين أركان الجريمة من ناحية وعناصر الركن الواحد من ناحية أخرى، وعليه فإذا اقتصر التجريم على حالات وجود اتفاق أو التزام قانوني لخرجت حالات عديدة من نطاق التجريم، وبالتالي تهددت المصلحة المحمية.ومن ناحية أخرى أن البحث في توافر القصد من عدمه في حالات الترك أو الامتناع، بحث في توافر اركان الجريمة، وقد تقع الجريمة دون قصد بطريق الخطأ.ومن ناحية أخرى أن البحث في توافر العلاقة السببية من فعل الترك أو الامتناع والنتيجة بحيث في عناصر الركن المادي للجريمة وهو يتحقق بالفعل بين فعل الترك أو الامتناع والنتيجة التي ترتبت عليه كأثر له، وقد تبنى المؤتمر الدولي لقانون العقوبات، الاتجاه الثاني في موضوع جرائم الامتناع.إن الجرائم التي تقع على الانترنيت ومادياته، يمكن أن تقع سلوك الجاني أو الامتناع عن هذا السلوك الايجابي وأن جرائم السرقة والاعتداء على الاموال يمكن تطبيق نصوصها، ويلزم النص على هذه الجرائم صراحة، وفقاً للمشرع والدستور والقانون وشريعة الجرائم والعقوبات لا يجوز القياس بالتجريم، ولكن يجوز القياس في الإباحة لأنها الأصل[٧٥].

الفرع الثاني السلوك السلبي في الجريمة الالكترونية التي تقع من خلال الانترنيت.

إن السلوك الإجرامي السلبي يقع بطريقة سلبية في هذه الحالة لا على الانترنيت وماديات بل بواسطته، أي بإستخدام الحاسب الالي، فيكون هو مصدر الخطر على الاموال والماديات والمصالح المحمية، ومن هذه الجرائم التدوير الذي يقع عليه أو من خلال لمصلحة أشخاص، كما في التنصت على الافراد والاعتداء على حياتهم وأسرارهم الخاصة.إن بعض هذه الصور قد تقع بسلوك سلبي وبعضها يقع بسلوك إيجابي، وبصفة خاصة من جانب متعمد الايذاء الوصول ناقل المعلومات في الانترنيت، وذلك إذا ما علم بوجود هذا السلوك الاجرامي وامتنع عن الابلاغ أو التدخل للحفاظ على حقوق الغير أو للحفاظ على أسرار الدولة في جرائم أمن الدولة[٧٦] ومن جانب آخر فإن هؤلاء يعدون من قبيل الشركاء في الجرائم كل حسب دوره، لكن الجريمة بالنسبة لهم وقتية، فإذا علم أي منهم بالطابع الاجرامي للفعل ولم يتدخل بمجرد علمه يعد شريكاً بالامتناع.فالجريمة مستمرة بالنسبة إلى الفاعل الاصلي صاحب الموقع الالكتروني (web) ومن ناحية أخرى لو علم بالسلوك الاجرامي ولم يتدخل يعد شريكاً إيجابياً ايضاً، لانه ارتضى في هذا السلوك الاجرامي، ولو لم يكن هناك اتفاق مسبق على ارتكاب الجريمة، وهذا ما يحدث في جرائم أمن الدولة بتجريم هذا السلوك حماية للمصلحة المحمية في هذا النوع من الجرائم[٧٧].بالحقيقة إن هذه الجرائم تعد من قبيل جرائم السلوك أو الجرائم الشكلية التي يجرم فيها السلوك فقط لخطورته على المصلحة محل الحماية، وبالتالي فإن هذا السلوك السلبي من جانب متعهد في الايواء أو الوصول يشكل خطراً على المصلحة المحمية، ولكن من ناحية أخرى يلزم النص عليه صراحة، وإلا اصطدمنا بقاعدة شرعية الجرائم والعقوبات.

الخاتمة

إن الجريمة الالكترونية تستخدم الوسائل والتقنيات الحديثة ليس للاتصال بين المجرمين أو شبكات الفساد فقط وإنما أصبحت هذه الوسائل الحديثة تستخدم بذاتها كأداة للجريمة ووسيلة لتنفيذها حيث أن الجريمة الالكترونية باتت من أكبر الخدميات في عالمنا المعاصر لانا تعد صنفاً مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجريم والعقاب والتي تتطلب ضرورة تحقق أركان الجريمة طبقاً لمبدأ الجرائم والتي يتطلب تدخل المشرع والعقوبات ومن خلال بحثنا توصلنا إلى عدة نتائج ومقترحات.

النتائج:

١- الجريمة الالكترونية من الجرائم المستحدثة ولم تعالج في القوانين العقابية في العراق، ولم يألف المجتمع مثل هذه الجرائم.

٢- إن الجريمة الالكترونية تختلف عن الجرائم التقليدية في أسلوب ارتكابها والوسيلة المستخدمة في إرتكبها وأنها من الجرائم الخفية التي يصعب اكتشافها وتحتاج إلى خبراء في هذا المجال من المحققين حيث أن المجرم الالكتروني لا يترك أثراً عند ارتكابه فعله الاجرامي وسهولة اتلاف الدليل.

٣- إن الجرائم الالكترونية كثيرة ومتشعبة منها ما يتعلق بالمساس بالحق العام ومنها بالاشخاص وصورها متعددة كالارهاب والاتجار بالبشر والسرقة واختراق المواقع والسب والقذف فهي جرائم لا يمكن حصرها مع التطور الكبير وأسلوب ارتكابها المتقن بما يمتلكه المبرمجين المعلوماتيين.

المقترحات:

١- أصبحت الحاجة ملحة إلى إقرار مشروع مكافحة الجرائم الالكترونية مع عدم المساس بالحريات الشخصية والتي ينسجم التشريع مع الدستور العراقي لسنة ٢٠٠٥.

٢- إن الجرائم الالكترونية تحتاج إلى وسائل إثبات مختلفة من وسائل الاثبات في الجرائم التقليدية لهذا تحتاج إلى إعادة النظر في قانون الاحوال الجزائية رقم (٢٣) لسنة ١٩٧١ المعدل من حيث التحري عنها وعن الدلالة وجمع الادلة والتحقيق والاحكام اللازمة اتباعها في حال التفتيش على الحاسبات وعند ضبط المعلوات التي تحرز وضبط البريد الالكتروني حتى يستمد الدليل مشروعيته.

٣- لابد من أن تكون هناك حملات توعية واسعة بين أفراد المجتمع من مخاطر استخدام الانترنيت من قبل ضعاف النفوس ومخاطر الاستخدام من قبل الصغار والمبتدئين في أن يقعوا فريسة لافعال المجرمين المعلوماتيين.

٤- يجب البدء بخطوات حقيقية وصحيحة ومدروسة لاقرار مشروع قانون الجريمة الالكترونية.

٥- ضرورة التعاون واقامة الندوات والدورات والورش لتوعية افراد المجتمع كافة عن الجرائم الالكترونية.

٦- ضرورة إشراك المواطنين في مكافحة الجرائم الالكترونية عن طريق إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم ولاسيما الجرائم الاخلاقية ونشر حملات توعوية واسعة عبر وسائل التواصل الاجتماعي.

المصادر

اولاً: الكتب

١. احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري (دراسة مقارنة)، ط١، دار النهضة العربية، القاهرة، ٢٠١٠.
٢. اكرم عبد الرزاق المشهداني، الجريمة التكنولوجية، ط١، شركة الوفاق، بغداد، ٢٠٠١.
٣. أمير فرج يوسف، جرائم تقنية المعلومات بدول الخليج العربي، دار الكتب والدراسات العربية، ٢٠١٦.
٤. ايمن عبد الحفيظ، الاتجاهات الفنية والامنية لمواجهة الجرائم الالكترونية، بدون ناشر، ٢٠٠٥.
٥. توم فوريستر، مجتمع التقنية العالية، قصة ثورة تقنية المعلومات، ط١، ترجمة ونشر المكتب الاردني، عمان، ١٩٨٩.
٦. جلال محمد الزعبي وأسد احمد المناعسة، جرائم تطبيق المعلومات الالكترونية، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠.
٧. جمال إبراهيم الحيدري، شرح احكام القسم الخاص من قانون العقوبات، بيروت، ٢٠١٥.
٨. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة واستخدام الحاسب الالي، دار النهضة العربية، القاهرة، ١٩٩٢.
٩. حنان ريحان مبارك، الجرائم الالكترونية، منشورات الحلبي الحقوقية، بيروت.
١٠. خالد ممدوح إبراهيم، الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩.
١١. رامي متولي القاضي، مكافحة الجرائم الالكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠١١.
١٢. رمسيس بهنام، القسم الخاص في قانون العقوبات، منشأة المعارف، الإسكندرية، ١٩٨٢.
١٣. زين العابدين عواد كاظم الكردي، جرائم الارهاب الالكتروني (دراسة مقارنة)، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٨.
١٤. سامي حامد عباد، الجريمة الالكترونية وجريمة الانترنيت، دار الفكر الجامعي، القاهرة، ٢٠٠٧.
١٥. سعد عبد اللطيف حسن، جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنيت، ط١، دار النهضة العربية، القاهرة، ١٩٩٩.

١٦.شمس الدين إبراهيم احمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال التقنية الالكترونية في القانون السوداني والمصري، ط١، دار النهضة العربية، القاهرة، ٢٠٠٥.
١٧.عادل عازر، النظرية العامة في ظروف الجريمة، المطبعة العالمية، القاهرة، ١٩٦٧.
١٨.عادل يحيى، السياسة الجنائية في مواجهة الجريمة الالكترونية، دار النهضة العربية، القاهرة، ٢٠١٤.
١٩.عادل يوسف الشكري، فن صياغة النص العقابي، منشورات زين الحقوقية، ٢٠١٧.
٢٠.عبد الاحد جمال الدين، النظرية العامة للجريمة، دار الثقافة الجامعية، القاهرة، ١٩٩٦.
٢١.عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون الالكتروني)، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، ٢٠٠٧.
٢٢.عمار عباس الحسيني، جرائم الحاسوب والانترنيت، ط١، مكتبة زين الحقوقية والادبية، ٢٠١٧.
٢٣.غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنيت، ط١، دار الفكر والقانون، المنصورة، ٢٠١٣.
٢٤.مأمون محمد سلامة، قانون العقوبات، القسم العام، ط١، دار الفكر العربي، القاهرة.
٢٥.محمد حماد مرجح الهيتي، التكنولوجيا الحديثة والقانون الجنائي، ط١، دار الثقافة، عمان، ٢٠٠٤.
٢٦.محمد زكي أبو عامر، قانون العقوبات، القسم العام، الدار الجامعية، ١٩٩٣.
٢٧.محمد سامي البنوا، ثورة المعلومات وانعكاساتها على قانون العقوبة، دار النهضة المصرية العامة للكتاب، القاهرة، ٢٠٠٣.
٢٨.محمد عبد الله أبو بكر سلامة، موسوعة الجرائم الالكترونية، جرائم الكمبيوتر والانترنيت، منشأة المعارف، الإسكندرية، ٢٠٠٦.
٢٩.محمد علي العريان، الجرائم الالكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٤.
٣٠.محمد محمود مكاوي، الجوانب الاخلاقية والاجتماعية للجرائم الالكترونية، المكتبة العصرية، المنصورة، ٢٠١٠.
٣١.محمد منير الجنبيهي وممدوح محمد الجنبيهي، جرائم الانترنيت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥.
٣٢.محمود احمد عناينة، جرائم الحاسوب وابعادها الدولية، دار الثقافة، عمان، ٢٠٠٥.
٣٣.محمود محمود مصطفى، شرح قانون العقوبات، القسم الخاص، القاهرة، ١٩٨٦.
٣٤.مصطفى محمد موسى، اساليب إجرامية بالتقنية الرقمية –ماهيتها، مكافحتها (دراسة مقارنة)، دار الكتب القانونية، القاهرة، ٢٠٠٥.
٣٥.نائلة عادل محمد فريد، جرائم الحاسب الالي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ٢٠١٢.
٣٦.سليمان عبد المنعم، علم الاجرام والجزاء، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠٠٥.
٣٧.هلالي عبد الله احمد، التزام الشاهد بالإعلام في جرائم الالكترونية (دراسة مقارنة)، ط٢، الحصري للطباعة والكمبيوتر، ٢٠٠٨.

ثانياً: الرسائل الجامعية

١. محمد حسن الصواف، النظرية العامة للتمييز بين الجريمة الإيجابية والجريمة السلبية في القانون المقارن، اطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ١٩٩١.

ثالثاً: البحوث

٢. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية الصادرة عن كلية الحقوق، جامعة الإسكندرية، العدد الرابع والعشرون، ١٩٩٢.
٣. يونس عرب، جرائم الكمبيوتر والانترنيت، ورقة عمل مقدمة إلى مؤتمر الامن العربي الذي نظمه المركز العربي للدراسات والبحوث الجنائية المنعقد في أبو ظبي، ٢٠٠٢/١٢/٢.

رابعاً: القوانين

١. قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.
٢. قانون الجرائم الاقتصادية العراقي رقم (١١) لسنة ١٩٩٣.
٣. قانون العقوبات العسكري العراقي رقم (١٩) لسنة ٢٠٠٧

خامساً: المصادر الاجنبية

1. Joshua B. Hill, Nancy E. Marion, Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century, Praeger, 2016, P14.

---

(١) خالد ممدوح إبراهيم، الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩، ص٧١.

(٢) يونس عرب، جرائم الكمبيوتر والانترنيت، ورقة عمل مقدمة إلى مؤتمر الامن العربي الذي نظمه المركز العربي للدراسات والبحوث الجنائية المنعقد في أبو ظبي، ٢٠٠٢/١٢/٢.

(٣) محمود احمد عنابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ص٣.

(٤) محمد عبد الله أبو بكر سلامة، موسوعة الجرائم الالكترونية، جرائم الكمبيوتر والانترنيت، منشأة المعارف، الإسكندرية، ٢٠٠٦، ص٦٩، عمار عباس الحسيني، جرائم الحاسوب والانترنيت، ط١، مكتبة زين الحقوقية والادبية، ٢٠١٧، ص٣٥.

(٥) محمود أحمد عبابنة، المصدر السابق، ص١١، هلالي عبد الله احمد، التزام الشاهد بالإعلام في جرائم الالكترونية (دراسة مقارنة)، ط٢، الحصري للطباعة والكمبيوتر، ٢٠٠٨، ص١٣.

(٦) اكرم عبد الرزاق المشهداني، الجريمة التكنولوجية، ط١، شركة الوفاق، بغداد، ٢٠٠١، ص١٣.

٧ سليمان عبد المنعم، علم الاجرام والجزاء، منشورات الحلبي الحقوقية، ط١، ص٨٩، ٢٠٠٥.

(٨) قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

(٩) قانون العقوبات العسكري العراقي رقم (١٩) لسنة ٢٠٠٧ وقانون الجرائم الاقتصادية العراقي رقم (١١) لسنة ١٩٩٣.

١٠ نائلة عادل، جرائم الحاسب الالي الاقتصادية، منشورات الحلبي الحقوقية، ص٢٨، ٢٠١٢.

(١١) محمود احمد عبابنة، المصدر السابق، ص١٦، علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية الصادرة عن كلية الحقوق، جامعة الإسكندرية، العدد الرابع والعشرون، ١٩٩٢، ص٢٦٩-٢٧٠.

(١٢) أكرم عبد الرزاق المشهداني، المصدر السابق، ص١٤.

(١٣) محمد حماد مرجح الهيتي، التكنولوجيا الحديثة والقانون الجنائي، ط١، دار الثقافة، عمان، ٢٠٠٤، ص١٥٢، وعمار عباس، المصدر السابق، ص٤٠.

(١٤) محمد علي العريان، الجرائم الالكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٤، ص٤٥.

(١٥) شمس الدين إبراهيم احمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال التقنية الالكترونية في القانون السوداني والمصري، ط١، دار النهضة العربية، القاهرة، ٢٠٠٥، ص١٠٢.

16 16 – Joshua B. Hill, Nancy E. Marion, Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century, Praeger, 2016, P14.

(١٧) خالد ممدوح إبراهيم، الجرائم الالكترونية، المصدر السابق، ص٧٤.

(١٨) محمد علي العريان، المصدر السابق، ص٤٤-٤٥، عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، ٢٠٠٧، ص٥٣.

(١٩) محمد عبد الله أبو سلامة، المصدر السابق، ص١٣.

(٢٠) محمد عبد الله أبو سلامة، المصدر ذاته، ص١٣.

(٢١) زين العابدين عواد كاظم الكردي، جرائم الارهاب المعلوماتي (دراسة مقارنة)، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٨، ص٧٨.

(٢٢) عادل عازر، النظرية العامة في ظروف الجريمة، المطبعة العالمية، القاهرة، ١٩٦٧، ص١٦٢.

٢٣ عمار عباس الحسيني، جرائم الحاسوب والانترنت، منشورات زين الحقوقية، بيروت، ط١، ص٤٨، ٢٠١٧.

(٢٤) محمد أحمد عبابنة، المصدر السابق، ص٣٥-٣٦.

(٢٥) محمد حماد مرهج الهيتي، المصدر السابق، ص١٤١.

(٢٦) محمد منير الجنبيهي وممدوح محمد الجنبيهي، جرائم الانترنيت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥، ص١٤.

[٢٧] محمود احمد عبابنة، المصدر السابق، ص٣٧.

[٢٨] خالد ممدو، الجرائم الالكترونية، المصدر السابق، ص٨٤.

[٢٩] عمار عباس، المصدر السابق، ص٥٢.

[٣٠] نائلة عادل، المصدر السابق، ص٤٩.

[٣١] هدى حامد قشقوش، المصدر السابق، ص٣٢.

[٣٢] عمار عباس الحسيني، المصدر السابق، ص٥٩.

[٣٣] احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري (دراسة مقارنة)، ط١، دار النهضة العربية، القاهرة، ٢٠١٠، ص٢١، رامي متولي القاضي، مكافحة الجرائم الالكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠١١، ص٥٥، وسامي حامد عباد، الجريمة الالكترونية وجريمة الانترنيت، دار الفكر الجامعي، القاهرة، ٢٠٠٧، ص٤٩.

[٣٤] نائلة عادل، المصدر السابق، ص٥٦.

[٣٥] رامي متولي القاضي، مكافحة الجرائم الالكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠١١، ص ٥٥. وأيضاً: سامي علي حامد عياد، الجريمة الالكترونية وجريمة الإنترنت، دار الفكر الجامعي، القاهرة، ٢٠٠٧، ص ٤٩.

[٣٦] عمار عباس الحسيني، المصدر السابق، ص٦١.

[٣٧] محمد سامي البنوا، ثورة المعلومات وانعكاساتها على قانون العقوبة، دار النهضة المصرية العامة للكتاب، القاهرة، ٢٠٠٣، ص٤٩-٥٠.

[٣٨] مصطفى محمد عوسي، أساليب إجرامية بالتقنية الرقمية ماهيتها –مكافحتها (دراسة مقارنة)، دار الكتب القانونية، القاهرة، ٢٠٠٥، ص١٦.

[٣٩] عادل يحيى، السياسة الجنائية في مواجهة الجريمة الالكترونية، دار الهضة العربية، القاهرة، ٢٠١٤، ص٥٩.

[٤٠] عادل يحيى، المصدر نفسه، ص٥٩.

[٤١] سامي علي حامد عياد، المصدر السابق، ص٥٠.

[٤٢] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنيت، ط١، دار الفكر والقانون، المنصورة، ٢٠١٣، ص٤-٥.

[٤٣] رامي متولي القاضي، المصدر السابق، ص٥٥.

[٤٤] عمار عباس الحسيني، المصدر السابق، ص١٧، ٢٠.

[٤٥] خالد ممدوح ابراهيم، المصدر السابق، ص١٤١.

[٤٦] ايمن عبد الحفيظ، الاتجاهات الفنية والامنية لمواجهة الجرائم الالكترونية، بدون ناشر، ٢٠٠٥، ص٢٥ وما بعدها.

[٤٧] توم فوريستر، مجتمع التقنية العالية، قصة ثورة تقنية المعلومات، ط١، ترجمة ونشر المكتب الاردني، عمان، ١٩٨٩، ص٤٠٧.

[٤٨] محمد محمود مكاوي، الجوانب الاخلاقية والاجتماعية للجرائم الالكترونية، المكتبة العصرية، المنصورة، ٢٠١٠، ص٤٥.

[٤٩] محمد علي العريان، المصدر السابق، ص٦٣.

[٥٠] جلال محمد الزعبي وأسد احمد المناعسة، جرائم تطبيق المعلومات الالكترونية، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠، ص١٤.

[٥١] منير محمد الجنبيهي وممدوح الجنبيهي، المصدر السابق، ص٥١.

[٥٢] محمود احمد عبابنة، المصدر السابق، ص٤٠-٤١.

[٥٣] محمد محمود مكاوي، مصدر سابق، ص٤٧-٤٨، ايمن عبد الحفيظ، المصدر السابق، ص٣٤.

[٥٤] عمار عباس الحسيني، المصدر السابق، ص٧٠.

[٥٥] خالد ممدوح إبراهيم، المصدر السابق، ص١٤٧.

[٥٦] عمار عباس الحسيني، المصدر السابق، ص٧١.

[٥٧] مصطفى محمد موسى، اساليب إجرامية بالتقنية الرقمية –ماهيتها، مكافحتها (دراسة مقارنة)، دار الكتب القانونية، القاهرة، ٢٠٠٥، ص٢٤-٢٧.

[٥٨] عمار عباس الحسيني، مصدر سابق، ص٧٢.

[٥٩] خالد ممدوح إبراهيم، مصدر سابق، ص١٤٤.

[٦٠] خالد ممدوح، المصدر السابق، ص١٤٥.

[٦١] عمار عباس الحسيني، المصدر السابق، ص٧٣.

[٦٢] خالد ممدوح إبراهيم، مصدر سابق، ص١٤٨.

[٦٣] أمير فرج يوسف، جرائم تقنية المعلومات بدول الخليج العربي، دار الكتب والدراسات العربية، ٢٠١٦، ص٢٣٩.

[٦٤] محمد حسن الصواف، النظرية العامة للتمييز بين الجريمة الإيجابية والجريمة السلبية في القانون المقارن، اطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ١٩٩١، ص١٣٥.

[٦٥] امير فرج يوسف، المصدر السابق، ص٢٤٥، مأمون محمد سلامة، قانون العقوبات، القسم العام، ط١، دار الفكر العربي، القاهرة، ص١٢٨.

[٦٦] عبد الاحد جمال الدين، النظرية العامة للجريمة، دار الثقافة الجامعية، القاهرة، ١٩٩٦، ص٣١١.

[٦٧] سعد عبد اللطيف حسن، جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنيت، ط١، دار النهضة العربية، القاهرة، ١٩٩٩، ص٢٢٨.

[٦٨] أمير فرج يوسف، المصدر السابق، ص٢٤٣.

[٦٩] محمد زكي أبو عامر، قانون العقوبات، القسم العام، الدار الجامعية، ١٩٩٣، ص٦١.

[٧٠] رمسيس بهنام، القسم الخاص في قانون العقوبات، منشأة المعارف، الإسكندرية، ١٩٨٢، ص٤٣٩.

[٧١] محمود محمود مصطفى، شرح قانون العقوبات، القسم الخاص، القاهرة، ١٩٨٦، ص٤٦٦.

[٧٢] حنان ريحان مبارك، الجرائم الالكترونية، منشورات الحلبي الحقوقية، بيروت، ص١٥٩.

[٧٣] نائلةعادل، المصدق السابق، ص١٥٩.

[٧٤] جمال إبراهيم الحيدري، شرح احكام القسم الخاص من قانون العقوبات، بيروت، ٢٠١٥، ص١٨٣ ؛ المادة ٣٤ من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩.

[٧٥] عادل يوسف الشكري، فن صياغة النص العقابي، منشورات زين الحقوقية، ٢٠١٧، ١٣٣.

[٧٦] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة واستخدام الحاسب الالي، دار النهضة العربية، القاهرة، ١٩٩٢، ص١٣٧.

[٧٧] مأمون محمد سلامة، المصدر السابق، ص٤١.