عنوان البحث

الإشكاليات التطبيقية للجريمة الإلكترونية – دراسة مقارنة

اسم الباحث: محمد سالم عبد العالي محمود

Researcher name: MOHAMMED SALIM ABDULALI MAHMOUD

الدرجة العلمية : محاضر كلية الشريعة والقانون

الملخص

يؤدى انتشار الجرائم الإلكترونية في المُجتمعات إلى الكثير من المخاطر والتهديدات، ومنها المساس بالاقتصاد والأمن الوطني وتهديده، وذلك بسبب الكثير من النتائج التي تسببها بعض أنواع الجرائم الإلكترونية كالتشهير ببعض الأفراد ونشر الأخبار الكاذبة والإشاعات ، وكلما ازداد الاعتماد على الحاسبات في المجلات الاقتصادية والإدارية ازدادت مخاطر الغش والتجسس والسرقة والإتلاف ألعمدي، وغير ذلك من الجرائم، وما يزيد من خطورة هذا النوع الجديد من الجرائم أنها قد تتعدى حدود المكان، ويصعب بالنسبة لها حساب الزمان.

كلمات مفتاحيه :– دليل رقمي– جرائم الإنترنت – الدليل الإلكتروني . مسرح الجريمة الإلكتروني – الإجرام المعلوماتي .

Summary

The spread of electronic crimes in societies leads to many risks and threats, including harming and threatening the economy and national security, due to many of the consequences caused by some types of electronic crimes, such as defaming some individuals and spreading false news and rumours. The greater the reliance on computers in economic and administrative journals, the greater the risk of fraud. Espionage, theft, intentional destruction, and other crimes. What increases the seriousness of this new type of crime is that it may exceed the boundaries of place, and it is difficult for them to calculate time.

مقدمة

الحمد لله رب العالمين والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آلِه وصحبه أجمعين.

وبعد

إنَّ أهم ما يجب النظر فيه مِن خلال التَّمعُّن في أنظمة المجتمع، هي تلك الأنظمة التي تظهر في حركته وسيره، سواء أكانت الخارجية منها أو الداخلية، مثل أنظمة العلاقات مع الأمم الأخرى، أو النظم الحكومية الإدارية، أو التشريعية القانونية والقضائية، وكلها تدور في فلك التشريعات، التي هي من أهم، وأخطر ما يجب مراجعتها ونقدها، ومن ثَمَّ يتمُّ التقويم والتقييم لتِلك التَّشريعات، فالنظم والتشريعات محدِّدات للمجتمع؛ فهي التي توجه حركته، وتضبط آلية انتقاله وسيره؛للوصول إلى الوطر المنشود، وعندئذ يتحقق الاستقرار عبر ميزان العدالة، الذي جاءت التشريعات القانونية والقضائية لإقامته.

ومن هنا...من هذا المنطلق، تأتي الدراسة البحثية العلمية، باعتبارها وسيلة فاعلة من وسائل الدراسة والتقييم، ومِن ثَمَّ وضع برامج الإصلاح، وآليات حركة المجتمع ومسيرته.

ازداد التوجّه لاستخدام شبكات المعلومات الإلكترونيّة في الفترة الأخيرة مُوفرةً السّرعة والمسافات والجهد و كل هذا قاد إلى الكثير من المشاكل وقدّم ظواهر جديدة من الجرائم لم تكن متداول ة سابقاً، سُميّت بالجرائم الإلكترونية فما أكثر من يخترقون حياة الناس، بداعي الفضول والغيرة، والإيذاء وزاد المُتطفّلون،والمُجرمون،وزادت نسبة تعرّض الشخص للابتزاز، والمُلاحقة، والتهديد وأصبحت هذه الشبكات تحوي معلومات غير محصورة في مجال محدد، بل تتعلق بكافة ميادين الحياة الاجتماعية، الاقتصادية، العلمية و غيرها،إلا أن الاستخدام المتزايد لهذه الأنظمة المعلوماتية أدى إلى الكثير من المخاطر وأظهر أنواعا من الجرائم، أصبح يعرف بالجرائم الإلكترونية.

أهمية الموضوع:

دراسة الإشكاليات التطبيقية للجريمة الإلكترونية تكتسب أهمية متزايدة بسبب استغلال وسائل الاتصالات الحديثة كالفاكس والإنترنت وسائر صور الاتصال الالكتروني عبر الأقمار الصناعية التي استغلها مرتكبو الجرائم لتسهيل ارتكابهم لجرائمهم ولموضوع البحث أهمية من الناحية النظرية والعملية لكونه يمس كثيراً من مصالح المجتمع وعلى وجه الخصوص المصارف من خلال التعامل الإلكتروني والسحب من الأرصدة بواسطة البطاقة الممغنطة أو الدفع الالكتروني، وأيضا المساس بالحياة الخاصة للأفراد عن طريق التسجيل وغيرها من المجالات التي تدخل في استعمال الحاسب الآلي ،،.

وعليه فان الحاجة لوجود دراسة تحليلية نقدية لنصوص القوانين، بقصد مناشدة المشرع والقاضي والفقيه، في الوقت الذي يصدر المشرع فيه القوانين الجنائية، لكي يطبقها القاضي، ويُعْنَى بشرحها ودراستها الفقهية، بأن يضع الحلول الناجعة لما قد يظهر لنا من عيوب، أو قصور بالصورة التي أوجدها المشرع الليبي؛ للاستفادة منها على الصعيد النظري والفلسفي، أو على الصعيد العملي التطبيقي، وعنوان البحث يفي بتذكيرنا، ويترجم هذه الرغبة.

نطاق الموضوع:

إنَّ موضوع الإشكاليات التطبيقية للجريمة الإلكترونية عموماً له أهمية وشأن متميز، بسبب أنها تمس أموراً على قدر كبير من الأهمية، هي في معظمها خروج على قيم المجتمع، وما يؤمن به من أخلاق تضمن أمنه واستقراره، ولأجل هذه الخطورة خصّها الباحث بمزيد من العناية والتحليل، من حيث، أن تسارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية استغله مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة ، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضرباً من ضروب الذكاء الإجرامي، مثل المخدرات الرقمية، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على

استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية ومبدأ الشرعية الإجرائية من ناحية أخرى، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية والتحديات التي تواجه الجريمة الإلكترونية يمكن رصدها من خلال ما أطرحه من حلول لتجاوزها وذلك في موضعه مظاهر تحديات الجريمة الإلكترونية، وإسهاماً في توضيح ما تقدم، كان اختيار الموضوع :- " **الإشكاليات التطبيقية للجريمة الإلكترونية** "

منهج البحث:

يعتمد منهج البحث على الدراسة التحليلية والنقدية لنصوص القوانين، التحليل لكل وجهة بانفراد، ومقارنة بين الآراء المختلفة لفقهاء وشُرَّاح القانون الجنائي، بالإضافة إلى تحليل الآراء الفقهية، والأحكام القضائية، وكل ذلك مشفوع بالتحليل والمقارنة بين نصوص القوانين غالباً، مع الاستعانة بكتب معاصرة، قانونية وفقهية لها قيمتها بغية الوصول إلى نتائج تطابق المذهب الحق، وتساير أهداف التشريع الجنائي، كما تعتبر طبيعة الموضوع من الصعوبات التي واجهت الباحث، فإذا كانت الدراسة قانونية، فإن لهذا الموضوع طبيعة تقنية بحتة لا غنى للباحث عن فهمها وتناولها فارتباط الجرائم محل الدراسة بالتقنية الحديثة في مجال الحاسوب والأنظمة المعلوماتية وشبكة الإنترنت وتكنولوجيات الإعلام والاتصال يحتاج من الباحث بذل جهد إضافي لفهم هذه الجوانب التقنية، والتي ستقوده حتمًا إلى فهم أفضل للجوانب القانونية .

ويظهر فرضاً للموضوع ضرورة إيجاد ترسانة تشريعية خاصة بالجرائم الالكترونية تحدد الدليل الالكتروني، وإجراءاته الشكلية وخاصة انه دليل فني وليس مادي كما في الجرائم التقليدية، كإثبات جنائي يعرض أمام القاضي الجنائي، وتحدد فيها الفصول أنواع الجرائم وعقوبتها، وحتى يستساغ فهم الفرضية في ارتباط بالإشكالية سيتم التعرض للموضوع عبر دراسة مقارنة.

إشكالية الموضوع:

إن ظهور هذا النوع من الدراسة، وهو **الإشكاليات التطبيقية للجريمة الإلكترونية** ، يغري الباحث بالخوض في غمارها، وذلك بقصد تحديد أهم معالمها،حيث ترجع إشكاليات البحث إلى ما يتميز به من صفة فنية، ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشكل محلا للاعتداء أو تستخدم وسيلةً للاعتداء، معظم مستندات موضوعه (الجريمة الإلكترونية) عبارة عن تسجيلات إلكترونية تتم عبر شبكات الاتصال المعلوماتي، ذات طبيعة خاصة متميزة، وذلك راجع إلى عدة عوامل منها طبيعة المال المعلوماتي وحداثة ظهور الحاسب الآلي وتقنية تشغيله، ولهذا أصبح لا يكفي أن يكون الباحث متخصصا في القانون، بل يتعين عليه أن يكون ملما بالجوانب الفنية للحاسب الآلي والإنترنت ليتمكن من إيجاد الحلول للتحديات والمشاكل القانونية التي تثيرها شبكة الاتصال والمعلومات، وجرائمها الإلكترونية، كما، أن عدم وجود قانون يجرم التقنيات الفنية الجديدة الناشئة عن استخدام الإنترنت في ارتكاب الجرائم التقليدية أدى إلى اللجوء إلى التفسير، الأمر الذي أثار إشكاليات التكييف القانوني للفعل كما يثير مشكلة التمييز بين العمل التحضيري والبدء في تنفيذ الجريمة وغيرها، كما أن التعامل مع دليل هذا النمط من الجرائم فتح مجالاً جديداً في الإثبات فبعد أن كان مجال الإثبات ينحصر فقط في المستند الورقي أصبح الدليل الرقمي ينازعه في هذه المرتبة، ناهيك عن وجود بعض الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي كونها مبدأ الشرعية وسريان القانون من حيث الزمان والمكان واختصاص القضاء الوطني.

هذه الإشكاليات في جُلّها تتمحور في الآتي:

– ما مدى علاقتها بالقانون الجنائي سواء فيما يتعلق بالتكييف القانوني لهذه الفئة من الجرائم،أو من حيث موضوعها، وخصائصها، وأشخاصها، وأساليب ارتكبها، ومدى إمكانية الكشف عنها.

– كما أن الضرر الناجم عنها لا يمكن الاستهانة به، وهو ما يطرح التساؤل حول إشكالية الإثبات الجنائي في الجريمة الإلكترونية، وكيفية الحصول على الدليل الإلكتروني حتى يعرض أمام القاضي الجنائي.

– هل يأخذ التحقيق في الجرائم الإلكترونية بعين الاعتبار سلامة الدليل، وحماية الحياة الخاصة للمتهم، وسرية المعلومات التي يحتويها الكمبيوتر، وأجهزة الاتصال الذكية؟

– كيف يتم إخراج الدليل من الأجهزة موضوع ارتكاب الجريمة الالكترونية، ومن هو الشخص القائم بهذا الإخراج للدليل.

– وهل هناك أجل قانوني مابين إخراجه، وما بين عرضه على المحكمة.

– هل المقاربة القضائية كفيلة بالاستناد على دليل إلكتروني محدد كإثبات جنائي في الجرائم الالكترونية، أم أن الأمر يستدعى تناول هذه الأخيرة من علوم متعددة ومتكاملة .

الخطة:

للوصول إلى منهج سليم في معالجة **الإشكاليات التطبيقية للجريمة الإلكترونية**، اقتضت طبيعة البحث في هذا الموضوع الإتيان بخطة ثنائية تقوم على مبحثين،وتلتها خاتمة فيها الخلاصة والمقترحات،وهناك قائمة بالمراجع،وهذه محددات الخطة كما يلي:–

" الإشكاليات التطبيقية للجريمة الإلكترونية "

دراسة مقارنة

المبحث الأول :–

الإشكاليات الموضوعية للجرائم الإلكترونية

المطلب الأول :– ماهية الجرائم الإلكترونية.

الفرع الأول:– تعريف ا لجرائم الإلكترونية.

الفرع الثاني :– أنواع الجرائم الإلكترونية.

المطلب الثاني :- الجوانب الموضوعية للجرائم الإلكترونية.

الفرع الأول:- بـموجـــب قـانون الـعقوبـات .

الفرع الثاني :- بموجب النصوص الخاصة والاتفاقيات الدولية

المبحث الـثـانـي :-

الإشكاليات الإجرائية للجرائم الإلكترونية

المطلب الأول :- إجـــراءا ت الـدلـيـل الإلـكـتـرونـي.

الفرع الأول :- صعوبات جمع الأدلة وصعوبات تتعلق بالجانب الفني.

الفرع الثاني:- حجية الدليل الإلكتروني في الإثبات الجنائي.

المطلب الثـاني:- القضاء المختص بالجرائم الإلكترونية.

الفرع الأول :- القواعد الخاصة للوقاية من الجرائم الرقمية .

الفرع الثاني :- التعاون الدولي في مكافحة الجرائم الالكترونية.

المبحث الأول

الإشكاليات الموضوعية للجرائم الإلكترونية:

لما كانت الجريمة الإلكترونية ظاهرة إجرامية حديثة نظراً لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحالة هذه الظاهرة بكثير من الغموض، لأجل ذلك بدأ لي أنه وقبل الخوض في المسائل الشكلية والإجرائية التي تنطبق على الجريمة الإلكترونية التنويه على جانب من القواعد الموضوعية لهذه الظاهرة الإجرامية المستحدثة وعلى ضوء ذلك في هذا المبحث ما يلي: -

المطلب الأول: - ما هي الجرائم الإلكترونية.

إن السلوك الإجرامي في هذه الجريمة عبارة عن تدفق للمعلومات عبر نظم الحساب الآلي لا يمكن الإمساك مادياً بها، ولذلك ينبغي الوقوف على تحليل سلوكها الإجرامي خاصة فيما يتعلق ببعض الأفكار مثل فكرة المال في جريمة الاعتداء على المال الخاص أو المال العام، وكذلك فكرة التزوير في مخرجات الحاسب الآلي، ويبدو أنه لا أتفاق بين الفقهاء حول مصطلح للدلالة على هذه الظاهرة المستحدثة باعتبار أن موضوع الجريمة الإلكترونية يختلف بحسب ما إذا كان الاعتداء

موجهاً إلى أحد مكونات النظام ألمعلوماتي أو كان وسيلة لتنفيذ جرائم معينة ، لذلك سوف نتطرق في هذا المطلب لما يلي :-

الفرع الأول :- تعريف الجرائم الإلكترونية :-

لا يوجد تعريف موحد للدلالة على الجرائم الإلكترونية، فتعددت التعاريف واختلفت باختلاف وجهات النظر[1] حيث يصعب الاتفاق على تعريف موحد للجريمة الإلكترونية، فعرف البعض الجريمة الإلكترونية بأنها كل سلوك غير مشروع أ غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها، أو أنها نشاط غير مشروع موجه لفسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول عن طريقة،[2] ومن التعريفات المضيفة للجريمة الإلكترونية أنها الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية أو أنها مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات ونقلها[3].

ومن التعريفات والموسعة لمفهوم الجريمة المعلوماتية إنها سوء استخدام الحاسب الآلي فتمتد لتشمل الاعتداءات المادية على جهاز الحاسب الآلي ذاته أو المعدات المتصلة به، كذلك الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك ماكينات الحاسب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق الكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب الآلي في حد ذاته أو أي مكون من مكوناته.[4]

عليه، يجب أن يكون للجاني الدراية الكاملة بتقنية وتكنولوجيا الحاسب، وأن يتوافر لدى أجهزة العدالة الجنائية سواء أكانت سلطة جمع الاستدلالات، أو التحقيق الابتدائي، أو المحاكمة الإلمام الكافي بهذه التكنولوجيا بمعنى أن جريمة إلكترونية لم يكن لدى فاعلها، أو لدى أجهزة الدولة الدراية الكاملة بتقنية الحاسب واللازمة لملاحقة الجاني، وإقامة الدعوى الجنائية وتقديمه للمحاكمة لا تعد جريمة إلكترونية، في حين ذهب جانب آخر من الفقهاء إلى التعريف بالجريمة الإلكترونية على

1 – د.محمد صلاح محمد عبدالمنعم – الجرائم الالكترونية وتحدياتها – دراسة مقارنة – رسالة دكتوراة – كلية الحقوق جامعة المنصورة – بدون سنة نشر – ص 7 .

2 – د. عادل حامد بشير – الإثبات الجنائي للجريمة الإلكترونية – دار النهضة العربية – الطبعة الأولى – سنة 2020 – 202 – ص9 .

3 – د. عادل حامد بشير – مرجع سبق ذكره – ص10 .

4– د. عادل حامد بشير – المرجع نفسه – ص10 .

أساس موضوع الجريمة ذاتها، أو السلوك محل التجريم، وينقسم إلى اتجاهين الأول انطلق من كون الحاسب الآلي هو وسيلة ارتكاب الجريمة، والثاني وهو في منطق أنصاره لا يكون الحاسب الآلي أداة ارتكابها فقط بل تقع الجريمة على الحاسب،أو داخل نظامه.[5]

ومن ناحية أخرى عرفها القانون رقم[5] لسنة 2022م بشأن مكافحة الجرائم الإلكترونية بأن الجريمة الإلكترونية "هي كل فعل يرتكب من خلال استخدام أنظمة الحاسب الآلي، أو شبكة المعلومات الدولية، أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون" وهذا ما نصت عليه المادة [1 فقرة 1 من هذا القانون][6]

وبناءً على ما سبق ذكره، فالجريمه الالكترونية هي كل فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه، أوهي التي تكون المعرفة بالحاسب، أو استخدامه شرطاً ضرورياً لأرتكبها، أو أنها الجريمة التي يكون محلها أو موضوعها المعلومات بصرف النظر عما إذا كان الحاسوب هو الوسيلة المستخدمة من عدمه أو أنها كل غش معلوماتي ينصرف إلى سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها[7].

خلاصة القول يمكن إعطاء تعريف ملخص فهي : سلوك غير مشروع معاقب علية قانوناً صادر عن إرادة جرمية محله معطيات الكمبيوتر يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفى عن الفعل الصفة الإجرامية ومعاقب عليها قانوناً،لان إسباغ الصفة لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع، ومن خلال النص على ذلك ومحل جريمة الكمبيوتر هو دائماً معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة ، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها،المعلومات المستخرجة، والمتبادلة بين الأنظمة المعلوماتية ...الخ)، وأما الكمبيوتر فهو النظام التقني بمفهومه الشامل الذي يزاوج بين تقنيات الحوسبة والاتصال بما في ذلك شبكات المعلومات، وعلى هذا الأساس فأن محاولة أعطاء تعريف

5 – د. محمد كمال شاهين – الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة – دار الجامعة الجديدة سنة 2018– ص 18 .

6 – قانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية – الجريدة الرسمية مجلس النواب الليبي ديوان مجلس النواب – العدد الأول – السنة الأولى – سنة 2023 .

7 – د. محمد على سويلم – مكافحة الجرائم الالكترونية، دراسة مقارنة بالتشريعات العربية والأجنبية – دار المطبوعات الجامعية – الطبعة الأولى– سنة 2019– ص 25.

لهذا النوع من الجرائم المستحدثة الذي يتم في بيئة افتراضية يجب أن يراعى فيه عدة اعتبارات منها:

1- يجب أن يتلاءم هذا التعريف مع فكرة عالمية المعلومات، والاتصالات، وأن يكون واضحاً عالمياً.

2- يجب مراعاة التطورات المتلاحقة في عالم الحوسبة والاتصالات، ويسمح باستيعاب كل ما يستجد من صور للجرائم الالكترونية .

3- يجب توضيح خصوصية الجرائم الالكترونية لما تحتويه عل أشكال مختلفة للسلوك الإجرامي بحيث يظهر جلياً دور الحاسوب في ارتكاب هذه الجرائم[8].

الفرع الثاني :- أنـــواع الـــجـرائـــم الإلـــكـــتـــرونـيـة .

تمر الجريمة الالكترونية بست مراحل هي :

1- البحث عن نظام الحاسب الآلي المقصود بالجريمة.

2- الوصول إلى نقطة الضعف في نظام معلوماته.

3- الاستفادة من نقطة الضعف والتحكم في النظام .

4- تنفيذ السلوك الإجرامي المقصود .

5- تحويل السلوك لربح غير مشروع للفاعل، أو خسارة للمجني عليه.

6- إخفاء جميع الأدلة تجنباً لكشف الجريمة وفاعلها.[9]

حيث أن جرائم الإنترنت تكاد تكون كثيرة ومتطورة ومتجددة، ونحاول الوقوف على أنواع هذه الجرائم مستندين إلى تصنيف معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985، والذي قام بتصنيف جرائم الحاسب إلى أنواع من الجرائم، وذلك على النحو التالي :

أولاً : ارتكاب جرائم تقليدية باستخدام الانترنت : ويدخل ضمن ذلك جميع الجرائم التقليدية المتعارف والمنصوص عليها في القوانين العقابية والمتصور وقوعها باستخدام الانترنت، ومن أهم هذه الجرائم جريمة السرقة، تلك الجريمة التي نشأت مع شيوع أنظمة نقل وتحويل الأموال إلكترونياً

8 - د. يزيد بوحليط- الجرائم الالكترونية والوقاية منها في القانون الجزائري- دار الجامعة الجديدة - 2019- ص 53.

9 - د.محمد على سويلم - مرجع سبق ذكره - ص 26.

وتزايدت بشكل ملحوظ الأموال المتداولة بهذه الطريقة مما جعلها تصبح محلاً لجريمة السرقة بواسطة التحويل الإلكتروني للأموال عن طريق بعض موظفي البنوك، أو بعض المبرمجين المشرفين على الأجهزة الالكترونية في البنوك لمعرفتهم بالشفرات وكلمات السر .

وتعد جرائم السب، والقذف، والتهديد، وفض الرسائل، والاعتداء على حرمة الرسائل الخاصة، والتحريض على الفجور والدعارة، وبث مواد مخلة بالآداب العامة والإباحية،من الجرائم التقليدية، التي من الممكن وقوعها بطريق الانترنت بالإضافة إلى جرائم النصب والاحتيال بنشر مواقع على الشبكة لأسماء محلات وشركات وهمية بقصد الكسب غير المشروع، كذلك جرائم خيانة الأمانة والقمار، وإتلاف الأموال، والمعلومات، والبيانات، وذلك باستخدام الفيروسات بشتى أنواعها.[10]

ثانياً : جرائم الإنترنت حسب اتفاقية بودابست الأوربية لسنة 2001، حول جرائم الكمبيوتر جرائم فضاء التخيل{ المعلوماتية والكمبيوتر] ومنها: 1- الجرائم المتعلقة بالبيانات : مثل التعدي علي سرية، وخصوصية سلامة المعطيات الشخصية، كذلك الدخول غير المسموح به والاعتراض غير القانوني للمعطيات، وسرقه أو تدمير، أو تخريب، أو محو البيانات الشخصيه، وأيضاً الحيازة غير المشروعة للمعلومات وإساءة استخدام المعلومات ونقل معلومات خاطئة .

2- الجرائم المتعلقة بالنظم وأجهزة الكمبيوتر: وهي مثل التعدي على سلامة النظم المعلوماتية وأجهزة الكمبيوتر{إتلاف تخريب} ، والدخول غير المسموح به على أنظمة الكمبيوتر، وكذلك اعتراض النظم المعلوماتية {إساءة استخدام أجهزة الكمبيوتر} والتزوير، والغش المرتبطين بالكمبيوتر، خلف البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات، وإدخال معطيات خاطئة أو مزورة إلى نظام الكمبيوتر.

3- جرائم الكمبيوتر ضد الحكومة : وهي تعطيل الأنشطة والأعمال الحكومية والإخفاق في الإبلاغ،أو بلاغ خاطئ عن جرائم الكمبيوتر، وكذلك الحصول عل معلومات سرية تخص الدولة والعبث بالأدلة القضائية، أو التأثير بها، وبث بيانات تهدد الأمن والسلامة العامة، وأيضا بث بيانات تشمل الإرهاب الإلكتروني، والأعمال الثأرية الإلكترونية.

10 – د .محمد صلاح محمد عبدالمنعم – مرجع سبق ذكره – ص 54.

4-تقسيم الجرائم تبعاً لطبيعة ودور الحاسوب، أو الانترنت في ارتكاب الجريمة إذ قد يكون الحاسوب الآلي، أو الانترنت هدفاً للجريمة، وذلك كما في حال الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزونة، أو تعديلها وكما في حالة الاستيلاء على البيانات المخزونة أو المنقولة عبر النظام .

ومن ناحية أخرى يكون الحاسوب أو الانترنت بيئة الجريمة : كما في تخزين البرامج المقرصنة فيه أو في حالة استخدامة لنشر المواد غير القانونية، أو استخدامه أداة تخزين أو إتصال لصفقات تروج المخدرات، وأنشطة الشبكات الإباحية ونحوها.

وفى ذات السياق، هناك دور الحاسوب والانترنت في اكتشاف الجريمة : حيث يستخدم الحاسوب على نطاق واسع، وفى جميع مراحل الإثبات بدء من مرحلة جمع الاستدلالات، وحتى تنفيذ الحكم مروراً بالإثبات العلمي الجنائي المتمثل بأعمال الخبرة القضائية حيث يلعب الحاسوب ذاته دوراً رئيسياً في كشف جرائم الحاسوب والانترنت وتتبع فاعليتها وإبطال أثر الهجمات التدميرية لمخترق النظم وتحديداً هجمات الفيروسات، وقرصنة البرمجيات فالحاسوب يعد أداة قوية في مجال مقارنة المعلومات ومعرفة هوية الأشخاص الذين لهم سوابق إجرامية[11].

ثالثاً :- وأخيراً هناك الاعتداء على حقوق الملكية الفكرية: ويتضمن ذلك عملية نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية الموضوعية على شبكة الإنترنت دون تفويض من صاحبها أو سرد قيمتها، وإعادة استخدامها، أو طبعها، أو تسويقها، أو استغلالها بأية صوره كانت، هذه بعض الجرائم على سبيل المثال وغيرها الكثير من الجرائم التي نشأت عن استخدام الشبكة وتتطور باستمرار ، كبث شبكة الانترنت من أفكار وآراء إرهابية تدعو إلى الجريمة وتحرض عليها ،وما تحويه من مخاطر على الأمن القومي لبعض الدول من خلال اختراق لمواقعها الموجودة على الشبكة من قبل القراصنة، [12] وهذا ما نصت علية المادة (45) من القانون مكافحة الجرائم الالكترونية(يعاقب بالسجن كل من أنشأ موقعاً، أو نشر معلومات على شبكة المعلومات الدولية، أو إحدى الوسائل الالكترونية لجماعة إرهابية تحت مسميات تمويهية ؛ لتسهيل الاتصال بقيادتها أو أعضائها ، أو ترويج أفكارها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات

11 - د. أمير فرج - سلطة القاضي الجنائي في تقدير الدليل الالكتروني - دار المطبوعات الجامعية - بدون سنة طبع - ص161.

12- د. محمد صلاح محمد عبدالمنعم - مرجع سبق ذكره - ص 56.

تستخدم فى أعمال محظورة.)[13] وفى ذات السياق نصت المادة (79) من القانون رقم (6)، بشأن المعاملات الالكترونية، على انه (يحظر على الجهات التي تقوم بتجميع بيانات شخصية طبقاً للمادة (73) من هذا القانون إرسال وثائق الكترونية إلى الشخص الذي جمعت عنه البيانات، إذا كان يرفض قبولها صراحة، ولا يجوز معالجة بيانات شخصية بواسطة من قام بتجميعها، إذا كان يرفض قبولها صراحة، ولا يجوز معالجة بيانات شخصية بواسطة من قام بتجميعها ، إذا كانت تلك المعالجة تسبب ضررًا للأشخاص الذين جمعت عنهم البيانات، أو تنال من حقوقهم، أو حرياتهم، كما لا يجوز استعمال تلك البيانات في أي أغراض أخرى غير المتفق عليها، إلا بموافقة صاحب البيانات).[14]

المطلب الثاني : الجوا نب الموضوعية للجرائم الالكترونية .

تعد تقنية المعلومات ، تعتبر من أكبر التحديات المطروحة فى عالم الحاضر والمستقبل، ومواجهة هذه التحديات يستلزم إعطاء صورة عامة عن تحديد ماهيتها، بموجب قانون العقوبات وكذلك موقف الاتفاقيات الدولية، وهذا على النحو الأتي:-

الفرع الأول :- بموجب قانون العقوبات .

يتمثل أساس المسؤولية الجنائية في الالتزام القانوني بتحمل التبعة، فهي تنشأ تابعة لالتزام أخر وهو في حقيقته واجب، فالمسؤولية الجنائية ركنان أساسيان : الأول هو الرابطة المادية بين الواقعة والنشاط المادي أي الإسناد المادي من جهة، والثاني هو الرابطة المعنوية بين الشخص والسلوك [15]. حيث يشكل الوصول للمجرم المعلوماتي، أو الالكتروني عبء فني وتقنى بالغ على القائمين بأعمال التتبع والتحليل لملابسات الوقائع الإجرامية المختلفة، وتفترض التشريعات على اختلاف طرائقها التي تنتهجها في التقنين مبدأ مسلماً به أنه لا يكفى لقيام المسئولية الجنائية إسناد الجريمة مادياً إلى شخص ما، بل يجب أن تُثبت قبله معنوياً أيضاً، أي أن تكون صادرة من إدراكه وإرادته ويرى جانب من الفقه والقضاء سواء في القانون المصري أم في القانون الفرنسي قصر

13 – القانون رقم (5) لسنة 2022. بشان مكافحة الجرائم الالكترونية – الجريدة الرسمية – العدد الأول – السنة الأولى 2023.

14 – القانون رقم (6) لسنة 2022. بشان المعاملات الالكترونية – الجريدة الرسمية – العدد الأول – السنة الأولى 2023.

15 – د. محمود رجب فتح الله – الشرعية الجنائية للأدلة الرقمية – دراسة مقارنة – دار الجامعة الجديدة – سنة 2020 – ص 167.

المسئولية الجنائية على ضرورة توافر التمييز وحرية الاختيار، بينما يضيف إليها جانباً أخر هو الركن المعنوي فيوصف هذا الركن بأنة ركن المسئولية الجنائية

ويلاحظ أن كل من الرأيين يقيد مفهوم المسئولية ويقصرها على النواحي والجوانب المعنوية للجريمة دون سند صحيح من الواقع والقانون، والواقع أن التحليل العلمي الدقيق يقود إلى بيان موضوع المسؤولية الجنائية من البنيان القانوني للجريمة، فهي لا تعد ركناً، أو عنصراً من عناصر الجريمة، وإنما هي الأثر المترتب على توافر كافة الشروط اللازمة لتحمل التبعة والخضوع للجزاء الجنائي، سواء أكانت هذه الشروط موضوعية مرتبطة بالجريمة ذاتها، أم متعلقة بالجاني، إذ يجب توافر شروط عديدة ومتنوعة لقيام المسؤولية الجنائية عن جرائم الكمبيوتر والإنترنت، وهي : توافر الصفة غير المشروعة بالفعل، أو الامتناع وقيام الركن المادي للجريمة وصدوره عن إرادة مدركة وحرة واعية، وتوافر القصد الجنائي الخاص لدى مرتكب الجريمة .

وفي ذات السياق، فان الركن المادي : للنشاط الإجرامي عنصران، عنصر مادي هو الحركة المادية وآخر نفساني هو العملية العقلية، ويتطلب النشاط أو السلوك المادي في جرائم الإنترنت وجود بيئة رقمية واتصال بالإنترنت، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجة، ولا تستلزم كل جريمة وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، لكن الأمر يختلف بعض الشيء في مجال تكنولوجيا المعلومات فشراء برنامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال تمثل جريمة في حد ذاتها، وتثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية .

أما الركن المعنوي : هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلاقات التجارية في القانون الفيدرالي الأمريكي، وأحياناً أخرى أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي .

أما بالنسبة للقضاء الفرنسي فأن منطق سوء النية هو الأعم في شأن جرائم الانترنت، لذ يشترط الشارع الفرنسي وجود سوء نية في الاعتداء على بريد إلكتروني خاص بأحد الأشخاص[16] وفي ذات السياق أشار القانون رقم (5) بشأن مكافحة الجرائم الإلكترونية بذلك من خلال نص المادة (49)على انه (في غير الجرائم المنصوص عليها في هذا القانون يعاقب كل من ارتكب جريمة معاقبًا عليها بموجب قانون العقوبات ، والقوانين المكملة باستخدام الشبكة المعلوماتية، أو أي نظام معلوماتي، أو اشترك في ارتكابها بالعقوبة المنصوص عليها في ذلك القانون).[17]

خلاصة القول، يتحقق الركن المادي في هذه الجريمة بدخول المجرم المعلوماتي إلى نظام المعالجة الآلية للمعطيات بطرق الغش، أو بالبقاء فيه، أو في جزء منه، إما أنه ليس من بين المشتركين، أو أنه غير مرخص له بالدخول، أو له الحق في الدخول إلا أنه بقى في النظام بعد انتهاء المدة المصرح له بها .

أما الركن المعنوي فيلزم لتوافره أن تتجه إرادة الجاني إلى فعل الدخول، أو إلى فعل البقاء بهدف الإدخال، أو المحو، أو التعديل، وأن يعلم بأن سلوكه هذا يؤدي للتلاعب في المعطيات، كما يجب أن يعلم أنه ليس لهُ الحق في الدخول إلى النظام والبقاء فيه، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء[18] .

الفرع الثاني : بموجب النصوص ا لخاصة والاتفاقيات ا لدولية .

أن عدم كفاية الإجراءات التقليدية المتعلقة بجمع الدليل الإلكتروني لاستيعاب كافة أشكال هذا النوع المستحدث من الجرائم، مما دفع بعض الدول استحداث أساليب بحث وتحري جديدة تتلاءم وخطورة هذه الجرائم ضماناً لعدم إفلات المجرم من العقاب، ونظراً للطبيعة الخاصة للجرائم الإلكترونية، لم يكتفي المشرع الجزائري باستخدام هذه الأساليب حينما تقع الجريمة، ولكن أيضاً قبل وقوعها حيث نص في القانون رقم:(09 -04 المؤرخ في 05- غشت 2009) على القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء لتكريس إطار قانوني أكثر ملائمة وانسجاماً مع خصوصية وخطورة الجريمة الإلكترونية .

16 – د . محمد على سويلم – مرجع سبق ذكره – ص 53 وما بعدها .

17 – قانون رقم (5) لسنة 2022 – مرجع سبق ذكره .

18 – د . يزيد بوحليط – مرجع سبق ذكره– ص 134 .

كما أخذ المشرع بعين الاعتبار الاتفاقيات الدولية ذات الصلة بالموضوع، وكذلك التجانس مع النصوص الوطنية التشريعية التي سنها إلى حد الآن مثل : تلك المتعلقة بمكافحة الفساد،وتبييض الأموال، وتمويل الإرهاب، والمخدرات المؤثرات العقلية، حيث نص المشرع على جملة من الإجراءات المهمة خاصة ما تعلق بحالات اللجوء إلى المراقبة الإلكترونية وتفتيش المنظومة ألمعلوماتية وحجز المعطيات والتزامات مقدمي الخدمات، ومزودي خدمة الإنترنت والتعاون والمساعدة القضائية الدولية، والاستعانة بكل شخص لهُ دراية وخبرة لمساعدة جهات التحقيق في الكشف عن الجرائم الالكترونية [19] .

من ناحية أخرى ، سعت بعض المنظمات، والهيأة الدولية مثل هيئة الأمم المتحدة، ومنظمة التنمية الاقتصادية، والمجلس الأوروبي، والمنظمة العالمية للملكية الفكرية،والجمعية المصرية للقانون الجنائي، ومركز الدراسات الأمنية في الرياض لتحديد المشاكل التي تثيرها الجرائم الإلكترونية في نطاق التعاون الدولي، ولما كانت الجرائم الالكترونية عابرة للحدود لذا يتطلب الأمر يتطلب ما يأتي :

1- سن النصوص الجنائية الموضوعية على الصعيد الوطني للتجريم والمعاقبة عليها ،إضافة لسن قواعد إجرائية .

2- خلق وتطوير وإنماء العلم الدولي المشترك لمواجه هذه الظاهرة عبر وضع حلول للمشكلات التي تحد من فاعلية مكافحتها .

وينبغي مواجه هذه الجرائم ومكافحتها عبر القانون الوطني، ومن ثم يكون هناك تعاون وتضامن دولي لمواجهه مشاكلها من حيث مكان وقوعها واختصاص المحاكم فيها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها، وتحديد صورها وقواعد التسليم فيها وإيجاد الحلول لها، أما فيما يتعلق بمشاكل التعاون الدولي بشأن الجرائم الالكترونية، تتمثل غالباً بأن الجرائم الالكترونية هو أنها عابرة للحدود، لذا فهي تثير المشاكل، مثل الإتجار بالمخدرات، والرقيق الأبيض والتلوث البيئي والإتجار بالأسلحة .

ولعل المشكلة الأهم أن هذه الجرائم لا يتم التعامل معها كونها وحدة واحدة في إطار الحماية الجنائية للمعلومات بل على نصوص متناثرة في كل قانون نص مستقل عن الآخر في القوانين

19 - د. يزيد بوحليط – مرجع سبق ذكره – ص 427 .

ذات العلاقة.[20]، وبالتالي نلاحظ العديد من الدول لا تقر قوانينها بعض الاختصاصات القضائية خصوصاً إذا لم تربط هذه الدول بالجريمة محل التتبع أية علاقة إقليمية أو شخصية أو أمنية، وهذا المنحى من جانب بعض الدول خلف فراغاً في ردع الجريمة الالكترونية، لذلك سعى القانون الدولي الى الضغط على الدول لكي تقر قوانينها بما يعرف بالاختصاص الشامل أو القضاء العالمي، تمنح بمقتضاه أي دولة حقاً وأحياناً واجباً هو ممارسة الاختصاص القضائي في جرائم معينة ارتكبت خارج إقليمها واعتبرتها الجماعة الدولية مخلة، ليس فحسب لمصالح بلد معين، ولكن بالنسبة لمصالح جميع الدول[21]. وفي ذات السياق، نص القانون رقم (5) لسنة 2022 م بشأن مكافحة الجرائم الالكترونية في المواد (7 ، 10 ، 14 ، 16 ، 20 ، 24 ، 43 ، 44)[22].

المبحث الثاني

الإشكاليات الإجرائية للجرائم الإلكترونية

إنَّ طبيعة الجرائم الإلكترونية بعناصرها، ووسائل ارتكابها قد تدفع المشرع الجنائي إلى إعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون، ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لا بد أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام به، مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يُمكن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها في الوصول إلى الدليل المناسب في إثبات الجريمة الالكترونية، وسوف نعالج ذلك على النحو التالي :-

المطلب الأول : إجراءات الدليل الإلكتروني

يجب أن تكون الأدلة المأخوذة من الكمبيوتر لها نفس سمات الأدلة التقليدية، بمعنى أخر يجب أن تكون مقبولة وسليمة ودقيقة وكاملة ولكن تلك الأدلة لها أيضاً سمات محددة تخلق مصاعب تواجه من يرغبون في الاعتماد عليها، فهي غير مستقرة، ويسهل تغييرها دون أن يترك ذلك أثر واضح، كما إنها مبتكرة للغاية مما يوجد مشاكل لا

20 - د . على حسن الطوالبة - الجرائم الالكترونية - جامعة العلوم التطبيقية كلية الحقوق - بدون طبعة - بدون سنة نشر - ص 96

21 د. محمد على سويلم - مرجع سبق ذكره - ص- 560.

22 - القانون رقم (5) لسنة 2022م مرجع سبق ذكره .

تتعلق بتفسيرها فحسب بل أيضا بالفحص الجنائي، ويعتبر علم الفحص الجنائي للكمبيوتر من المجالات الراسخة بشكل معقول الآن[23].

ومن هذا المنطلق سوف نتطرق لهذا المطلب على النحو الأتي :-

الفرع الأول :- صعوبات جمع الأدلة .

من المسلم به قانوناً أن طلبات ودفوع الخصوم في الدعوى الجنائية، لابد لها من الإثبات عبر الدليل وهذا الدليل قد يكون تقليدياً أو إلكترونياً، فالإثبات الجنائي بوجهه عام هو نشاط إجرائي موجه مباشرة للوصول لليقين القضائي والحقيقة طبقاً لمعيارها الواقعي الخاص (تحديد الجرم) وذلك بشأن الاهتمام سواء بتأكيده أو نفيه، كما أن الدليل الجنائي هو وسيلة القاضي في تحديد فاعل الجريمة (أو حتى الشريك فيها) فهو كل وسيلة مسموح بها قانوناً يلجأ لها القاضي لإثبات وجود، أو عدم وجود الواقعة المرتكبة، أو صحة، أو كذب الواقعة، فالدليل هو قوام حكم القاضي ولهُ أن يقدر أهميته كي يكون، ثم فصل في الدعوى العمومية أما بالبراءة، أو الإدانة .

ومن ناحية أخرى، يمكن تعريف الدليل إلكتروني في مجال الجنائي وخصوصاً الإثبات، بأنه مجموعة الموجات المغناطيسية، أو النبضات الكهربائية التي يمكن تجميعها وفحصها باستخدام تطبيقات وبرامج معينة لتظهر في شكل صور، أو تسجيلات صوتية، أو مرئية، ويتميز الدليل الإلكتروني في مجال الإثبات الجنائي بعدة خصائص تجعله ذو طبيعة وأهمية خاصة بالمقارنة مع الدليل الكلاسيكي التقليدي، فيعتبر الدليل المعلوماتي دليلاً غير ملموس، فهو دليل مادي بالمعنى التقليدي، فترجمة هذا الدليل، وإخراجه في شكل ملموس، أو مادي لا يعني أن هذا التجميع هو الدليل، بل هي مجرد عملية لنقل تلك الموجات، أو النبضات الالكترونية إلى الشكل الذي يمكن الاستدلال على المعلومات[24].

ومن ناحية أخرى، الأدلة الرقمية يمكن استرجعها بعد محوها، وإصلاحها بعد إتلافها وإظهارها بعد إخفائها مما يؤدى إلى صعوبة التخلص منها وهي خصيصة من أهم خصائص الدليل الرقمي بالمقارنة مع الدليل التقليدي فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة

---

23 – د . محمد صلاح محمد عبد المنعم – مرجع سبق ذكره – ص 203 .

24 – د. محمد عبد الحميد عرفه – مدى حجية الأدلة الالكترونية الرقمية في الإثبات في المواد الجنائية ، دراسة تحليله تطبيقه مقارنة – مجلة الحقوق للبحوث القانونية والاقتصادية – كلية الحقوق جامعة الإسكندرية – العدد الأول 2018 م – المجلد الأول – ص 441 .

البيانات التي تم حذفها، أو إلغائها سواء تم ذلك بالأمر (delete)أو إعادة التهيئة، أو تشكيل للقرص الصلب (hard disk) باستخدام الأمر (format) والبرامج التي تم إتلافها، أو إخفائها سواء أكانت صوراً، أم رسوماً، أو كتابات أو غيرها مما يعنى صعوبة إخفاء الجاني لجريمته، أو التخفي منها عن أعين الأمن والعدالة طالما تم علم رجال البحث والتحقيق الجنائي بوقوع الجريمة، بل أن محاولة الجاني محو الدليل الرقمي بذاتها تسجل علية كدليل حيث أن قيامه بذلك يتم تسجيله في الذاكرة الآلة، وهو ما يمكن استخراجه، واستخدامه كدليل ضده .

وفى ذات السياق، تتسم جرائم الإنترنت بصعوبة اكتشافها وإثباتها، فالجريمة المعلوماتية تتم في بيئة وإطار لاعلاقة لهما بالأوراق، أو المستندات، بل تتم بواسطة الحاسوب، أو الشبكة العالمية ويمكن للجاني عن طريق نبضات إلكترونية، لا ترى العبث في بيانات الحاسوب، أو برامجه، وذلك في وقت قياسي قد يكون في جزء من الثانية ،وهذه البيانات، أو المعلومات التي يتم العبث بها يمكن محوها كذلك في زمن قياسي قبل أن تصل يد العدالة إليه، لا سيما إن عملية الضبط لا تتم إلا بمعرفة خبير فني أو متخصص[25].

خلاصة القول، إن التحفظ على الأدلة داخل الحاسوب من العمليات المعقدة التي تحتاج بداية إلى رصد دقيق لمدى صحة البيانات التي يحتوى عليها الحاسوب ، وعملية حفظ الأدلة في العالم الرقمي يتطلب من الخبير التقني القيام برصد موقع على الانترنت أو المعلومات التي تشير إلى الجريمة، والتي تكون في مظاهر مختلفة الإشكال .

كذلك تستدعى عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير بعرض الأدلة على المحكمة، أو جهات التحقيق، وهذا الأمر يتطلب عمل الخبير يستمر لمرحلة المحاكمة، وأحياناً يتطلب منه القيام بعمله لمرحلة ما بعد المحاكمة كما هو الشأن في حالة عرض الدليل المقدم إلى المحكمة أمام جهة قضائية أعلى كالاستئناف، أو النقض ومنعاً للمشاكل التي يمكن أن تنجم عن حفظ الأدلة في العامل الرقمي، فإن العديد من المحاكم لجأت إلى ميكنة إدارتها رقمياً، بحيث يتم تسليم الأدلة إلى إدارة متخصصة تتولى بدورها حفظ الأدلة في العامل الرقمي لعرضها على القضاء كلما تطلب الأمر ذلك [26].

25 – د. أمير فرج –مرجع سبق ذكره – ص91.

26 – د . عادل حامد بشير – مرجع سبق ذكره – ص 66.

الفرع الثاني : – حجية الدليل الإلكتروني في الإثبات الجنائي .

استقر الفقه والقانون الوضعي على إن للقاضي سلطة واسعة في تقدير الأدلة، واستنباط القرائن، وما تحمله الوقائع من دلالات شريطة أن يكون الدليل ثابتاً بيقين، مرتبطة بالواقعة الرئيسة ومنسجماً مع التسلسل المنطقي للأحداث، وبالنسبة للأدلة الرقمية، فإنها تخضع للقواعد المقررة لباقي الأدلة فيما يخص حجيتها، ومقبوليتها على مستوى أنظمة الإثبات الجنائي .

ونظراً للطبيعة الخاصة للدليل الرقمي فإن حجيته على مستوى الإثبات الجنائي، قد تثير العديد من المشاكل خاصة فيما يتعلق بمصداقية هذا الدليل، وبناءً على ذلك، حتم التطور التكنولوجي على القاضي الجنائي اللجوء إلى نوع مستحدث من الأدلة والتي من بينها الدليل الرقمي، على أن هذا النوع من الأدلة لا بد أن يكون مقبولاً أمام القاضي الجنائي، ولهذا فهو مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات قد تأخذ شكل محاضر معدة بمناسبة تفتيش، أو اعتراض مراسلات، أو شكل تقرير خبرة محرر بمناسبة معاينة، وفحص الأدلة المضبوطة من جهاز الآلي، أو دعامات إلكترونية .

وفى ذات السياق، إن مجرد الحصول على الدليل الرقمي وتقديمه للقضاء، لا يكفى لاعتماده دليلاً للإدانة، إذ الطبيعة الفنية الخاصة للدليل الرقمي تُمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث[27] .

عليه، فأن القاضي الجنائي كما يصح له أن يؤسس اقتناعه على أي دليل، له أن يهدره أيضاً، ومقابل ذلك لا ينبغي أن يفهم من حرية القاضي في الاقتناع التحكم المطلق في الأمور والقضاء كيف ما شاء وفقاً لأهوائه ومزاجه الشخصي، إنما هو مطالب بتحري المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه واستلهام عقيدته، وألا يكون تفكيره هذا قد جافى الأصول المسلم بها في الاستدلال القضائي، ولتحقيق ذلك، إحاطة القانون بمجموعة من القيود التي تشكل في مجملها شروطاً لأعمال المبدأ وتطبيقه التطبيق السليم بما يضمن بلوغ الحقيقة دون المساس بالحقوق والحريات العامة للأفراد .[28]

27 – د. دريف مصطفى – الإثبات الجنائي بالوسائل الالكترونية الحديثة – رسالة ماجستير – جامعة عبدالحميد بن باديس مستغانم – سنة 2020–2021– ص 55.

28– د. محمد على سويلم – مرجع سبق ذكره – ص 621.

فالقاعدة في الدعاوى الجنائية هي جواز الإثبات بكافة الطرق والوسائل القانونية والقيد على القاعدة أنه يجب أن يكون الدليل من الأدلة المقبولة قانوناً، وبالتالي تظهر أهمية اعتراف القانون بالأدلة الرقمية خاصة مع احتمال ظهور أنماط إجرامية جديدة لجميع الجرائم، وخاصة في قطاع المعلومات المعالجة بواسطة الكمبيوتر، ومن هنا كان البحث القانوني في العديد من الدول يتجه إلى الإقرار بحجة قانونية للملفات والمستخرجات الحاسوبية والرسائل الالكترونية ذات المحتوى ألمعلوماتي ليس بصورتها الموضوعة ضعف وعاء مادي، ولكن بطبيعتها الإلكترونية المحضة، ذلك أن التطور العلمي قد أثر وبلا شك على نظام الاقتناع القضائي.[29]

وخلاصة القول، حول المشرع والقضاء والفقه المقارن تحديد الشروط الواجب توافرها في الدليل الرقمي، أو في مخرجات الحاسوب حتى يمكن قبوله من قبل القاضي، أي أنه عند إثبات مضمون كتابات، أو سجلات، أو صور، فأن أصل هذه الكتابات، أو السجلات، أو الصور يجب أن يكون متوفراً أي يجب تقديمه إلى المحكمة، وحتى يكون الدليل الرقمي مقبولاً أمام المحكمة يجب أن تتوافر فيه الشروط التالية :

1- سلامة محتويات السجل الالكتروني من أي تغيير ،أي أن يكون الدليل المقدم للمحكمة هو الدليل نفسه الذي تم جمعه، ويمكن للشخص الذي قام بجمع الدليل أن يشهد بذلك أمام المحكمة .

2- أن تكون المعلومات الموجودة في السجل، قد صدرت فعلاً عن المصدر المزعوم سواء أكان هذا المصدر الإنسان أم الآلة.

3- أن تكون المعلومات الموجودة في السجل، والمتعلقة بالوقت والتاريخ، معلومات دقيقة [30].

الطلب الثاني :- القضاء المختص بالجرائم الإلكترونية.

إن شبكة الإنترنت ليس لها مقر في دولة معينة، ولا تخص شخص محدد بل توجد موزعة على الكرة الأرضية كلها فهي تجمع عدداً كبيراً من الشبكات مختلفة النوع والمصدر والوظيفة وترتبط بها الخطوط التلفونية من كل دول العالم، ولذلك فأن الانترنت لا تخضع للرقابة، أو سيطرة دولة معينة بسبب عدم وجود قانون جنائي، أو رقابة، أو سيطرة دولة معينة بما يترتب على ذلك تعدد القوانين الجنائية التي تطبق عليها بتعدد الدول المرتبطة بها باعتبار أن القانون الجنائي يتعلق

29 - د. أمير فرج - مرجع سبق ذكره - ص 97.

30 - د. محمود رجب فتح الله - مرجع سبق ذكره - ص 576.

بسيادة الدوله، وهنا تكمن المشكلة، فالمشكلة الأساسية التي يطرحها الإنترنت تكمن إذاً في تدويل الجرائم المرتكبة خلالها؛ لأن نشر رسالة ما من خلال هذه الشبكة يمر عبر عدة دول مع غياب رقابة جهة معينة على هذه الشبكة، وعدم وجود قانون محدد يحكمها، وعلى الرغم من أن المبدأ السائد الآن هو مبدأ إقليمية القانون الجنائي لكن هناك استثناءات ترد على هذا المبدأ مردها جميعاً الحرص على عدم إفلات المجرم من العقاب بعد أن تطور الإجرام، وبدأ يأخذ أشكالاً مختلفه وكثرت العصابات الإجرامية التي يمتد نشاطها ليشمل عدد كبير من الدول، واتخذت الجريمة الطابع الدولي، وانتشرت الاتصالات عن بعد(شبكة الانترنت)، ولذلك كان لا بد من وجود نظام يسمح بالعقاب على هذه الجرائم كلها[31].

ومن هذا المنطلق سوف يتم تقسيم المطلب على النحو التالي :-

الفرع الأول :- القواعد الخاصة للوقاية من الجرائم الإلكترونية .

لم تنتهج الدول منهجاً واحداً في تحديد سلطات مكافحة الجرائم الإلكترونية، ويمكن تأصيل ورد مسلك الدول المختلفة إلى ثلاثة مناهج :

الأول: إسناد المكافحة إلى سلطات الضبط القضائية، حيث لم تأخذ الكثير من الدول بمبدأ تخصيص سلطات مكافحة جرائم الجرائم الإلكترونية، وأسندت المكافحة إلى سلطات الضبط القضائية .

الثاني : عدم تخصيص جهة، أو هيئة معينة بمكافحة الجرائم الإلكترونية حيث أنشأت فرنسا منذ أوائل التسعينات أجهزة خاصة من أجل مكافحة غسيل الأموال، وتم تكثيفها مؤخراً من أجل مكافحة تمويل الإرهاب، وأول ما يلاحظ في فرنسا هو عدم انفراد دائرة واحدة بمكافحة الجرائم المنظمة؛إذ يملك مأمور الضبط القضائي ودوائر الإدارة المركزية للشرطة القضائية التي أنشأة داخلها وحدة خاصة بمكافحة تمويل الإرهاب، ووحدة معالجة المعلومات اتخاذ الإجراءات ضد الشبكات المالية السرية، ومكافحة الجريمة المنظمة، فقد نصت المادة الثالثة من قانون 12 مايو 1990 الخاص بتعاون الأجهزة المالية في مكافحة غسيل الأموال علي أن هذه الأجهزة المالية يقع عليها التزام بتبليغ خلية الاستخبارات المالية الفرنسية المعروفة باسم " وحدة معالجة المعلومات واتخاذ الإجراءات ضد الشبكات المالية السرية" بالعمليات المشبوهة التي يبدو أن مصدرها الاتجار

31 – د. أمير فرج – مرجع سبق ذكره – ص 331.

بالمخدرات أو نشاط المنظمات الإجرامية، وتحيل وحدة الاستخبارات المالية بدورها نتائج هذا التحقيق الإداري عند الاقتضاء إلي السلطات القضائية".

المنهج الثالث : الجهات، أو الهيئات المخصصة لمكافحة الجرائم الالكترونية هذا هو المنهج الغالب في الدول التي سنت تشريعات مستقلة لمكافحة جرائم تقنية المعلومات كالقانون الجزائري.[32]

الفرع الثاني:- التعاون الدولي في مكافحة الجرائم الالكترونية .

إن التعاون الدولي في مكافحة هذه الجريمة من خلال الاتفاقيات الدولية واتفاقيات تسليم المجرمين، وقاعدة التعاون القضائية من شأنه أن يؤدى إلى تطويق هذه الجريمة والحد من أخطارها على المجتمع الدولي بأسره مما يجعل المسؤولية ملقاة على عاتق الدول.

حيث، أن العديد من الهيئات والمنظمات والمجالس الدولية تلعب دوراً ملحوظاً في إطار إبرام الاتفاقيات والمعاهدات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة جرائم الحاسوب الآلي، وعلى رأسها الأمم المتحدة، والمجلس الأوروبي، وبعض الهيئات الأخرى، حيث يتمثل ذلك في الأتي :

التعاون الدولي في مكافحة الجرائم الالكترونية،التعاون القضائي: إذ أن فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالانترنت غالباً ما تقتضى تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت، أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب بالإنترنت، حيث أن التعاون القضائي تتجسد أحد صوره في المساعدة القضائية الدولية، وهي عبارة عن كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم .

حيث يعد النظام إجراًء رئيساً بالنسبة لمعظم الجرائم المعلوماتية التي يقوم بارتكابها الجاني وهو في دولة وتتحقق الجريمة في إقليم دولة أخرى منتهكاً بذلك قوانينها وأنظمتها الداخلية، لذا فأن الدولة الأخيرة لا يكون أمامها سوى اللجوء إلى نظام تسليم المجرمين للملاحقة ومن محاكمة هذا المجرم عن جريمته تلك، أو لتنفيذ حكم صادر من محاكمها ضده في هذا الشأن .

دور المنظمات الدولية والإقليمية لحماية من الجرائم الالكترونية :

32 – د. محمد على سويلم – مرجع سبق ذكره – ص 527.

حيث أن التعاون الدولي يواجه الكثير من الصعوبات، فالتشريعات التقليدية تقف عائقاً أمام التعاون، وكذلك الاختلاف على مضمون الأفعال التي تعد من جرائم الحاسوب، وأن التمايز الحضاري والتشريعي بين الدول المختلفة، ومدى اعتمادها على التقنية العالية معوقات تقف في وجه التعاون الدولي في مجال توفير الحماية الجنائية الأزمة، ولكن هذه المعوقات لا تنفي، ولا تنكر الجهود الدولية المبذولة في هذا المجال، حيث بات أمر التعاون الدولي لمواجهة جرائم الحاسب الآلي ضرورة حتمية، وأكدت المنظمات العالمية، والإقليمية على حق الإنسان في حرمة حياته الخاصة من إخطار الاعتداء على البيانات الشخصية، وفى إطار الجهد الدولي المبذول فأن هناك العديد من الهيئات والمنظمات والمجالس الدولية التي تؤدي دوراً ملحوظاً في إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة جرائم الحاسب الآلي وعلى رأسها هيئة الأمم المتحدة والمجلس الأوروبي وبعض الهيئات الأخرى.[33]

33 - د.محمد صلاح محمد عبدالمنعم – مرجع سبق ذكره – ص 378.

الخاتمة

نستنتج من خلال هذا الطرح أن الجريمة الإلكتروني تختلف عن الجريمة التقليدية بطبيعة خاصة، لأنها تُرتكب في بيئة تقنية وتكنولوجيا المعلومات مما أضفى عليها وعلى مرتكبها سمات خاصة، وسمي المجرم فيها بالمجرم المعلوماتي مهارات فنية وتقنية عالية، فضلًا عن كونها جريمة عابرة للحدود، ومحل الاعتداء فيها غالبًا هو المعلومات، الذي يعد أمر جديد على المحقق الجنائي.

تعددت العقبات والصعوبات التي تواجه الأدلة الرقمية، التي لا تقف عند حد كيفية الحصول عليها وإجراءات حفظها، بل تمتد على مدى القوة الثبوتية التي يتمتع بها هذا الدليل ومدى حرية قاضي الموضوع بالاقتناع به لبناء الحكم على أساسه بالبراءة، أو الإدانة، إضافة إلى عجز النصوص الإجرائية الحالية في مساعدة سلطة التحقيق الابتدائي في الوصول إلى الدليل ألإلكتروني.

عليه نوصى بضرورة إلمام المحقق بالتقنيات الحديثة، وذلك لفهم لغة الحاسوب، وطبيعة الجريمة والمجرم الذي يتعامل معه، بل وشَكَّل الدليل، وطبيعته المعنوية غير الملموسة التي يبحث عنه.

ضرورة إنشاء نيابة مختصة بالتحقيق الابتدائي في الجريمة الإلكترونية وذلك على غرار النيابات المتخصصة، إضافة إلى أهمية مراعاة السرية وحماية الخصوصية، وتأهيل مأموري الضبط القضائي للتخصص في مجال مكافحة جرائم تقنية المعلومات، وكيفية التعامل مع أجهزة الحاسب والإنترنت، واستخلاص الأدلة الرقمية منها، وإنشاء مختبر للأدلة الرقمية الجنائية لجرائم تقنية المعلومات، بالتعاون مع المصارف، بغية إجراء التحقيقات المطلوبة والحصول على الأدلة، وتحليل الفيروسات والحد من انتشارها محليًا ودوليًا.

إن الجرائم الإلكترونية وإن كانت تبدو أنها منظمة من قبل بعض التشريعات إلا إنها تثير العديد والكثير من الصعوبات، والمشاكل، ولا سيما بتحديد شخص الجاني إذا ما كان مقيمًا خارج الدولة، فيصعب تحدد المسؤول جنائيًا إذا وقعت الجريمة عبر الإنترنت، وكذلك مسائل الإثبات لذا يجب أن تكون نصوص قانون الجرائم الإلكترونية تصاحب كلَّ ما هو موضوعي بكل ما هو إجرائي، وذلك لكي يتحقق التوازن بين الحق والمصلحة.

قائمة المراجع

أولاً:الكتب العامة :-

1- د.أمير فرج- سلطة القاضي الجنائي في تقدير الدليل الإلكتروني- دار المطبوعات الجامعية- من دون تاريخ نشر، ومن دون طبعه.

2- د. يزيد بوحليط- الجرائم الإلكترونية والوقاية منها في القانون الجزائري- دار الجامعة الجديدة - 2019 .

3-د. عادل حامد بشير – الإثبات الجنائي للجريمة الإلكترونية – دار النهضة العربية – الطبعة الأولى – سنة 2020 -2022.

4- د.على حسن الطوالبة- الجرائم الإلكترونية – جامعة العلوم التطبيقية كلية الحقوق – بدون طبعة – بدون تاريخ نشر .

5- د. محمود رجب فتح الله – الشرعية الجنائية للأدلة الرقمية – دراسة مقارنة – دار الجامعة الجديدة – سنة 2020

6- د. محمد على سويلم- مكافحة الجرائم الإلكترونية، دراسة مقارنة بالتشريعات العربية والأجنبية – دار المطبوعات الجامعية – الطبعة الأولى- سنة 2019.

7- د. محمد كمال شاهين – الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة – دار الجامعة الجديدة- سنة 2018.

ثانياً:الدراسات والبحوث العلمية :-

8- د. محمد عبد الحميد عرفه – مدى حجية الأدلة الإلكترونية الرقمية في الإثبات في المواد الجنائية، دراسة تحليلة تطبيقة مقارنة – مجلة الحقوق للبحوث القانونية والاقتصادية – كلية الحقوق جامعة الإسكندرية – العدد الأول- المجلد الأول- سنة 2018.

ثالثاً:الأطروحات والرسائل الجامعية :

9- د.محمد صلاح محمد عبدالمنعم – الجرائم الالكترونية وتحدياتها – دراسة مقارنة – رسالة دكتوراة – كلية الحقوق جامعة المنصورة – بدون سنة نشر.

10- د. دريف مصطفى – الإثبات الجنائي بالوسائل الالكترونية الحديثة – رسالة ماجستير – جامعة عبدا لحميد بن باديس مستغانم – سنة 2020-2021 .

رابعاً: القوانين واللوائح:-

11- قانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية- الجريدة الرسمية مجلس النواب الليبي ديوان مجلس النواب – العدد الأول- السنة الأولى – سنة 2023.

12- القانون رقم (6) لسنة 2022 بشان المعاملات الإلكترونية – الجريدة الرسمية – العدد الأول – السنة الأولى 2023.