وزارة التعليم العالي والبحث العلمي

جامعة عباس لغرور – خنشلة –

كلية الحقوق والعلوم السياسية

قسم الحقوق نيابة العمادة للدراسات وشؤون الطلبة

إثبات الجريمة الالكترونية في التشريع الجزائري

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في الحقوق

تخصص: قانون جنائي

من إعداد الطلبة:

- بوعجاجة مولدي
- دريدي عبد الحكيم

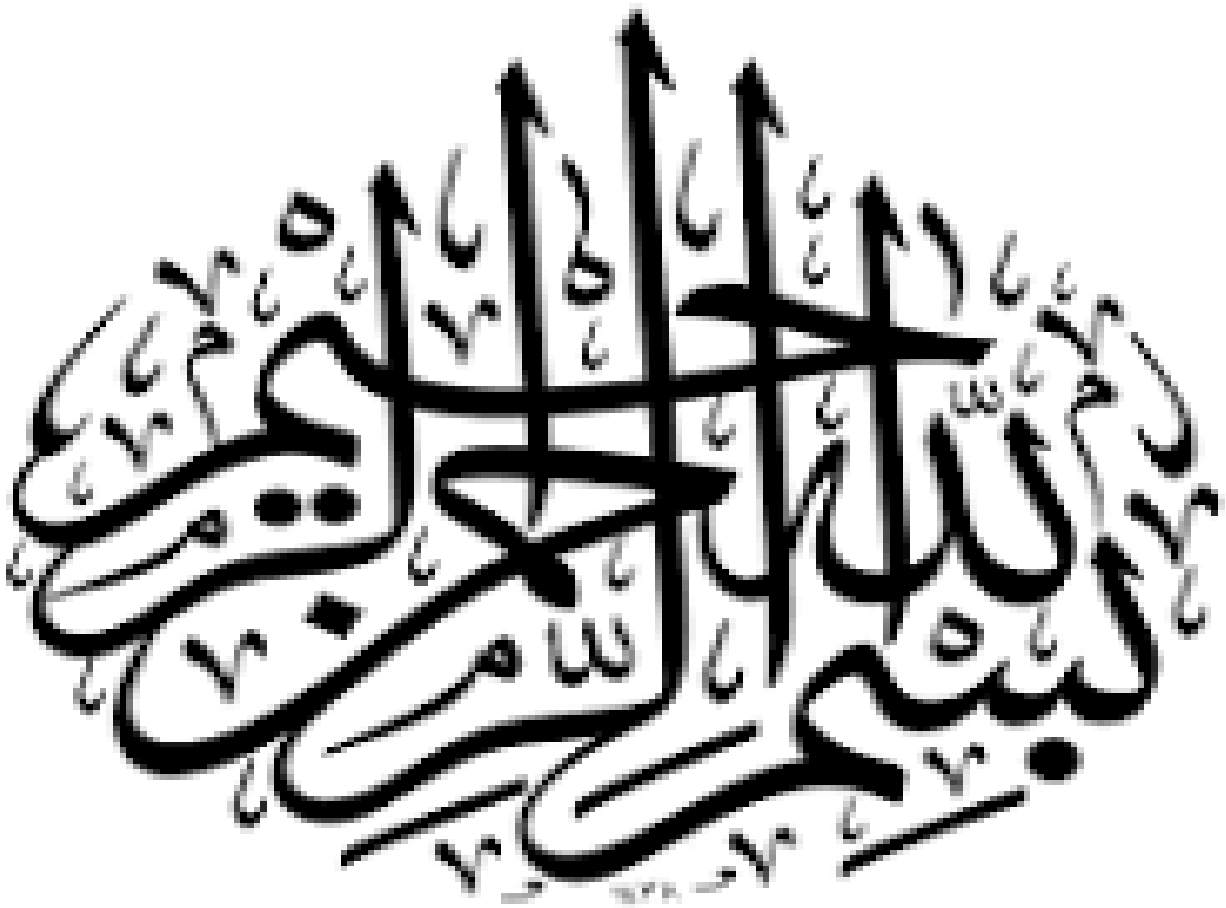
اشراف الأستاذ:

د. رمضاني السبتي

لجنة المناقشة

الأستاذ	الرتبة العلمية	الجامعة الأصلية	الصفة
خلاف بدر الدين	أستاذ التعليم العالي	جامعة عباس لغرور خنشلة	رئيسا
رمضاني السبتي	أستاذ محاضر أ	جامعة عباس لغرور خنشلة	مشرفا ومقررا
هباش عمران	أستاذ محاضر أ	جامعة عباس لغرور خنشلة	مناقشا

الموسم الجامعي 2024/2023



الشكر والتقديـر

الشكر الأول والأخير الله الواحد القهار، الذي يكور الليل على النهار تذكرة لذوي القلوب والأظفار والصلاة والسلام على سيدنا المختار، فالحمد لله حمدا تتم به الصالحات على توفيقه لنا و امدادنا بالعون وتيسير سبل إعداد هذا العمل المتواضع.

كما أتقدم بالشكر الى الدكتور المشرف "رمضاني السبتي" الذي لم يبخل علينا بنصائحه وتوجيهاته القيمة، فجزاه الله عز وجل خير الجزاء.

كما أتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة الذين تفضلوا بقبولهم مناقشة هذا العمل وقراءته وتصويبه فجزاهم الله عز وجل خير الجزاء.

كما لا يفوتني أن أعبر عن خالص امتناني لكل من كان لي عونا من قريب أو بعيد في إعداد هذا العمل، ونسأل الله التوفيق والسداد للجميع

الاهداء

اشكر أبي و أمي و اخوتي حسان ونبيل وأختاي واخوتي التي لم تلدهم امي خالد وسالم ورشدي وكيجي وكل من مد يد العون لي أشكركم جزيل الشكر

بوعجاجة مولدي

الاهداء

اشكر أبي و أمي و أخوتي عبد الله، حسان ،شعبان، رضوان، نور الدين وصديقي وليد ورشدي وكل صديق مد لي يد العون أشكركم جميعا كل واحد باسمه.

دريدي عبد الحكيم

مقدمة

المقدمة

المقدمة

تشهد مجتمعاتنا هذه الأيام تقدما رقميا كبيرا، يتسم بتطور التكنولوجيات الجديدة والتسهيلات التي تقدمها الأنترنت والذي يعتبر تقدما تكنولوجيا واجتماعيا فعلي، بالرغم ان الصعوبات والمخاطر التي تجلبها تمثل تحديات في الحاضر والمستقبل القريب، ولعل الرقي الذي تعيشه البشرية والتقدم المذهل في العقود الاخيرة من الزمن الذي شمل وسائل الاتصال والمعلومات تجسد في انتشار أجهزة الحاسب الآلي و واكبه من جهة أخرى تطور الفكر والعقل البشري الإجرامي و أدى بطبيعة الحال إلى إفراز أنواع جديدة من السلوك الإجرامي تمثلت في ظهور الجريمة المعلوماتية أو الإلكترونية و عرفت انتشارا واسعا بالأخص بعدما أصبحت العديد من الدول تعتمد عليها في تسيير مرافقها الحيوية كالدفاع والأمن والاقتصاد اين اصبح هذا النوع من الجرائم واقع ملموس يهدد وبشكل خطير حياة الأشخاص وممتلكاتهم في ظل العولمة.

ومن منطلق ان اهم خاصية تتميز بها الجريمة الإلكترونية هي صعوبة إثباتها باتفاق الفقهاء والدارسين في مجال المعلوماتية، وهو ما انعكس سلبا على العملية الإثباتية للجرائم المعلوماتية بالأخص مع عدم تناسب النصوص المنظمة لطرق الأثبات التقليدية مع طبيعة الجريمة الإلكترونية وتطورها بسبب الطابع الخاص والتقني لهذه الجرائم التي تتم في بيئة غير مادية لا علاقة لها بالمستندات وعملية إثباتها تقتضي البحث عن الدليل المناسب ما استلزم على المشرعين تبني أنواع جديدة من الأدلة الرقمية مع حرصهم على توفير الغطاء التشريعي لها.

ونظرا إلى أن الجريمة الإلكترونية من الموضوعات التي تتميز بندرة التطبيقات القضائية فيها، فإنه برز للوجود مسألة حجية الدليل الرقمي الذي يعد آلية إثبات في مجال جرائم المعلوماتية، فالقواعد العامة أصبحت قاصرة عن مواجهة خصوصية هذه الجرائم، خاصة بعد أن أصبح المجتمع المعلوماتي حقيقة لا يمكن الاستغناء عنها، وأصبحت المجتمعات المعاصرة تعتمد على البيئة الرقمية وازداد التوجه نحو التخلي عن الوثيقة في المعاملات المختلفة بما فيها عملية

الإثبات، مما أدى إلى استحداث أشكال جديدة من الأدلة في الإثبات الجنائي، استوجب توفرها على شروط معينة لاعتبارها دليلا كاملا يمكن من خلالها دحض قرينة البراءة واثبات عكسها عندما يصل اقتناع القاضي إلى حد الجزم واليقين.

1- أهمية الموضوع

تكمن أهمية هذه الدراسة في التعرف على الجريمة الإلكترونية لاسيما من حيث ضبطها وإثباتها، لأنه لا يختلف اثنان في أن أساس توقيع العقوبة على المتهم يكمن في إثبات إدانته وذلك بإقامة الأدلة عليه، لذا فإن الإثبات يعتبر موضوعا في غاية الأهمية، علما أن أهمية التحقيق الجنائي تتجلى في تحديد إجراءات التحقيق في الجرائم الإلكترونية، بالإضافة إلى التعريف بالبرامج والأنظمة الخاصة التي تساعد في إثبات مثل هذه الجرائم، والتي ينبغي على رجال الضبطية القضائية من جهة والقضاء من جهة أخرى معرفتها الإثبات وقوع هذه الجرائم.

2- أهداف الدراسة:

رغبة منا في تسليط ضوء الأهمية على هذه الجريمة، و كذا معرفة مدى مواكبة القانون للتطور التكنولوجي، وكيفية تعامله مع الأدلة الرقمية والكشف عن مدى حجية الدليل الإلكتروني في مجال الإثبات الجنائي.

3- أسباب اختيار الموضوع

تتمثل أسباب اختيار الموضوع في ما يلي:

- **أسباب ذاتية** تعود إلى الفضول الكبير الذي أحدثته الجرائم في نفسيتنا وإلى الأنماط الجديدة من الجرائم التي لم يكن لنا عهد بها سابقا وما صاحبه من اثر شمل العالم بأسره، حيث وقع اختيارنا على هذا الموضوع علنا نقدم نسق وإفادة في التعريف بها مستقبلا.

- **أسباب موضوعية** من بين الأسباب الموضوعية الرئيسية التي جعلتنا نختار هذا الموضوع المتمثل في إثبات الجريمة الإلكترونية في التشريع الجزائري كونه من الموضوعات التي ترقى

إلى مصاف المواضيع الحديثة بحكم الوسائل المستخدمة في ارتكاب الجريمة الإلكترونية، وصعوبات الإثبات بصفة عامة، كما يسمح لنا بملامسة طرق إثبات هذه الجريمة ومعرفة قيمة الدليل الرقمي الذي تثبت به أمام القضاء.

4- المنهج المتبع

اعتمدنا في دراستنا على المنهج الوصفي من حيث معرفة مواصفات الدليل الإلكتروني والتي جعلته يتميز عن باقي الأدلة، إلى جانب استخدام المنهج التحليلي وهذا بغرض تحليل الموضوع من الناحية القانونية الإجرائية .

5- صعوبات الدراسة

لحسن حظنا ونحن بصدد هذه الدراسة لم نواجه صعوبات كبيرة، وهذا راجع لوفرة المراجع في مجال الجريمة الإلكترونية بصفة عامة وإثباتها بصفة خاصة، ماعدا في التشريع الجزائري، حيث أنه لم يولي اهتمام كبيرا لموضوع إثبات الجريمة الإلكترونية بالطرق الحديثة أو ما يسمى بالدليل الالكتروني، حيث لم نجد نصوص قانونية صريحة تعنى بالدليل الرقمي في هذا الموضوع.

6- الدراسات السابقة

معظم الدراسات السابقة التي اطلعنا على محتواها ونحن بصدد انجاز مذكرتنا هذه، جاءت بمعظم الأفكار التي يجب التطرق إليها في هذا الموضوع، منها أطروحة دكتوراه للباحثة نبيلة هبة هروال، جرائم الأنترنت دراسة مقارنة، جامعة تلمسان، الجزائر 2013-2014، والتي كانت مشابهة لعنوان بحثنا.

رسالة ماجستير للباحث يوسف صغير، الجريمة المرتكبة عبر الأنترنت، جامعة مولود معمري، تيزي وزو الجزائر 2013، والتي كانت ايضا مشابهة لعنوان بحثنا.

7- الاشكالية

من خلال ما تم التنويه عنه سابقا وبالنظر إلى أهمية الموضوع فان محاولة الإلمام به وتحليله تطلب التطرق إليه وفق الإشكالية الآتية:

ماهي طرق إثبات الجريمة الإلكترونية والمعايير التي يخضع لها لإثباتها في التشريع الجزائري؟

ويترتب عن هذه الاشكالية عدة اسئلة فرعية:

- ما هي الأدلة العلمية الحديثة وأهميتها في تحقيق الإثبات الجنائي؟

- هل يعتبر الدليل الالكتروني دليلا كاملا للإثبات الجنائي؟

لمعالجة الإشكالية المطروحة و الإجابة عن باقي التساؤلات الفرعية التابعة لها

تم تقسيم الدراسة إلى فصلين:

الفصل الأول بعنوان **الإطار المفاهيمي للجريمة الالكترونية** حيث قسمناه الى مبحثين، المبحث الأول **ماهية الجرائم الالكترونية،** أما المبحث الثاني فكان عنوانه **تصنيف الجرائم الالكترونية.**

أما فيما يخص الفصل الثاني فقد عنوناه **اثبات الجريمة الالكترونية حجية الدليل الالكتروني في الاثبات،** والذي بدوره قسمناه الى مبحثين، حيث تناولنا في المبحث الأول **ضبط الجريمة الالكترونية وطرق اثباتها،** والمبحث الثاني **حجية الدليل الرقمي في اثبات الجريمة الالكترونية.**

وتوجنا بحثنا بخاتمة تضمنت مجموعة النتائج والتوصيات

الفصل الأول: الإطار المفاهيمي للجريمة الالكترونية

الفصل الأول: الإطار المفاهيمي للجريمة الالكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة والتي ظهرت في عصرنا الحديث والسبب يعود إلى ارتباط هذه الجرائم بوسائل التقنيات الحديثة من أجهزة كمبيوتر وشبكات الأنترنت والمواقع الإلكترونية، أما عن مفهوم الجرائم الإلكترونية فإنه لا يوجد إلى الوقت الحالي تعريف جامع مانع لهذا النوع من الجرائم، وقد اختلف الفقه القانوني في تعريفها[1]، وستتطرق من خلال هذا الفصل إلى **ماهية الجرائم الإلكترونية** في **المبحث الأول** وإلى **تصنيف الجرائم الالكترونية** في **المبحث الثاني**.

[1] اسمهان بوضياف، الجريمة الالكترونية والإجراءات التشريعية في مواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، الجزائر، العدد الحادي عشر، سبتمبر 2018،ص 350.

المبحث الأول: ماهية الجرائم الالكترونية

تعد الجرائم المعلوماتية من الجرائم المستحدثة والتي ظهرت في عصرنا الحديث والسبب يعود إلى إرتباط هذه الجرائم بوسائل التقنيات الحديثة من أجهزة كمبيوتر وشبكات الأنترنت والمواقع الإلكترونية، تعد الأنترنت من أكبر شبكات الكمبيوتر ذات الإرتباط الوثيق بالجرائم المعلوماتية وكلمة انترنت (Internet) وفي اللغة مشتق من اللغة الإنجليزية (Internet Network) أي شبكة التشبيك ويعني أنها شبكة تربط مجموعة من أجهزة الكمبيوتر المتصلة ببعضها البعض وتستطيع تبادل المعلومات فيما بينها، أما عن مفهوم الجرائم المعلوماتية فإنه لا يوجد إلى الوقت الحالي تعريف جامع مانع لهذا النوع من الجرائم[1]وسنتناول في هذا المبحث إلى **مفهوم الجريمة الالكترونية** من خلال تعريفها وهذا في المطلب الأول وإلى خصائص **وأسباب الجريمة الالكترونية** وهذا في المطلب الثاني.

المطلب الأول: مفهوم الجريمة الالكترونية وأركانها.

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية بإساءة استخدام الكمبيوتر"، ثم احتيال الكمبيوتر"، "فالجريمة المعلوماتية"، بعدها جرائم الكمبيوتر"، و"الجريمة المرتبطة بالكمبيوتر"، ثم "جرائم التقنية العالية"، إلى "جرائم الهاكرز"، "فجرائم الأنترنت"، وأخيرا "السيبركرايم".[2]

الفرع الأول: تعرف الجريمة الالكترونية

أولا: التعريف اللغوي

الجريمة لغة كلمة مشتقة من الجرم وهو التعدي أو الذنب وجمع الكلمة إجرام وجروم وهو الجريمة وقد جرم يجرم واجترم وأجرم فهو مجرم جريم، وهي طبقا للمفهوم الاجتماعي

[1] اسمهان بوضياف، المرجع السابق، ص350.

[2] مليكة عطوى، الجريمة المعلوماتية، حوليات جامعة الجزائر، ع 21، جوان 2012، ص 08.

كل سلوك إرادي غير مشروع يصدر عن شخص مسؤول جنائيا في غير حالات الإباحة عدوانا على مال أو مصلحة أو حق محمي بجزاء جنائي.[1]

وعرفت الجريمة أيضا: "على أنها على فعل غير مشروع صادر عن إرادة ..... يقرر له القانون عقوبة أو تدبيرا احترازيا، وتعتمد الجرائم الناشئة عن الاستخدام غير المشرع لشبكة الأنترنت على المعلومة بشكل رئيسي".[2]

الجريمة كلمة مأخوذة من الجرم وهي الذنب والجناية جمعها جرائم، وجرم الشيء قطعه وجرمه الرجل على قومه وإليهم، ذنب وجنى جنته.

ثانيا: التعريف الاصطلاحي

للوقوف على مفهوم الجريمة الالكترونية يقتضي منا الحال التعرض الى التعريف الفقهي لهذه الجريمة ومن ثم تبيان التعريف التشريعي.

أ- التعريف الفقهي للجريمة الالكترونية

بذل الفقه جهودا في محاولة لوضع تعريف محدد لماهية الجريمة الالكترونية وانقسم الفقه بين اتجاهين الأول يضيق من مفهوم الجريمة الالكترونية والآخر يوسع من مفهومها.[3]

ومن التعريفات التي وضعها أنصار الاتجاه الضيق أن الجريمة الالكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى، كما عرفها هذا الاتجاه بأنها هي التي تقع على جهاز الكمبيوتر أو داخل

[1] نبيلة هبة هروال، جرائم الأنترنت دراسة مقارنة، أطروحة دكتوراه، ، جامعة تلمسان، الجزائر 2014-2013، ص 12.

[2] يوسف صغير، الجريمة المرتكبة عبر الأنترنت، رسالة لنيل شهادة الماجستير، رسالة ماجستير، جامعة مولود معمري، تيزي وزو الجزائر 2013، ص 7.

[3] عادل محمد فريد نائلة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط1، بيروت، لبنان، 2005، ص 27.

نظامه فقط، أو هي "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه".[1]

بينما عرف أصحاب الاتجاه الواسع الجريمة الالكترونية بأنها: "كل سلوك إجرامي يتم بمساعدة الكمبيوتر"، أو هي كل جريمة تتم في محيط أجهزة الكمبيوتر".

أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو ينقلها.

وإذا كان مفاد هذه التعريفات أن الجريمة المعلوماتية هي كل نشاط إجرامي يؤدي فيه نظام الكمبيوتر دورا لإتمامه على أن يكون هذا الدور مؤثر في ارتكاب الجريمة ولا يختلف الأمر سواء أكان الكمبيوتر أداة لإتمام الفعل الإجرامي أم كان محلا لها إلا أن البعض يذهب أنه عند وضع تعريفا محدد للجريمة المعلوماتية يجب مراعات عدة اعتبارات هامة وهي:[2]

1- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.

2- أن يراعي في وضع التعريف التطور السريع والمتلاحق لتكنولوجيا المعلومات والاتصالات.

3- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.

ب- **التعريف القانوني للجريمة الالكترونية**

على خلاف المشرع الفرنسي الذي لم يعط تعريف للجريمة الإلكترونية فإن المشرع الجزائري قد اصطلح على تسميتها الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[3]"، حيث لم يعرف

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 75.

[2] عادل محمد فريد نائلة، المرجع السابق، ص 32.

[3] رحيمة نمديلي، خصوصية الجرائم الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الجرائم الإلكترونية، المنعقد بطرابلس يومي 24، 25 مارس 2017، ص100.

الجرائم الإلكترونية وإنما تبنى للدلالة على الجريمة مصطلح " المساس بأنظمة المعالجة الآلية للمعطيات[1]".

واستنادا لقانون العقوبات الجزائري المعدل والمتمم الذي لم يعرف الجرائم الإلكترونية واكتفى بالعقاب على بعض الأفعال تحت عنوان "الجرائم الماسة بالنظام المعالجة الآلية للمعطيات[2]."

وقد عرف المشرع الجزائري في نص المادة 02 من قانون 09/04 الجريمة الإلكترونية على أنها:

جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[3]".

ومما تجب الإشارة إليه، أن مصطلح نظام المعالجة الآلية للمعطيات تعبير ذا طابع فني تقني يصعب على القانوني إدراك مغزاه ببساطة، فضلا على أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسب الآلي.[4]

ومنه نخلص الى أن الجريمة الالكترونية هي تلك الجرائم الناتجة عن استخدام التقنية الحديثة والمتمثلة في الكومبيوتر والانترنت في أعمال اجرامية

فاذا كان هذا هو مفهوم الجريمة الالكترونية فماهي اركان هذه الجريمة؟ وهو ما سنتعرف عليه في الفرع التالي:

---

[1] قانون رقم 09-04 المؤرخ في 5-08-2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها، ج ر رقم 47 مؤرخ في 06-08-2009.

[2] قانون رقم 04-15 المؤرخ في 10-11-2004 يعدل ويتمم الأمر رقم 15666، يتضمن قانون العقوبات، ج ر عدد 71 مؤرخ بتاريخ 10-11-2004المعدل والمتمم.

[3] رحيمة نمديلي، المرجع السابق، ص100.

[4] محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخداماتها، مجلة الحقيقة، العدد 41 دط، 2018، ص، 438.

الفرع الثاني: أركان الجريمة الالكترونية

تتكون الجريمة الإلكترونية من ركنين الركن المادي والركن المعنوي وإذا تخلف أحدهما اعتبر الفعل غير مجرم قانونا.

أولا: الركن المادي

لابد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل.

وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر. وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها ، وهذا ما يدعو للتدخل التشريعي".[1]

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة كالتبليغ عن الجريمة قبل تحقيق نتيجتها، (مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة أنه لا مناص من معاقبة الفاعل).

[1] شريفة بن غدفة ، القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها، أعمال الملتقى الوطني. "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 48

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب (مثلا : جريمة الغش المعلوماتي الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية.[1]

ثانيا: الركن المعنوي للجريمة الإلكترونية

تعد الجرائم المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم والإرادة لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود القصد الخاص في الجرائم المعلوماتية، فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع أو ارتكاب الجريمة.[2]

– يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين هما العلم والارادة.

– العلم هو إدراك الفاعل للأمور.

– أما الإرادة فهي اتجاه السلوك الإجرامي لتحقيق النتيجة.

طبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخاصا القصد الجنائي العام هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود إرتكاب الفعل.

أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارك الجريمة، بل يذهب إلى التأكل على تحقيق النتيجة (مثلا: في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه وعليه ما هو القصد الجنائي الذي يجب توافره في الجريمة الإلكترونية.

[1] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية طرابلس بتاريخ 24-25 مارس 2017، ص ص 119-120

[2] اسمهان بوضياف المرجع السابق، ص 354.

الأصل إن الفاعل في الجريمة الإلكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام.[1]

إذن فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص (مثلا: جرائم تشويه السمعة عبر الأنترانت، وجرائم نشر الفيروسات عبر الشبكة) وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.[2]

أن القصد العام والخاص في جرائم المعلوماتية هو أساسي لتحديد المسؤولية الجزائية، والذي يحدد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونية الإضرار أو النية الخاصة للجاني والتي يمكن استشفائها من مكونات كل جريمة على حدا وبشكل مستقل، وبالتالي فإن الجرائم المعلوماتية وكجرائم مستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي لقيام الجريمة ولا يتصور قيام أي نوع من أنواع الجرائم المعلوماتية دون وجود الركن المعنوي.

أما عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا، والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات وتمحيصها بما لها من صلاحية باعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها.[3]

المطلب الثاني: خصائص وأسباب الجريمة الالكترونية

[1] اسمهان بوضياف المرجع السابق، ص 355.

[1] فضيلة عاقلي: المرجع السابق، ص 120.

[3] اسمهان بوضياف: المرجع السابق، ص 355.

في هذا المطلب سنحاول بيان خصائص هذه الجريمة وذلك بالتطرق للسمات الخاصة بالجريمة الإلكترونية والسمات الخاصة بالمجرم الإلكتروني وتنوع هذه الجريمة في التشريع الجزائري بحسب ما إذا ارتكبت باستخدام النظام المعلوماتي، أو كانت موجهة ضده، وهذا ما سنتطرق إليه في الفروع التالية.

الفرع الأول: خصائص الجريمة الالكترونية

تعتبر الجريمة المرتكبة عبر الأنترنت من بين الجرائم المستحدثة التي أتى بها التطور في مجال الاتصالات، فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي، ولذلك تتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل، وسوف نسرد هذه الخصائص التي ميزت الجريمة الإلكترونية عبر الأنترنت على النحو التالي:

أولا: جريمة عابرة للقارات

من أهم الخصائص التي تميز الجريمة الإلكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الأنترنت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد بسبب السرعة الهائلة في تنفيذها، فيمكن أن تقع الجريمة في دولة من طرف الجاني و المجني عليه في دولة أخرى في وقت يسير جدا.[1]

ثانيا: جرائم صعبة الاثبات

صعوبة متابعتها واكتشافها بحيث لا تترك أثرا، فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها. ويلاحظ أن

[1] نهلا عبد القادر مومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الأولى، عمان، 2008، ص 50.

الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها على أساس أنها تفتقر إلى الدليل المادي التقليدي كالبصمات، كما يصعب الاحتفاظ الفني بآثارها أن وجدت، وتحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها، لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل، وقد يلجا مرتكبها لتشفير التعليمات لمنع إيجاد أي دليل يدينه.[1]

ثالثا: جرائم ناعمة

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل السرقة وغيرها، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع، ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما.[2]

رابعا: جريمة مغرية للمجرمين

نظراً للصفات التي تتمتع بها مثل هذه الجريمة، والصعوبات التي تثور عند محاولة اكتشافها أو ملاحقتها، فإن ذلك يشكل إغراء كبيراً للمجرمين وخصوصاً أنه يمكن تحقيق مكاسب طائلة من وراء مثل هذا النوع من الجرائم، ونتيجة لكل ما سبق تعد مثل هذه الجرائم جريمة تستهوي الكثيرين لسهولتها، وكثرة مكاسبها.[3]

---

[1] هشام محمد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي العدد 02، 1999، ص24.

[2] عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، مصر، 2006، ص 46.

[3] عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية –دراسة مقارنة– أطروحة ماجستير، جامعة الشرق الأوسط 2014، ص22.

الفرع الثاني: أسباب الجريمة الالكترونية

لا شك أن مرتكبي الجريمة الإلكترونية يختلفون عن مرتكبي الجريمة التقليدية، ويرجع ذلك لاختلاف الاشخاص من حيث السن والجنس والمستوى التعليمي وغير ذلك من المؤثرات الخارجية، كما أن الأسباب أو الدوافع التي تدفعهم لارتكاب الجريمة هي أيضاً تختلف، حيث أنها العوامل المحركة للإرادة التي توجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام وكسب المال، فهي القوة النفسية التي تدفع الإرادة لارتكاب الجريمة ابتغاء تحقيق غاية معينة، ولذلك فإن الجريمة الالكترونية تختلف عن الجريمة التقليدية، وتبعاً لذلك فأن الأسباب والدوافع التي تدفع الجناة لارتكاب الفعل غير المشروع لها تختلف عن الاسباب والعوامل التي تدفع الجناة لارتكاب الفعل غير المشروع للجريمة التقليدية،[1] ويأتي في مقدمة أسباب ودوافع الجريمة الإلكترونية، ثمة أسباب ودوافع تتمثل في الرغبة أو الولع بجمع المعلومات التي قد تكون محفوظة في أجهزة الحاسب الآلي أو منقولة عبر الشبكة العالمية للمعلومات كما قد تكون الأسباب والدوافع الرغبة في الاضرار بالغير من جهات معينة وأشخاص وكذلك الرغبة في الربح والكسب الذي قد يدفع إلى التعدي على الحواسيب ونظم المعلومات إضافة إلى الدوافع الشخصية للجاني لإبراز الذات التي قد تكون سبباً في ارتكاب الجريمة المعلوماتية وتذكر بعضاً من تلك الأسباب والدوافع فيما يلي:

1 – الرغبة في جمع المعلومات وتعلمها.

أن الدخول إلى أنظمة الحاسب الآلي يمكن أن يعلمك كيف يسير العالم، والثاني أن جمع المعلومات يجب أن يكون غير خاضع للقيود، ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص، وكثيراً ما نجد أن قراصنة الأنظمة

[1] اعداد مجمع البحوث والدراسات، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016، ص27.

يعلنون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب الالكترونية هو التعلم فقط، فهم يتعاونون في البحث على شكل جماعات ويتقاسمون المعلومات والخبرات التي يحصلون عليها ويستفيدون منها في أنشطة هادفة ولو بطرق غير مشروعة.[1]

2- قهر النظام وإثبات التفوق على تطور وسائل التقنية.

في بعض الأحيان يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام وإثبات قدرة الجاني وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة، حيث يمضي كل وقته أمام شاشات أجهزته لكسر الحواجز الأمنية للأنظمة الالكترونية واختراقها لشت براعته في القدرة على تحدي أي تطور جديد في عالم التقنية والتكنولوجية.[2]

3- الضغوطات العامة

إن مصادر الضغوط لا تتوقف على الإحباط الذي يخبره الفرد عندما تسد الطرق لتحقيق هدف ما، وإنما يشمل المشاعر السلبية التي تحدث في المواقف الاجتماعية المتنوعة كما قد تلعب العوامل الاجتماعية والاقتصادية أيضا دورا هاما في زيادة الجريمة الإلكترونية، فالضغط على مؤسسات القطاع الخاص لخفض الإنفاق وخفض مستويات التوظيف يمكن أن يؤدي، على سبيل المثال، إلى تخفيضات في الأمن، وإلى فرص الاستغلال ثغرات وضعف تكنولوجيا المعلومات والاتصالات والشركات، مما يضطر لتوظيف المتعاقدين من الخارج أو المؤقتين، أو يصبح هناك موظفين ساخطين بسبب انخفاض الأجور والخوف من فقدان الوظيفة، والخطر يزداد من الأعمال الإجرامية والنفوذ من قبل منظمة إجرامية.[3]

[1] مجمع البحوث والدراسات، المرجع السابق، ص 28

[2] مجمع البحوث والدراسات، المرجع السابق، ص 28

[3] موسى البداينة ذياب، الجرائم الالكترونية –المفهوم والأسباب– ورقة مقدمة في الملتقى العلمي، – الجرائم المستحدثة في ضل التغييرات والتحولات الاقليمية والدولية، المملكة الأردنية الهاشمية، عمان، 2014، ص 12.

المبحث الثاني: تصنيف الجرائم الالكترونية

تصنف الجريمة التقليدية بحسب خطورتها إلى جناية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية،[1] على خلاف هذه الجريمة ، فإن الجريمة الإلكترونية عرفت اختلاف حول تقسيماتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدى عليه بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال، وسنتطرق في هذا المبحث إلى **الجرائم الواقعة بواسطة نظام المعلوماتية** وهذا في **(المطلب الأول)** وإلى **الجرائم الواقعة على النظام المعلوماتية والبرامج الالكترونية** في **(المطلب الثاني)**.

المطلب الأول: الجرائم الواقعة بواسطة نظام المعلوماتية

هنا لا يكون النظام المعلوماتي هو محل الجريمة، بل يكون الحاسب الآلي هو الوسيلة لتسهيل النتيجة الإجرامية باستخدام النظام المعلوماتي ويكون الهدف من ورائها الربح بطريق

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، ط1، 2002، ص 24.

غير مشروع الاعتداء على أموال الغير، الاعتداء على الأشخاص وسلامتهم وحياتهم الخاصة، أو في سمعتهم وشرفهم والاعتداء على أمن الدولة وأسرارها.[1]

الفرع الأول: الجرائم الواقعة على الأشخاص

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة بشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته.

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، ويقوم بنشرها عبر الأنترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإرادة على ذلك،[2] ورغم الإيجابيات والفوائد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد، إلا أنها جعلته أكثر عرضة للانتهاك، ومنها:

1- جريمة التهديد:

وهو الوعيد يقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان، وتخويفه من اضرار ما ستلحقه أو ستلحق أشخاص له بها صلة، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بالحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس أو

[1] سورية ديش، أنواع الجرائم الالكترونية وإجراءات مكافحتها، مجلة الدراسات الاعلامية، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، العدد الأول، يناير 2018، ص 241.

[2] اسمهان بوضياف، المرجع السابق، ص 353.

مال الغير، ولا يشترط أن يتم إلحاق الأذى فعلا أي تنفيذ الوعيد، لأنها تشكل جريمة أخرى قائمة بذاتها، تخرج من إطار التهديد الى التنفيذ الفعلي، وقد يكون التهديد مصحوبا بالأمر أو طل لقيام بفعل أو الامتناع عن الفعل، أو لمجرد الانتقام، ولقد أصبحت الانترنت الوسيلة لارتكاب جرائم التهديد، والتي في حد ذاتها تحتوي عدة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة كالبريد الإلكتروني أو الويب.[1]

2- جرائم السب والقذف:

تعد جرائم القذف والسب من أكثر الجرائم شيوعا في نطاق الشبكة المعلوماتية، إذ يتم استخدامها للنيل من شرف الغير أو كرامته أو اعتباره، ويتم السب والقذف على شكل رسالة بيانية أو عن طريق المطبوعات وذلك عن طريق المبادلات الإلكترونية، ويستعمل الجاني حسب القواعد العامة لجرائم القذف والسب عبارات بذيئة تمس وتخدش شرف الجاني عليه، ومهما كانت الوسيلة المعتمدة، مع علمه أن ما يقوم به بعد مساسا بسمعه الغير، بل إن إرادته اتجهت لذلك بالذات، وبالتطور أصبحت الإنترنت إحدى هذه الوسائل إذ لم نقل أكثرها رواجا، فعادة ترسل عبارات السب والقذف عبر البريد الصوتي أو تكتب على صفحات الويب ما يؤدي بكل ما يدخل هذا الموقع لمشاهدتها أو الاستماع إليها، ويتحقق بذلك ركن العلنية الذي تطلبه الكثير من التشريعات في السب العلني.[2]

الفرع الثاني: الجرائم الواقعة على الأموال

أصبحت المعاملات الشراء، البيع والإيجار تتم عبر الشبكة المعلوماتية، فابتكرت معه طرق ووسائل للسطو على هذا التداول المالي بطريق غير مشروع، كالتحويل الإلكتروني، السرقة، القرصنة وغيرها.

---

[1] سورية ديش، المرجع السابق، ص 242.

[2] محمد أمين، أحمد الشوابكة، جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2004، ص 30.

1- السرقة الواقعة على البنوك:

يتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم، والاستخدام الشخصية الضحية ليقوم بعملية السرقة المتخفية، ما يؤدي بالبنك إلى التحويل البنكي للأموال الالكتروني أو المادي إلى الجاني، حيث يستخدم الجاني الحاسب الآلي لدخول شبكة الانترنت والوصول إلى المصارف والبنوك، وتحويل الأموال الخاصة بالعملات إلى حسابات أخرى،[1] وعملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك، يتم فيها نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية، أو إنشاء صفحة أنترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها رسائل البريد الواردة من مصادر مجهولة التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي، والأمثلة كثيرة ..

2- تجارة المخدرات عبر الأنترنيت:

تتعلق بالترويج للمخدرات وبيعها، والتحريض على استخدامها، وصناعتها بمختلف أنواعها.

3- غسيل الأموال:

تمارس عبر الأنترنيت، حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل أموالهم، بتوفير السرعة، وتفادي الحدود الجغرافية،

[1] عباس أبو شاما، التعريف بالظواهر الاجرامية المستحدثة – حجمها، أبعادها، ونشاطها في الدول العربية– الندوة العلمية للظواهر الاجرامية المستحدثة وسبل مواجهتها، تونس، أيام 29–30 جوان 1999، ص 20.

والقوانين المعيقة لغسيل الأموال، وكذا لتشفير عملياتهم وسهولة نقل الأموال واستثمارها لإعطائها الصبغة الشرعية.[1]

4- الاستعمال غير الشرعي للبطاقات الائتمانية:

رافق استخدام البطاقات الائتمانية، الاستيلاء عليها باعتبارها نقود الكترونية إما بسرقة أرقام البطاقات ثم بيع المعلومات للآخرين، من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسب الآلي للضحية عن طريق الاحتيال، وذلك بإيهامه بحصول ربح، فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله،[2] أو إساءة استخدام الغير البطاقات الائتمانية، كان يقوم السارق استعمال البطاقة للحصول على السلع والخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة.

الفرع الثالث: الجرائم الواقعة على أمن الدولة

استغلت الكثير من الجماعات المتطرفة الطبعة الاتصالية للأنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في استعمال الأنترنت، التي سمحت لهم في ارتكاب جرائم غاية الشك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الأنترنت لكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية الاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون فيها نزاعات، ويبقى المساس بالأمن الفكري من بين اخطر الجرائم المرتكبة عبر الأنترنت، حيث

[1] صالحة العمري، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، العدد5 جامعة محمد خيضر بسكرة، د، س، ن، ، ص 179.

[2] صغير يوسف، المرجع السابق، ص 45.

تعطي الأنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى.[1]

1- الارهاب الالكتروني

يعرف الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو عرضه أو عقله أو ماله، بغير حق بشتى صنوف وصور الإفساد في الأرض. ولم يكن للجماعات الإرهابية أن تلجأ إلى وسائل الاتصال المستحدثة لارتكاب الجرائم الإلكترونية لإحداث أضرار جسيمة في دولة، أو خلق جو من عدم الاستقرار والرعب والفوضى أو في سبيل الضغط على أي دولة لتلبية طلباتهم الغير مشروعة، بالإضافة إلى ذلك يمكن أيضا للجماعات الإرهابية أن تستعمل هذه التكنولوجيا لنشر أفكارهم المتطرفة والترويج لأنفسهم عبر الشبكة العالمية "الإنترنت" كوسيلة اتصال فيما بين أعضائها، والتي تفلت غالبا من رقابة السلطات العمومية.[2]

ومهما كانت فئة المجرم المعلوماتي لا يمكن له أن يكون مرتكبا للإرهاب الإلكتروني إلا إذا نتج عن تصرفه إحداث عدم الاستقرار والخوف في دولة معينة، وبالتالي يعد من الجرائم الإلكترونية الإرهابية مثلا إذا اخترق هاكرز النظام المعلوماتي الخاص بإدارة وتنظيم توزيع الكهرباء في ولاية ما وتسبب في إتلافه وانقطاع الكهرباء، فهذا التصرف حسب رجال القانون يعد عملية إرهابية.

2- الجريمة المنظمة

[1] اسمهان بوضياف، المرجع السابق، ص 358.

[2] نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة ماجستير، جامعة منتوري، قسنطينة 2012/2013، ص- ص 157-158.

عرفها المؤتمر الخامس لمنع الجريمة ومعاملة المجرمين الذي انعقد في جنيف عام 1975 بأنها:

"الجريمة التي تتضمن نشاطا إجراميا معقدا وعلى نطاق واسع، تنفذه مجموعة من الأشخاص على درجة من التنظيم، ويهدف إلى تحقيق ثراء للمشتركين فيها على حساب المجتمع وأفراده، وهي غالبا ما تتم عن طريق الإهمال التام للقانون وتتضمن جرائم ضد الأشخاص ونكون مرتبطة في معظم الأحيان بالفساد السياسي".[1]

ولقد انتقد التعريف السابق لأنه لم يشر إلى المنظمة الإجرامية بشكل مباشر، بل ركز على السلوك الإجرامي دون بيان العناصر الأساسية لقيام المنظمة الإجرامية، ومنها الدوام والاستمرار، والتخطيط لارتكاب الجريمة أو استخدام وسائل العنف أو التهديد بارتكابها.[2]

المطلب الثاني: الجرائم الواقعة على النظام المعلوماتية والبرامج الالكترونية

إضافة إلى الجرائم الالكترونية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية يمس النظام المعلوماتي ويستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي.

الفرع الأول: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

قد عالج المشرع الجزائري هذا النمط من الجرائم من خلال نص المادة 394 مكرر من قانون العقوبات والتي تنص على أنه يعاقب بالحبس من سنة (6) أشهر إلى ثلاث (3) سنوات وبغرامة مالية من 5000.00 دج إلى 20.000.00 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها،

[1] جهاد محمد البريزات، الجريمة المنظمة –دراسة تحليلية–، دار الثقافة للنشر والتوزيع، ط1، عمان، 2008، ص331.

[2] المرجع نفسه.

من خلال هذا النص ومن أجل معالجة عناصر هذه الجريمة يتوجب تحديد معنى الإتلاف ثم الوسائل التي يتحقق بها الإتلاف.

يعرف البعض الإتلاف بأنه هو ذلك الفعل الذي يجعل الشيء غير الصالح للاستعمال أو بإعدام صلاحيته أو تعطيله وقف عمله سواء بصفة كلية أو جزئية.

ويقصد كذلك بالإتلاف إفناء مادة الشيء أو هلاكه كليا وبالتالي توقف الشيء تماما على أن يؤدي منفعته ولو لم تفنى مادته سواء كان هذا التوقف كليا أو جزئيا و يكون الشيء غير صالح للاستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الأكمل.[1]

كما يقصد أيضا بإتلاف برامج الحاسوب الآلي ومعلوماته إتلاف أو محو تعليمات البرامج والبيانات ذاتها ويطلق عليها مصطلح تدمير نظم المعلومات وعادة لا يستهدف مرتكب هذا الاعتداء فائدة مالية لنفسه بل لمجرد إعاقة نظام المعلومات

وعلى ضوء هذه التعريفات يمكن القول بأن الإتلاف لا يتحقق فقط في التأثير على مادة الشيء بل يتحقق كذلك حتى في حالة الانتقاص من قيمة الشيء الاقتصادية مما يعني أن الحكمة من الإتلاف هي ليس التعرض لمادة الشيء وإنما العبرة بمدى مساس الفعل بقيمته المالية ذلك أن الفعل الذي يترتب عنه فقدان الشيء لقيمته المالية أو الانتقاص منها هو الذي يحقق الاعتداء الذي يعاقب عليه القانون على اعتبار أنه قد ذهب بأهمية الشيء بالنسبة لمالكه.

ومن أجل الإشارة إلى مدلول الإتلاف استخدم المشرع الجزائري عدة تعابير حيث استخدم عبارة أزال، عدل وإن كان لهذه التعابير مدلولات خاصة إلا أنها تندرج تحت مدلول الإتلاف وهو ما ذهبت إليه بعض التشريعات المقارنة خاصة التشريع الفرنسي، وبالتالي يمكن القول كذلك أن المشرع الجزائري قد أورد هذه الصور الت ي يتحقق بها الإتلاف على سبيل المثال لا الحصر.

[1] اسمهان بوضياف، المرجع السابق، ص 359.

وبمعنى أخر يمكن أن يتحقق الإتلاف بصور أخرى غير تلك التي أوردها المشرع الجزائري في قانون العقوبات.

إن المقصود بالإتلاف في هذا الإطار ذلك الذي يوجه إلى الجانب المنطقي والمعنوي في الحاسب الآلي، والذي بات يشكل قيمة اقتصادية عالية، فإتلاف برامج ومعلومات الحاسب الآلي فيه إفقاد المنفعة هذه البرامج والمعلومات.[1]

الفرع الثاني: الجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي

تتحقق جريمة التعدي على المكونات غير المادية للنظام المعلوماتي عندما تكون مكونات الكمبيوتر المعلوماتية الغير مادية مثل البرامج المستخدمة والبيانات المخزنة في ذاكرة الكمبيوتر محلا أو موضعا للجريمة، والمقصود بالبرنامج logiciel أو الكيان المنطقي أنه مجموعة من الأوامر التي تسمح بتشغيل جهاز الحاسب الآلي أو نظم المعلومات المخصصة لمعالجة المعلومات بهدف إنجاز عملية معينة أو إعطاء نتائج محددة.

وجرائم الاعتداء على برامج الكمبيوتر تأخذ شكلين الأول يكون في شكل الاعتداء على البرامج التطبيقية والثاني في شكل الاعتداء على برامج التشغيل، وفيما يتعلق بالبرامج التطبيقية يشكل هذا النوع من الجرائم نسبة تقدر بحوالي 15% من مجموعة حالات الجرائم

[1] أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، العدد الأول، المجلد العاشر، جامعة الجلفة، 2017 ص ص 486-487

الالكترونية، أما بالنسبة لبرامج التشغيل تتحقق الجريمة في هذه الحالة بتزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تتيح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[1].

خلاصة الفصل الأول

تطرقنا لماهية الجريمة الإلكترونية من خلال مفهومها وتعريفها، بالإضافة إلى التطرق لخصائص الجريمة الالكترونية، حيث تتميز بصعوبة اكتشافها وسرعة تطورها وانتشارها لتعبر حدود الدولة الواحدة، وتتكون الجريمة الإلكترونية مثلها مثل الجريمة التقليدية من ثلاث أركان، ركن شرعي وهو اعتراف المشرع والنص على النص المجرم وتحيد الجزاءات المناسبة له، وركن مادي يتمثل في السلوك الذي يقوم به الجاني والنتيجة الإجرامية الناتجة عن هذا الفعل والرابطة السببية بينهما، وركن معنوي وهو الحالة النفسية التي يكون عليها الجاني والمتمثلة في عنصري العلم والإرادة وتنقسم الجريمة الإلكترونية إلى عدة أنواع منها ما أقرها الفقه ومنها ما نصت عليها التشريعات.

[1] هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص 15.

وكأي جريمة وجب قانونا اثباتها وسنتناول في الفصل الآتي بعض طرق الاثبات وحجية الدليل الالكتروني في اثبات الجريمة الالكترونية وهذا ما سنتطرق اليه.

الفصل الثاني: اثبات الجريمة الالكترونية

حجية الدليل الالكتروني في الاثبات

الفصل الثاني: اثبات الجريمة الالكترونية حجية الدليل الالكتروني في الاثبات.

الجريمة الإلكترونية نوع جديد ومستحدث من الجرائم له خصوصيته والمتمثلة في الدليل الناتج عنه، وهو الدليل الرقمي، وللحصول على هذا الدليل لا بد من أن يقوم رجال الضبطية القضائية بعدة إجراءات خاصة تحكمها ضوابط وقواعد عامة.

ولكي يتم الوصول إلى الحقيقة في مرحلة الحكم لابد أن يتم الأمر عن طريق أدلة متوفرة لدى القاضي يمارس سلطته التقديرية عليها، وفي مجال الجريمة الإلكترونية يكون الدليل الإلكتروني هو الأوفر، وهو دليل خاضع للقواعد العامة فيما يخص حجيته.

ونظرا للطبيعة الخاصة التي يتمتع بها الدليل الإلكتروني، فإن حجيته على مستوى الإثبات الجنائي قد تثير عدة مشاكل خاصة فيما يتعلق بمصداقيته، وعليه سيتم تقسم الفصل الى مبحثين، **(المبحث الاول)** ضبط الجريمة الالكترونية و طرق اثباتها، أما **(المبحث الثاني)** حجية الدليل الرقمي في اثبات الجريمة الالكترونية

المبحث الاول: ضبط الجريمة الالكترونية و طرق اثباتها.

يعتبر الإثبات خطوة أساسية لحماية الحقوق، حيث يحمل أهمية كبيرة في جميع الأنظمة القانونية وخاصة ما يتعلق بالإثبات الخطي الذي يعتمد على وجود وثيقة مادية محررة بشكل ورقي ومختومة وموقعة، ومع ظهور وسائل الاتصال الإلكترونية التي تتيح لنا إبرام التزامات وعقود إلكترونيا، أصبح لدينا مفهوم جديد للإثبات[1].

وسنتطرق في هذا المبحث الى ضبط الجريمة الالكترونية وهذا في **(المطلب الاول)**، وطرق اثبات الجريمة الالكترونية وهذا في **(المطلب الثاني)**.

[1] محمد ناصر حمودي، العقد الدولي الإلكتروني المبرم عبر الانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى ، 2012 ص 382.

المطلب الاول: ضبط الجريمة الالكترونية

من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس مقتصرا على أسباب التقدم التقني فقط، بل يحدث دوما وبصفة مستمرة، فالمجرم والجريمة في تقدم وتجدد مستمرين.

ولا شك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق، ونحن لا نزال في بداية عصر الانفجار المعلوماتي، يعني توقع ظهور المزيد من هذه الأنماط الجديدة، والتي يتوجب معها تحديث الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو مايتبع بتطوير أسلوب التحقيق فيها وكيفية إثباته[1].

الفرع الأول: القواعد العامة التي تحكم إثبات الجريمة الإلكترونية

تتنوع قواعد إثبات الجريمة الإلكترونية، حيث يمكن أن تصنف على النحو التالي:

أولا: من زاوية قوتها الثبوتية: هناك أدلة مباشرة تثبت الجريمة بصورة مباشرة، وأدلة غير مباشرة تنصب على وقائع لا تشير إلى الجريمة مباشرة، وإنما يحتاج الأمر إلى إعمال العقل والمنطق لاستخلاص الأدلة منها.

ثانيا: من زاوية النتيجة القضائية المستخلصة منها: هناك دليل يدل على وقوع الجريمة، ودليل على تحديد شخص مرتكبها، ودليل يثبت ارتكابها على المتهم. ثالثا: من زاوية وظيفة الدليل الإثباتية فهنالك أدلة تنصب على إثبات توافر أحد ركني الجريمة المادي أو المعنوي، وهناك أدلة تنصب على تحديد شخصية المتهم[2]، فأما التحديد القاطع فيشير إلى تحديد شخصية الجاني دون أدنى شك، كالبصمات، وآثار الأقدام العارية، والشهادة بالرؤية، والاعتراف، وضبط محصلات الجريمة في حوزة المتهم، آثار المقاومة على جسده أو بأظافر

[1] محمد على العربان الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،(دط)، الإسكندرية 2011، ص 31.

[2] تنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية ، جامعة نايف للعلوم الأمنية، الرياض، 2012، ص 72 ص 73.

المجني عليه، أو التحديد غير القاطع يشير إلى مجرد احتمال لتحديد شخصية الجاني وهي مجرد قرائن[1].

رابعا: من زاوية مضمون الدليل

هناك أدلة مادية محسوسة بإحدى الحواس، وهناك أدلة معنوية مثل الشهادة، وأدلة قولية مثل أقوال المتهم.

ولذلك فقواعد الإثبات النظامية يقصد بها الأدلة التي حددها المنظم وعين حالات استخدامها ومدى حجيتها، وبالرغم من أن هناك من يعد تلك الأدلة الإلكترونية مرحلة متقدمة من الأدلة المادية، أو أدلة فنية لأنها تنبعث من رأي خبير فني، إلا أنها تعد نوعا متميزا من وسائل الإثبات، وذلك بسبب كونها نبضات غير محسوسة، وأن حجمها وشكلها تخيلي وأنها سريعة الانتقال، ويمكن استخراج نسخ من الأصل والحصول على نفس الدليل الموجود بمسرح الجريمة التقليدي بالمسرح الإلكتروني أو بمسرح الكتروني آخر وقد يكون بمقدور المحققين استرجاع الدليل بعد حذفه[2].

الفرع الثاني: عناصر اثبات الجريمة الالكترونية

هناك العديد من العناصر المختلفة لإثبات الجريمة الإلكترونية، والتي يمكن توضيحها فيما يلي:

أولا: العنصر الأول: إظهار الركن المادي للجرائم الإلكترونية

إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالأنترنت، ويتطلب أيضا هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له، فيقوم بتحميل برامج اختراق، أو أن يقوم بإعداد هذه البرامج

[1] تنيان ناصر آل ثنيان، المرجع السابق، ص73.

[2] أحمد الأمين البشري، التحقيق في جرائم الحاسب والانترنت، المجلة العربية للدراسات العربية والتدريب، المجلد 15، العدد 30، جامعة نايف للعلوم الأمنية، الرياض، 2001، ص 115.

بنفسه، وكذلك قد يحتاج إلى تهيئه صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على جهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق وبرامج فيروسات، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور مخلة بالآداب للأطفال، فمثل هذه الأشياء تمثل جريمة في حد ذاتها[1].

ثانيا: العنصر الثاني إظهار الركن المعنوي للجرائم الإلكترونية

الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويتحد الركن المعنوي للجريمة الإلكترونية من خلال مبدأ الإرادة ومبدأ العلم، فالمجرم المعلوماتي تارة يستخدم الإرادة للتخطيط للجريمة، وتارة يستخدم العلم من أجل تنفيذ الجريمة الإلكترونية[2].

ثالثا: العنصر الثالث تحديد وقت ومكان ارتكاب الجريمة الإلكترونية

تثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في الإمارات، وهذا الخادم موجود في الصين، فكيف يمكن معرفة وقت حدوث الجريمة، هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين وهذا بالتالي يثير مشكلة أخرى وهي مكان ارتكاب الجريمة

[1] عبد الحميد عبد المطلب ممدوح، جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية الجريمة عبر الانترنت، (دط)، مكتبة دار الحقوق، الشارقة، 2001، ص226.

[2] محمد على العربان، الجرائم المعلوماتية المرجع السابق، ص 157.

الإلكترونية، ويثار أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن، حيث أن هناك بعد دولي في هذا المجال ذلك أن الجريمة الإلكترونية جريمة عابرة للحدود[1].

المطلب الثاني: طرق إثبات الجريمة الالكترونية.

إن التطور التقني في شبكة الانترنت سوف يقود دون شك إلى تغيير كبير، إن لم يكن كليا في المفاهيم السائدة حول الدليل. ويقود مثل هذا القول في الحقيقة إلى إعلان انضمام الخبرة التقنية إلى علم الخبرة المتميزة للتعامل مع موضوع الدعوى من حيث ضرورة الاستعانة بالمختصين في مجال النزاع[2].

ويعد كل من المعاينة والتفتيش والشهادة والإقرار، أحد وسائل جمع الأدلة ولكل منها قواعده يتم إتباعها

الفرع الأول: الاستدلالات الأولية لإثبات الجريمة الإلكترونية

يمكن توضيح طرق الاستدلالات الأولية لإثبات الجريمة الإلكترونية من خلال ما يلي:

أولا: تلقي وضبط البلاغ:

يعرف ضبط البلاغ على أنه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، والضبط بهذا المعنى ينصرف إلى الأشياء دون الأشخاص. وبناء على ذلك، يجب توضيح مدى صلاحية الجرائم المرتكبة في البيئة الإلكترونية لضبط البلاغ ويعد البلاغ هو المشكلة الحقيقية التي تواجه الجريمة الإلكترونية، فغالبية المنظمات تخشى من الإبلاغ لكي لا تفقد ثقة عملائها، ومن ثم يفلت مرتكب الجريمة الإلكترونية بفعله نتيجة إحجام المنظمات والشركات والمؤسسات المالية عن الإبلاغ خوفا على سمعتها، حيث تفضل هذه المرافق عدم إبلاغ السلطات المختصة للمحافظة على

[1] أحمد محمد شتاء، فكرة الحماية الجنائية لبرامج الحاسب الآلي، (دط)، دار الجامعة الجديدة القاهرة، 2000، ص192.

[2] هشام فريد رستم الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، ص141

ثقة عملائها أكثر من اهتمامها بكشف الجريمة، ويفضلون الترضية المالية لعملائهم ومنحهم الأموال التي سلبت منهم نتيجة الاختراق والتعدي[1].

ثانيا: المعاينة

المعاينة هي "مشاهدة مسرح الجريمة و إثبات الحالة فيها أي مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة للمساعدة على اكتشاف الحقيقة[2]".

وعرفها البعض أيضا، بأنها" الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء و أشخاص والفحص الدقيق لكافة المحتويات بهدف كشف مخلفات و آثار الجاني بالمكان و التي تشير إلى شخصيته أو شركائه وما قد يفيد في إثبات ارتكاب الجريمة و توضيح قدرا من الاستنتاجات المنطقية تشكل في حد ذاتها الأساس الذي تقام عليه عملية التحقيق والبحث[3]".

وكذلك المعاينة هي عبارة عن انتقال ضابط الشرطة القضائية إلى مكان وقوع الجريمة إذا تطلب الأمر ذلك ، من أجل إثبات حالة الأماكن ومعاينة مخلفات الجريمة و ضبط الأشياء المتحصلة أو المتخلفة عنها أو التي استعملت في تنفيذ الجريمة، وهو ما نصت عليه المادة 42 من قانون الإجراءات الجزائية[4].

وإذا تمت المعاينة بعد وقوع الجريمة في المجال الإلكتروني، فيجب مراعاة ما يلي

---

[1] أحمد حماد الهيتي، جرائم الحاسوب ماهيتها، أهم صورها والصعوبات التي تواجهها، (دط)، دار المناهج للنشر والتوزيع، عمان، 2005، ص218.

[2] عماد حامد أحمد القدو وإسراء جاسم محمد العمران، التحقيق الابتدائي، مركز الكتاب الأكاديمي، عمان الأردن ، ط1، 2015، ص34.

[3] محمد فاروق عبد الحميد كامل ، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ط1، (د س ن)، ص246.

[4] علي شملال، المستحدث في قانون الإجراءات الجزائية الجزائري ، الكتاب الأول(الاستدلال والإتهام) ، دار هومة للطباعة والنشر والتوزيع الجزائر، ط 2، 2017، ص 39.

– تصوير الحاسب والأجهزة الطرفية المتصلة به على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

– العناية بملاحظة الطريقة التي تم بها إعداد النظام.

– ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

– عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي الموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

– التحفظ على المعلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة.

– التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

– قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات الآلية[1]".

ثالثا: التفتيش

كما عرفه البعض الآخر بأنه:" إجراء من إجراءات التحقيق فهو ليس عملا إداريا من أعمال الضبط الإداري وإنما هو عمل من أعمال التحقيق والضبط القضائي لجمع الأدلة عن جريمة معينة بعد قيام الاتهام ضد شخص معين[1]".

[1] معبد الحميد عبد المطلب ، أدلة الصور الرقمية، ورقة عمل مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخاصية الجرائم الإلكترونية الملامح والابعاد المنعقدة بلكلية الملك فهد الأمنية بالرياض مرة من 22 إلى 24 فريل 2007، الرياض، 2007، ص6

وهناك من يعرفه التفتيش هو "البحث عن مكنون سر الأفراد على دليل للجريمة المرتكبة أو البحث عن الدليل وهو إجراء من إجراءات التحقيق الابتدائي الذي يخوله القانون لقاضي التحقيق أصلا واستثناء لضباط الشرطة القضائية[2]. "

أما تفتيش الأنظمة المعلوماتية، فقد عرفه بعض الفقهاء بأنه "البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو هو البحث الدقيق والاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكناً أو جهاز حاسوب أو أنظمة أو الانترنت".

وتفتيش النظم المعلوماتية، "هو إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، ويستهدف ضبط أدلة الجريمة مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب والمعطيات المعلوماتية والاتصالات الإلكترونية"[3].

وإجمالا فإن التفتيش، سواء أكان في شكله التقليدي أو الحديث، هو إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق، وكل ما يفيد في كشف الحقيقة، وعن أشياء تفيد في معرفتها ونسبتها إلى المتهم[4].

رابعا: التسرب

عرفه البعض بأنه تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية

[1] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد5، كلية الحقوق السياسية، جامعة الوادي، الجزائر، 2012، ص160.

[2] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، المرجع السابق، ص 160.

[3] علي حسن محمد الطوالبة التفتيش الجنائي على نظم الحاسوب والانترنت – دراسة مقارنة، عالم الكتاب الحديث اربد الطبعة الأولى 2004، ص13.

[4] رضا هميسي، المرجع السابق، ص161.

آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية، ولتقديم المتسرب نفسه على انه فاعل أو شريك[1]".

ويوجد من عرفه بأنه عملية إجرائية تتميز بالاستمرار النسبي وتتم بشروط معينة ومحددة قانونا يقوم بها شخص مخول أو مجموعة أشخاص يستعينون بوسائل مختلفة غايتها الوصول إلى حقائق معينة تتعلق بالمشتبه بهم في ارتكاب جرائم معينة واردة على سبيل الحصر[2].

الفرع الثاني: اثبات الجريمة الالكترونية بالشهادة والخبرة الفنية

سنقوم في هذا الفرع بدراسة اثبات الجريمة الالكترونية بكل من الشهادة والخبرة الفنية على حدى.

أولا: اثبات الجريمة الالكترونية بالشهادة

تعد الشهادة الإلكترونية من أهم الإجراءات والتدابير القضائية المستحدثة التي لا تختلف عن الشهادة التي تتم بالطرق التقليدية إلا من حيث الوسيلة المستخدمة لأدائها، ولقد تبني المشرع الجزائري فكرة الشهادة الإلكترونية في القسم الجزائي بموجب الأمر رقم 02-15 المتضمن قانون الإجراءات الجزائية بوصفها آلية إجرائية تستهدف إرساء نظام خاص بالشهود[3].

لم يتضمن التشريع الجزائري تعريفا خاص بالشهادة الإلكترونية غير تلك القواعد المقررة لحماية الشهود باعتبارها تعد من بين المفاهيم الحديثة التي ظهرت نتيجة الثورة التكنولوجية خاصة في مجال الإجراءات القضائية، وكذا الاعتماد على تكنولوجيا الحاسوب والأنترنت في إدارة الخصومة القضائية.

[1] عبد الرحمان خليفي، محاضرات في القانون الجنائي العام دون طبعة، دار الهدى، الجزائر،2010، ص 89.

[2] عبد الرحمان خليفي، محاضرات في القانون الجنائي العام، المرجع السابق، ص 89

[3] نور الهدى قادري، الشهادة الالكترونية وحجيتها في الاثبات، مجلة الفكر القانوني والسياسي، المجلد السابع، العدد الاول، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الاغواط، 2023، ص1595.

تعد الشهادة الإلكترونية مصطلح حديث ومركب من مصطلحين هما " الشهادة " و الإلكترونية" التي تعني الوسيلة التقنية المستخدمة في نقل شهادة الشاهد، وعليه إعمالا بالاجتهادات الفقهية واتجاهات القضائية في تعريفهم لشهادة بوجهها التقليدي، يمكن تعريف الشهادة الإلكترونية على أنها إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شاهده بحواسه عن هذه الواقعة بطريقة مباشرة بالإدلاء بأقواله بواسطة منظومة إلكترونية أو وسيط معلوماتي[1].

أو هي عبارة عن دليل من أدلة الإثبات يتم التوصل إليها نتيجة تسخير منظومة معلوماتية أو أجهزة إلكترونية أو وسائط معلوماتية توضع تحت تصرف الشخص لينقل وقائع يكون قد رآها أو سمعها أو عاينها بإحدى حواسه أو أدركها بها عن على وجه العموم في واقعة ذي أهمية قانونية يوجب القانون إقامة الدليل لإثباتها[2].

وبالتالي تعد الشهادة الإلكترونية هي ذاتها الشهادة التي تقام بالطرق التقليدية بذات الشروط والأركان ولا تختلف إلا من حيث الوسيلة المستخدمة لأدائها التي تتم عبر الوسائط الإلكترونية، بحيث تتحول الشهادة من أن تكون وجها لوجه داخل المحكمة، إلى أن تصبح عبر وسيلة الاتصال الحديثة من خلال المحكمة أي عن بعد[3].

ثانيا: اثبات الجريمة الالكترونية بالخبرة الفنية

تعد عملية الحصول على الأدلة الرقمية أمرا صعب الوصول إليه لما تتطلبه من خبرة ومهارة كبيرة في مجال الحاسب الآلي، ويرجع ذلك لتعدد صور وأشكال الجرائم الإلكترونية ما بين مهاجمة المعلومات بغرض تدميرها أو الاستيلاء عليها، أو قد يكون المقصود بالهجوم هو الأجهزة، كنشر فيروس يعمل على إتلاف وحداته الرئيسية مثلا، أو قد يكون

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي، الإسكندرية ، 2010 ، ص 260

[2] عادل بوزيدة ، دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية ، مجلة النبراس للدراسات القانونية ، المجلد الأول، العدد الأول، جامعة العربي التبسي، تبسة ، 2016، ص 137

[3] نور الهدى قادري، المرجع السابق، ص1996.

الأمر مجرد اختراق لكلمة مرور خاصة ببنك أو مؤسسة كبرى بغرض الاحتيال والحصول على الأموال،

وقد تكون لمجرد إثبات الذات وإظهار المقدرة العالية في مجال الحاسب الآلي[1].

ولما كانت عملية تجميع الأدلة الرقمية الجنائية في الجرائم الإلكترونية أو الرقمية تعد من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، فقد كان لزاما أن يتم اللجوء إلى خبير قضائي معلوماتي متخصص، لاشتقاق الدليل العلمي الفني الجنائي. ويرى البعض المتخصصين أن عملية تجميع الأدلة الرقمية في الجرائم الإلكترونية التي تتم عبر الشبكة العالمية (الانترنت) تتم عبر ثلاث مراحل:

المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة، حيث تتبع الحاسبات الخوادم التي دخل المجرم منها ومحاولة إيجاد أي أثر له.

المرحلة الثانية: وهي مرحلة المراقبة، فهناك فرضية تقول بأن المجرم لا بد وأن يعود أو يحوم حول مسرح جريمته، وتتعدد طرق مراقبة هذه الحواسيب، ويمكن توضيح هذه الطرق كما يلي[2]:

1- استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

2- استخدام أجزاء توضع في الحاسب الآلي لمراقبته.

3- استخدام كاميرات مراقبة لشاشة الحاسب الآلي معدة للاستخدام التجاري، وأبسط الطرق المراقبة الحاسب هي الدخول لمكان وجوده.

[1] عبد الناصر محمد محمود فرغلي محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف للعلوم الأمنية، الرياض، 2007، ص 13

[2] المرجع نفسه.

المرحلة الثالثة: ضبط الأجهزة المشتبه فيها وفحصها فحصا فنيا وشرعيا، حيث يبدأ في هذه المرحلة عمل الخبير المعلوماتي في فحص النظام الحاسوبي المشتبه فيه بمكوناته المادية ومكوناته البرمجية، سعيا لاشتقاق الدليل الرقمي لتقديمه لجهة التحقيق أو الحكم، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه، ولتقرير إدانة المتهم أو تأكيد براءته، ويتم ذلك وفق القواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة المعلوماتية، مع مراعاة القواعد القانونية لمبدأ المشروعية[1].

[1] عبد الناصر محمد محمود فرغلي محمد عبيد سيف سعيد المسماري، المرجع السابق، ص14.

المبحث الثاني: حجية الدليل الرقمي في اثبات الجريمة الالكترونية

لقد أدت الثورة المعلوماتية في مجال العولمة والاتصال إلى استحداث وسيلة تقنية جديدة سهلت عملية الإثبات الجنائي وهي ما يعرف بالدليل الرقمي، حيث أصبح لهذا الأخير دور جد فعال في التصدي للجريمة الإلكترونية وإثباتها ومعرفة مرتكبيها، وبالرغم من الإيجابيات التي يتمتع بها الدليل الرقمي إلا أنه أصبح في مواجهة الحق في الخصوصية المعلوماتية والذي يشكل جزءا مهما من الحياة الخاصة للأفراد، وسنتطرق في هذا المبحث الى مفهوم الدليل الالكتروني وهذا في **(المطلب الاول)**، والى القيمة الثبوتية للأدلة الرقمية وهذا في **(المطلب الثاني)**.

المطلب الأول: مفهوم الدليل الالكتروني

سنتناول في هذا المطلب تعريف الدليل الالكتروني**(الفرع الأول)**، ثم أنواعه **(الفرع الثاني)**

الفرع الاول: تعريف الدليل الالكتروني

أولا: الدليل لغة

يقصد بالدليل لغة المرشد وما يتم به الإرشاد، وما يستدل به، وهو أيضاً الدال، والجمع أدلة ودلائل[1]، والدليل ما يستدل به، ودله على الطريق أي أرشده، يدله بالضم، ودلالة يفتح الدال وكسرها ودلولة بالضم والفتح أعلى، ويقال أدل والاسم الدال بتشديد اللام فلان يدل فلاناً أي يثق به.

[1] جميل صليبا، المعجم الفلسفي، الجزء الأول، دار الكتاب العالمي، مكتبة المدرسة، بيروت، 1994 ، ص 564.

وقد جاء في القرآن الكريم معنى الدليل بقوله تعالى: " اَلَمْ تَرَ إِلَى رَبِّكَ كَيْفَ مَدَّ الظِّلَّ وَلَوْ شَاءَ لَجَعَلَهُ سَاكِنًا ثُمَّ جَعَلْنَا الشَّمْسَ عَلَيْهِ دَلِيلًا[1]."

قال أبو عبيدة: الدال قريب المعنى من الهدى وهما في السكينة والوقار في الهيئة والمنظر وغير ذلك[2].

ثانيا: الدليل اصطلاحا

أما الدليل اصطلاحاً فهو الذي يلزم من العلم به علم بشيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل إلى معرفة الحقيقة، وأيضاً يقصد بالدليل ما يمكن التوصل به إلى معرفة الحقيقة[3].

ثالثا: الدليل في القانون

أما الدليل في القانوني فيقصد به الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، ويقصد بالحقيقة في هذا السياق بأنها كل ما يتعلق بالإجراءات والوقائع المعروضة على القاضي لإعمال حكم القانون عليها[4]، ويقصد بالدليل أيضا الوسيلة الإثباتية المشروعة التي تسهم في تحقيق حالة اليقين لدى القاضي بطريقة سائغة يطمئن إليها . كما يشار إلى الدليل بأنه كل إظهار النشاط عام أو خاص داخل الخصومة أو من أجلها يؤدي مباشرة إلى التأثير في تطور رابطة الخصومة أو بمعنى آخر هو كل عمل يجري في الخصومة أو يهدف إلى إعدادها أو له قيمة في الخصومة – أيا كانت طبيعته أو معناه – نظمه القانون بقصد الوصول إلى تطبيق القانون الموضوعي فيها.

[1] الآية 45 من سورة الفرقان.

[2] محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح المطبعة الأميرية القاهرة 2016 م / 1338هـ ص 209.

[3] المرجع نفسه.

[4] أحمد ضياء الدين مشروعية الدليل في المواد الجنائية رسالة دكتوراه منشورة ، كلية الحقوق جامعة عين شمس القاهرة 1982 ، ص 473.

وعليه يمكن القول من ذلك بأن الدليل الجنائي بشكل عام هو الوسيلة التي تؤدي بالقاضي إلى الحقيقة التي يطلبها عن طريق إجراءات قانونية لإثبات واقعة معينة، وبعد تعريف الدليل في اللغة والاصطلاح والمجال القانوني له بشكل عام، نتطرق بعد ذلك إلى تعريف الدليل الإلكتروني باعتباره كما أسلفنا هو ما يستند عليه لإثبات الجريمة الإلكترونية.

رابعاً: تعريف الدليل الإلكتروني

تعددت تعريفات الدليل الإلكتروني واختلف الفقه فيها، فاتجه البعض منه نحو التوسع في تعريف الدليل الإلكتروني، والبعض الآخر نحو تضييقه وحصره في نواح معينة وذلك بحسب الزاوية والمجال الذي ينظرون إليه، وعليه سنتناول أهم التعريفات التي وردت حول الدليل الإلكتروني، فقد عرف البعض الدليل الإلكتروني بأنه: الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة ، وكذلك عرف بأنه : معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية من خلال ترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه، كما تم تعريف الدليل لإلكتروني بأنه[1] بيانات يمكن إعدادها وتراسلها وتخزينها رقمياً بحيث تمكن الحاسب الآلي من تأدية مهمة ماء، وقد أخذ بهذا التعريف الأخير التقرير الأمريكي المقدم إلى ندوة الانتربول العلمية حول الدليل الرقمي عام 2001، وأيضاً عرف بأنه: الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهي مكون رقمي التقديم معلومات في أشكال متنوعة مثل النصوص

[1] محمد الامين البشري، لتحقيق في الجرائم المستحدثة الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، 2004، ص234.

المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون[1].

الفرع الثاني: خصائص الدليل الالكتروني

إن البيئة الافتراضية التي يتواجد بها الدليل الإلكتروني وهي البيئة الرقمية، تحتوي على بيانات رقمية متعددة الأنواع، وهي ما تكون دليلا سواء بصورة منفردة أو مجتمعة لذا فهي بيئة متطورة بطبيعتها، وينعكس ذلك على الدليل الإلكتروني ذاته الذي يتأثر بالبيئة التي يعيش فيها، فقد أضفت هذه البيئة عليه طبيعة خاصة وخصائص تميزه كدليل جنائي عن الأدلة الجنائية التقليدية الأخرى[2]، ويمكن الإشارة إلى تلك الخصائص التي تميزه وفق الآتي:

أولاً: الدليل الإلكتروني دليل علمي

إن الطبيعة الخاصة للدليل الإلكتروني والوسط الذي يتواجد به وهي بيئة افتراضية غير ملموسة، تجعل من الدليل دليلا غير مادي كذلك، فهو دليل غير ملموس يتكون من بيانات ومعلومات على هيئة الكترونية، حيث إن العالم الافتراضي التقني هو عالم أعده متخصصون في التقنية، وبالتالي لا يمكن الحصول على البيانات والمعلومات في ذلك العالم التقني إلا بأساليب علمية وتقنية كذلك، وهو ما يميز الدليل الإلكتروني بهذه الخاصية بأنه دليل علمي، فاستخراج الدليل الإلكتروني يحتاج إلى بيئة مشابهة للبيئة التي نتج عنها، لذا

[1] المرجع نفسه ، ص234.

[2] مسعود بن حميد المعمري، الدليل الالكتروني لإثبات الجريمة الالكترونية، مجلة كلية القانون الكويتية العالمية، كلية الحقوق، العدد3، الجزء الثاني، جامعة السلطان قابوس، مسقط، سلطة عمان، 2018، 197.

يتطلب الاستعانة بأجهزة وأدوات التقنية واستخدام برامج حاسوبية ملائمة، للاطلاع عليه أو استخراجه في هيئة ملموسة أو مادية، وهي تعد أساليب علمية[1].

ثانيا: الدليل الإلكتروني دليل تقني

يقصد بالتقنية العلم التطبيقي لوسائل وأدوات تم اختراعها من أجل تسهيل حياة الفرد والمجتمع، وهي تقوم على أساس علمي، مثلها مثل الدليل الإلكتروني الذي هو كذلك دليل علمي، لذا يمكن استنتاج أن الدليل الإلكتروني يتميز بأنه دليل تقني، استناداً للمصدر الذي جاء منه وهو البيئة الرقمية أو التقنية، مثلما هو دليل علمي استناداً للبيئة التي يتواجد بها والتي تم انشاؤها من قبل مختصين فنيين على أساس علمي إن الدليل الإلكتروني التقني ليس كالأدلة الجنائية التقليدية الأخرى، فالتقنية لا تنتج أدلة مادية ملموسة كالسلاح أو البصمات أو الاعتراف المكتوب تدل على مرتكب الجريمة، إنما ما تنتجه التقنية نبضات رقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل بين أجزاء وسائل التقنية وشبكات الاتصال متعدية حدود المكان والزمان الواحد[2].

وتفيد هذه الخاصية للدليل الإلكتروني أنه لابد المأموري الضبط القضائي وسلطات التحقيق أن يبنوا عملهم على أساس الخبرة في التقنية، فلدى بعض الدول المتقدمة يكون السلطات التحقيق المقومات التقنية الكاملة التي تحتاجها، ويكون هناك فصل بين الخبرة وسلطة التحقيق في الجرائم التي يكون الاعتماد فيها على الدليل الإلكتروني، حيث تضم سلطة التحقيق عناصر ذات كفاءة عالية تمتلك الخبرة في التقنية كما هو الحال في الولايات المتحدة الأمريكية، أما سلطات التحقيق التي لا تمتلك ذلك فإنها تعتمد على الخبرة في تحقيق مثل هذه الجرائم الإلكترونية التي تستند على الدليل الإلكتروني لإثباتها، وبالتالي لا

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، 2010، ص ص 61-62.

[2] عائشة بن قارة مصطفى، المرجع سابق، ص 62.

يتحقق الفصل بين سلطة التحقيق والخبرة، حيث إن الخبرة تقوم بدور في التحقيق المساعدة سلطة التحقيق لإثبات الجريمة والدليل التقني[1].

ثالثا: الدليل الإلكتروني دليل متنوع ومتطور

إن مصطلح الدليل الإلكتروني يشمل كافة أنواع وأشكال البيانات الرقمية والتي من الممكن تداولها تقنياً بين وسائل تقنية المعلومات، بحيث تكون بين تلك البيانات وبين الجريمة المرتكبة رابطة معينة وتتصل من الجانب الآخر بالمجني عليه، كما يكون للجاني صلة بها، ومن ذلك تتضح خاصية أن الدليل الإلكتروني هو دليل متنوع، ولو كان الدليل متحد التكوين بلغة التقنية. وتعني هذه الخاصية من حيث التنوع أن الدليل الإلكتروني يمكن أن يظهر على هيئات مختلفة، فقد يكون غير مقروء للأشخاص مثلما هو الحال في المراقبة عبر الشبكات أو الخوادم التقنية للشبكات، وقد يكون مقروءاً ومفهوماً للأشخاص مثلما يكون عليه الدليل في صورة وثيقة أو صورة مخزنة بجهاز حاسب آلي أو في البريد الإلكتروني، أما خاصية الدليل الإلكتروني كدليل متطور فهي تفيد أنها تستخدم في جرائم مستحدثة، فجريمة النصب مثلاً يمكن ارتكابها بالطرق التقليدية التي تنتج أدلة مادية، وكذلك أصبح مع التقدم التكنولوجي من الممكن ارتكابها باستخدام التقنية سواء اكانت باستخدام جهاز حاسب آلي، أم أن يكون الحاسب الآلي محلاً لارتكاب جريمة النصب[2].

وهذا التطور في مجال الدليل الإلكتروني وتطور الجرائم معه، ومع التقدم المستمر في مجال التكنولوجيا، فإن ذلك قد يشكل عائقا في الوصول للأدلة الإلكترونية والتي تفيد في اكتشاف الجريمة ومرتكبيها، لذا فإنه يكون من الواجب مواكبة التطور التقني، سواء من حيث الأجهزة المستحدثة أو البرامج التشغيلية والمستخدمة داخل هذه الأجهزة وبرامج الحصول على الأدلة الإلكترونية، إلى جانب الاطلاع على تلك التطورات والتحديثات المستمرة للأجهزة

[1] مسعود بن حميد المعمري، المرجع السابق، ص 198.

[2] عائشة بن قارة مصطفى، المرجع سابق، 62.

والبرامج، وهو ما يساعد على الكشف عن الأدلة الإلكترونية وإثبات الجريمة بطريقة أسهل وأسرع[1].

رابعاً: الدليل الإلكتروني يصعب التخلص منه

تعتبر هذه الخاصية من أهم الخصائص التي يتميز بها الدليل الإلكتروني عن الأدلة التقليدية الأخرى، حيث إنه يمكن التخلص بسهولة من الأدلة الأخرى كالأوراق والسلاح والأموال المزورة بإتلافها وحرقها لتختفي معالمها، وأيضاً بالنسبة لبصمات الإصبع، حيث يمكن مسحها بسهولة وإخفاؤها من موضعها، أما الدليل الإلكتروني بشكل خاص وكل ما يتعلق بتكنولوجيا المعلومات بشكل عام، فإنه كلما حدث ارتباط أو اتصال مع شبكة الاتصال أو وسيلة تقنية المعلومات وبمعنى إدخال البيانات معينة[2].

فإنه يصبح من الصعب التخلص من ذلك ولو استخدمت أدوات الحذف والإلغاء، وكما أن التخلص من الدليل الإلكتروني باستخدام الأدوات المتوفرة في وسيلة التقنية مثل خيارات الحذف أو الإلغاء أو الإزالة، لا تعتبر من العوائق التي تمنع من استرجاع الدليل فهناك برامج متخصصة من ذات طبيعة الدليل التقني تمكن الجهات القضائية المختصة من الحصول على الدليل المحذوف واسترجاع البيانات الملغاة من الجهاز محل ارتكاب الجريمة.

ويترتب على أن الدليل الإلكتروني يصعب التخلص منه مسائل قانونية مهمة، ومنها مسألة التخلص من الدليل محل ارتكاب الجريمة التي تعتبر جريمة مستقلة كذلك، فإعداد أو استخدام برامج من قبل مرتكبي الجريمة الإلكترونية تكون مهمتها حذف البيانات وإزالتها من الجهاز أو شبكات الاتصال، تشكل بذاتها جريمة، وبالتالي فإنه يمكن إدانة الجناة على ذلك

[1] مسعود بن حميد المعمري، المرجع السابق، ص 199.

[2] مسعود بن حميد المعمري، المرجع السابق، ص 200.

حسب تجريم قوانين الجزاء لها، فإذا أثبت الخبير التقني حدوث الجريمة واستخدام تلك البرامج، التي قد تكون غير قانونية في الأصل، فتشملهم عقوبة ذلك الجرم[1].

وعليه فإن المشرع مطالب بوجود نصوص قانونية تجرم تلك الأفعال التي تتضمن التخلص من الأدلة الجنائية التي يمكن الاستناد عليها لإثبات جريمة معينة، فالتشديد في هذا المجال يمنع إفلات المجرم من العقاب إذا ما قام بحذف وإلغاء الأدلة التي تدينه على ارتكاب جريمة ما، وكما أنه لابد من مواكبة التطور نحو استخدام برامج تساعد على استخراج الأدلة حتى لو قام الجاني بحذفها ببرامج متخصصة أخرى.

وأيضاً هناك مسألة قانونية تقابل مسألة التخلص من الدليل الإلكتروني، وهي مسألة اعتبار أن الدليل الإلكتروني أو التقني ذو طبيعة مرنة، ونتيجة ضعفه فإنه يسهل إتلافه وفقده. وبالتالي يمكن التخلص منه بغير طريقة الحذف والإلغاء، وذلك مثل عملية إتلاف الدليل المادي، على أن هذا القول قد واجه انتقاداً باعتبار أن الإتلاف نتيجة القصور من الجهات القضائية المختصة في قدراتها التكنولوجية وليس في الدليل ذاته، كما اعتبر أنصار هذا الرأي الذي لا يعيب الدليل الإلكتروني أن الدليل بطبيعته المرنة يصل إلى استحالة التخلص منه[2].

المطلب الثاني: مشروعية الدليل الالكتروني

إن مجرد وجود دليل يثبت وقوع جريمة وينسبها للمتهم لا يكفي لبناء وتسبيب حكم الإدانة، إذ يجب أن يكون لهذا الدليل قيمة قانونية، تتوقف على خضوعه للقواعد المقرر في الإثبات الجنائي، بما فيها الأدلة الرقمية التي لا تكون مقبولة ومشروعة إلا إذا أجريت عملية البحث والكشف والحصول عليها وتقديمها أمام القضاء في إطار أحكام القانون والإجراءات

[1] يحي محمد انور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع الإسكندرية 2010، ص 655

[2] مسعود بن حميد المعمري، المرجع السابق، ص 200.

التي رسمها، وقيم العدالة وأخلاقياتها التي يحرص على حمايتها، وفي حالة الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد به مهما كانت دلالته الحقيقية، وحجيته في الاثبات وذلك لعدم مشروعيته[1].

الفرع الاول: المقصود بحجية الحصول على الدليل الالكتروني

المقصود بمشروعية الحصول على الدليل الالكتروني الجنائي يتمثل في الإجراء الذي استنبط منه القاضي الدليل يتفق مع القواعد القانونية التي تحكمه غير مخالف لأحكام الدستور أو قانون الإجراءات الجزائية، ويكون الدليل مشروعا متى كان من يباشره يستند إلى قواعد قانونية دون تعسف أو تجاوز، والهدف من ذلك هو حماية الحريات والحقوق الشخصية من تعسف سلطة التحقيق في غير الحالات التي رخص فيها بذلك[2].

كما أن قاعدة مشروعية الحصول على الدليل الجنائي الرقمي لا تقتصر فقط على مجرد مطابقة القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا مراعاة إعلان حقوق الإنسان والمواثيق والاتفاقيات الدولية وقواعد النظام العام، ومثال ذلك ما نصت عنه المادة 12 من الإعلان العالمي لحقوق الإنسان لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته. ولكل شخص حماية القانون من مثل هذا التدخل أو تلك الحملات[3].

ومشروعية الدليل هي إحدى أهم ما وصى به المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، المنعقد في عاصمة البرازيل في الفترة 4-9 سبتمبر 1994 في مجال اصلاح حركة الإجراءات الجنائية بالتوصية رقم 18 التي تنص على " كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة

[1] خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، ط 1، 2011، ص 235.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص213.

[3] المرجع نفسه.

ولا يمكن التمسك بها أو مراعاتها كما أشارت إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي والجرائم التقليدية في بيئة تكنولوجيا المعلومات وإلا ترتب عليها بطلان الإجراء فضلا عن تقرير المسؤولية لرجل السلطة العامة الذي انتهك القانون[1]".

ومن قبيل الأدلة غير المشروعة تلك المتحصل عليها من خلال إجراء مراقبة الاتصالات دون أن تكون محل لإذن من سلطة قضائية مختصة، أو اتخاذ ترتيبات تقنية من أجل تفتيش منظومة معلوماتية تؤدي بالمساس بالحياة الخاصة للغير، أو ممارسة أي إكراه معنوي على المشتبه فيه لفك شفرة نظام من نظم المعلوماتية، ويعد من الطرق غير المشروعة استخدام التدليس والخداع في الحصول على الأدلة الإلكترونية[2].

الفرع الثاني: مشروعية الحصول على الدليل الالكتروني

أكد المشرع الجزائري على ضرورة حماية الحياة الخاصة وعدم المساس بها وهذا الحق مكفول دستوريا من خلال نص المادة 39 من الدستور الجزائري والتي تنص لا يجوز انتهاك حرمة المواطن الخاصة، وحرمة شرفه، ويحميها القانون، وأضافت نفس المادة في فقرتها الثانية على أن سرية المراسلات والاتصالات الخاصة مضمونة بكل أشكاله وتأتي الحماية القانونية لهذا الحق الدستوري من خلال نص المادة 303 مكرر من قانون العقوبات إذ يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دينار جزائري إلى 300.000 دينار جزائري كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص وبأي تقنية كانت وذلك بالتقاط الصور أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

[1] سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي ورقة بحثية مقدمة إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة الجزائر، يومي 16 17 نوفمبر 2015

[2] عائشة بن قارة مصطفى، المرجع السابق، ص 218.

كما نص قانون الإجراءات الجزائية الجزائري على تقرير البطلان في حالة الحصول على دليل بطريقة غير مشروعة بما فيها الأدلة الرقمية وفقا لأحكام المادة 1-157 و 105 والمادة 191 وهذا الأمر يثير مسألة مهمة هي المعيار الذي يبين العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له، حتى يمتد إليها البطلان، وقد تعددت المعايير التي جاء بها الفقه إلا أن المعيار السائد في الجزائر هو أن العمل اللاحق يعتبر مرتبطا بالإجراء السابق إذا كان هذا الإجراء ضروريا لصحة العمل الاحق، فإذا أوجب القانون مباشرة اجراء معين قبل الآخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه كان الإجراء الأول شرطا لإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه[1].

وأما فيما يخص المشرع الفرنسي فقد كان السباق في حماية الحياة الخاصة وذلك بموجب إصداره لقانون رقم 70/643 المؤرخ في 17-07-1970بالإضافة إلى القانون رقم 78/17 الصادر في سنة 1978 والمتعلق بالمعالجة الالكترونية للبيانات الرسمية والذي تضمن حماية البيانات الشخصية المرتبطة بحياة الخاصة للأفراد[2].

بناء على ما سبق ذكره فقد حرص كل من المشرعين الجزائري والفرنسي على حماية الحياة الخاصة للأفراد، وذلك بالرفع من مكانة هذا الحق، وجعله في مصاف الحقوق الدستورية، بالإضافة إلى تقرير عقوبات على كل الأفعال التي تخل به، ولكن هذا لا يعني أنه لا يمكن المساس بهذا الحق بتاتا، إذ وضع القانون استثناءات على هذه القاعدة الدستورية وذلك بإمكانية المساس بهذا الحق إذا اقتضت الضرورة على نحو ما سار عليه المشرع الجزائري في المادة 03 من قانون 09/04 والتي تنص على " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو

[1] شهرزاد حداد، الدليل الالكتروني في مجال الاثبات الجنائي، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة العربي بن مهيدي أم البواقي 2016،2017، ص 91

[2] سوزان عدنان، انتهاك حياة حرمة الحياة الخاصة عبر الإنترنت دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانون، المجلد 29، العدد03، سوريا، 2013، ص 437.

المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانونا الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية، لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها، في حينها ، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية[1]

خلاصة الفصل الثاني

وفي خلاصة هذا الفصل يجدر بنا القول أنه لإثبات الجريمة الإلكترونية لا بد من إتباع طرق الإثبات المتعارف عليها، والتي تخضع للقواعد العامة للإثبات الجنائي.

ولكن ما يميز الجريمة الإلكترونية أنه عند تطبيق طرق الإثبات في مجالها ينتج دليل خاص بها وهو الدليل الإلكتروني.

[1] المرجع نفسه، ص 437.

خاتمة

الخاتمة

تعد هذه الدراسة حصيلة جهد قمنا به بهدف التصدي لموضوع إثبات الجريمة الإلكترونية، غير أنه لا يجب أن يكون الطابع التقني لمثل هذا النوع من الجرائم عقبة تمنعنا محاولة التوسع في قاعدة النقاش حول الإجرام المعلوماتي.

ونظرا لإلمامنا بالجوانب التقنية والجوانب القانونية لهذا الموضوع، إلا أن ذلك لا يمنعنا أيضا القول بأنه توصلنا في ختام هذه الدراسة إلى عدة جوانب يمكن بلورتها في عدة نتائج وتوصيات اتضحت من خلال تحليل وتفسير البيانات التي تم الحصول عليها خلال هذه الدراسة، وفي هذا الصدد سيتم عرض ملخص لأهم النتائج والتوصيات المتوصل إليها وذلك على النحو الآتي :

1- النتائج

هناك العديد من النتائج التي توصلت إليها هذه الدراسة، علما أنه ما تم التوصل إليه من نتائج الآن ربما يتغير مستقبلا بحكم طبيعة الجريمة الإلكترونية المرتبطة بالتقنية التي تتطور بشكل كبير، ويمكن إيجاز هذه النتائج كما يلي :

- أظهرت هذه الدراسة غياب مفهوم عام متفق عليه بين الدول حول التعريف القانوني للنشاط الإجرامي المتعلق بالجريمة المعلوماتية و الأنماط المكونة لها

- يعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية ويزداد الإثبات صعوبة في الجرائم الالكترونية حيث أن اكتشاف الجريمة الالكترونية أمر ليس بالسهل، وفي حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من الصعاب، مما يستلزم الكثير من الجهد والخبرة الفنية.

- إن الجريمة الالكترونية قد تكون جريمة تقليدية تضم جانب الكتروني، لاسيما في ظل ارتباط الناس بالتقنيات الحديثة التي انتشرت بشكل كبير وأهمها الحاسبات الآلية والهواتف الذكية، وقد تكون جريمة الكترونية مستقلة بذاتها.

– تواجه طرق التحقيق في إثبات الجريمة الالكترونية صعوبات متعددة، حيث تستدعي هذه الطرق في المقام الأول اكتشاف الجريمة الالكترونية ومحلها وبيئتها ثم الإبلاغ عنها، وأخذ إذن الجهات المختصة قبل القيام بالمعاينات والتفتيش للموقع أو الجهاز المشتبه به، وذلك للبحث عن الدليل الرقمي الالكتروني بالطرق الفنية ومن ثم إجراء التحريات والأبحاث التي تساعد في عملية الإثبات.

– تتسم الجرائم ذات الصلة بالحاسب الآلي بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو أثارها، هذه الخصائص العامة تقتضي أن تكون جهات التحري والتحقيق بل و حتى المحاكمة على دراية كبيرة بأنظمة الحاسب الآلي وكيفية تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها. تمثل الشهادة أهمية كبيرة في إثبات الجريمة الالكترونية في المواد الجزائية، فهي ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها، حيث يكون للشهادة أثناء التحقيق أثر كبير في ما يتعلق بالبراءة والإدانة كما لها أهميتها في الكشف عن الأدلة التي تساعد في إثبات الجريمة الالكترونية.

– إن محل الدليل الالكتروني ونطاق العمل به هو الجريمة الالكترونية، غير أنه يصلح كذلك لإثبات الجرائم التقليدية التي تم ارتكابها عن طريق تقنية الحاسب الآلي.

– تمتع الدليل الالكتروني بيقينية كبيرة بسبب الحرص على العمل بمبدأ مشروعية الدليل الالكتروني.

2– التوصيات

على ضوء هذه النتائج المتوصل إليها يمكن وضع جملة من التوصيات يمكن أن تساهم في تفعيل إثبات الجريمة الالكترونية وذلك كما يلي :

– تستدعي عملية التحقيق في الجرائم الالكترونية تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، بصورة تمكن رجال التحريات من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمة لذلك، ولتحقيق ذلك يجب زيادة الاهتمام بتدريب المكلفين بمباشرة التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال.

– فيما يتعلق بمعاينة الجريمة الالكترونية، فيجب تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد مواقعها بأسرع وقت ممكن، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملفات بهدف تعطيل الاتصالات لمنع تخريب الأدلة المتحصل عليها، مع تصوير الأجهزة الموجودة وبصفة خاصة الأجهزة الخلفية.

– يجب التأكد أيضا من عدم وجود مجالات كهرومغناطيسية في المحيط الخارجي لمسرح الجريمة حتى لا يتم أي إتلاف للبيانات المخزنة، وهذا يتطلب اختبارات وفحوصات تقنية قبل نقل أي مادة معلوماتية من مسرح الجريمة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر

1- القرآن الكريم

2- **القوانين**

- قانون رقم 04-15 المؤرخ في 10-11-2004 يعدل ويتمم الأمر رقم 15666، يتضمن قانون العقوبات، ج ر عدد
71 مؤرخ بتاريخ 10-11-2004المعدل والمتمم.

- قانون رقم 09-04 المؤرخ في 5-08-2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها، ج ر رقم 47 مؤرخ في 06-08-2009.

ثانيا: المراجع

1- الكتب

- عادل محمد فريد نائلة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط1، بيروت، لبنان، 2005.

- نهلا عبد القادر مومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الأولى، عمان، 2008.

- عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، مصر، 2006.

- اعداد مجمع البحوث والدراسات، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016.

- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، ط1، 2002.

- محمد أمين، أحمد الشوابكة، جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2004.

- جهاد محمد البريزات، الجريمة المنظمة -دراسة تحليلية-، دار الثقافة للنشر والتوزيع، ط1، عمان، 2008.

- محمد ناصر حمودي، العقد الدولي الإلكتروني المبرم عبر الانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى ، 2012.

- محمد على العربان الجرائم المعلوماتية، (دط)، دار الجامعة الجديدة للنشر، الإسكندرية 2011.

- هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

- عبد الحميد عبد المطلب ممدوح، جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية الجريمة عبر الانترنت، (دط)، مكتبة دار الحقوق، الشارقة، 2001.

- أحمد محمد شتاء، فكرة الحماية الجنائية لبرامج الحاسب الآلي، (دط)، دار الجامعة الجديدة القاهرة، 2000.

- هشام فريد رستم الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، 1994.

- أحمد حماد الهيتي، جرائم الحاسوب ماهيتها، أهم صورها والصعوبات التي تواجهها، (دط)، دار المناهج للنشر والتوزيع، عمان، 2005.

- عماد حامد أحمد القدو وإسراء جاسم محمد العمران، التحقيق الابتدائي، مركز الكتاب الأكاديمي، عمان الأردن ، ط1، 2015.

- محمد فاروق عبد الحميد كامل ، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ط1، (د س ن).

- علي شملال ، المستحدث في قانون الإجراءات الجزائية الجزائري ، الكتاب الأول(الاستدلال والإتهام) ، دار هومة للطباعة والنشر والتوزيع الجزائر، ط 2، 2017.

- علي حسن محمد الطوالبة التفتيش الجنائي على نظم الحاسوب والانترنت – دراسة مقارنة، عالم الكتاب الحديث اربد الطبعة الأولى 2004.

- عبد الرحمان خليفي، محاضرات في القانون الجنائي العام دون طبعة، دار الهدى، الجزائر،2010.

- خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي، الإسكندرية ، 2010.

- عبد الناصر محمد محمود فرغلي محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف للعلوم الأمنية، الرياض، 2007.

- جميل صليبا، المعجم الفلسفي، الجزء الأول، دار الكتاب العالمي، مكتبة المدرسة، بيروت، 1994.

- محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح المطبعة الأميرية القاهرة 2016 م / 1338هـ.

- محمد الامين البشري، لتحقيق في الجرائم المستحدثة الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، 2004.

- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، 2010.

- يحي محمد انور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع الإسكندرية 2010.

- خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، ط 1، 2010.

2- الاطروحات والمذكرات الجامعية

- نبيلة هبة هروال، جرائم الأنترنت دراسة مقارنة، أطروحة دكتوراه، ، جامعة تلمسان، الجزائر 2013-2014.

- - أحمد ضياء الدين مشروعية الدليل في المواد الجنائية رسالة دكتوراه منشورة ، كلية الحقوق جامعة عين شمس القاهرة 1982.

- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، رسالة لنيل شهادة الماجستير، رسالة ماجستير، جامعة مولود معمري، تيزي وزو الجزائر 2013.

- عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية -دراسة مقارنة- أطروحة ماجستير، جامعة الشرق الأوسط 2014.

- نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة ماجستير، جامعة منتوري، قسنطينة 2012-2013.

- تنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية ، جامعة نايف للعلوم الأمنية، الرياض، 2012.

- شهرزاد حداد، الدليل الالكتروني في مجال الاثبات الجنائي، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة العربي بن مهيدي أم البواقي 2016،2017

3- المقالات والمجلات العلمية

- اسمهان بوضياف، الجريمة الالكترونية والإجراءات التشريعية في مواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، الجزائر، العدد الحادي عشر، سبتمبر 2018.

– سوزان عدنان، انتهاك حياة حرمة الحياة الخاصة عبر الإنترنت دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانون، المجلد 29، العدد03، سوريا، 2013.

– رحيمة نمديلي، خصوصية الجرائم الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الجرائم الإلكترونية، المنعقد بطرابلس يومي 24، 25 مارس 2017.

– محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخداماتها، مجلة الحقيقة، العدد 41 دط، 2018.

– شريفة بن غدفة ، القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها، أعمال الملتقى الوطني. "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017.

– فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية طرابلس بتاريخ 24–25 مارس 2017.

– هشام محمد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي العدد 02، 1999.

– موسى البداينة ذياب، الجرائم الالكترونية –المفهوم والأسباب– ورقة مقدمة في الملتقى العلمي، – الجرائم المستحدثة في ضل التغييرات والتحولات الاقليمية والدولية، المملكة الأردنية الهاشمية، عمان، 2014.

– سورية ديش، أنواع الجرائم الالكترونية وإجراءات مكافحتها، مجلة الدراسات الاعلامية، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، العدد الأول، يناير 2018.

– صالحة العمري، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، العدد5 جامعة محمد خيضر بسكرة، د، س، ن.

– أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، العدد الأول، المجلد العاشر، جامعة الجلفة، 2017.

– أحمد الأمين البشري، التحقيق في جرائم الحاسب والانترنت، المجلة العربية للدراسات العربية والتدريب، المجلد 15، العدد 30، جامعة نايف للعلوم الأمنية، الرياض، 2001.

– معبد الحميد عبد المطلب ، أدلة الصور الرقمية، ورقة عمل مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخاصية الجرائم الإلكترونية الملامح والابعاد المنعقدة بلكلية الملك فهد الأمنية بالرياض مرة من 22 إلى 24 فريل 2007، الرياض، 2007.

– رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد5، كلية الحقوق السياسية، جامعة الوادي، الجزائر، 2012.

– نور الهدى قادري، الشهادة الالكترونية وحجيتها في الاثبات، مجلة الفكر القانوني والسياسي، المجلد السابع، العدد الاول، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الاغواط، 2023

– عادل بوزيدة ، دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية ، مجلة النبراس للدراسات القانونية ، المجلد الأول، العدد الأول، جامعة العربي التبسي، تبسة ، 2016.

– مسعود بن حميد المعمري، الدليل الالكتروني لإثبات الجريمة الالكترونية، مجلة كلية القانون الكويتية العالمية، كلية الحقوق، العدد3، الجزء الثاني، جامعة السلطان قابوس، مسقط، سلطة عمان، 2018.

– سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي ورقة بحثية مقدمة إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة الجزائر، يومي 16 17 نوفمبر 2015.

فهرس الموضوعات

فهرس الموضوعات

فهرس الموضوعات

الملخص

ملخص:

تقتضي الجريمة الالكترونية على غرار بقية الجرائم التقليدية أساليب خاصة للبحث والتحري عنها لطبيعتها الخاصة، الأمر الذي أدى بالمشرع إلى إستحداث إجراءات وأساليب إستثنائية لاثبات هاته الأخيرة.

بالاضافة إلى أنه يتوجب مع انتهاج هذه السياسة المغايرة في الاثبات معرفة مدى حجية هذا الدليل في اثبات وتكوين قناعة القضاة لأن هذا الدليل يواجه صعوبات اثناء تقييمه كونه مستحدث.

الكلمات المفتاحية:

الجريمة الالكترونية، حجية الدليل الرقمي، أساليب البحث، قناعة القاضي، إجراءات إستخلاص الدليل الرقمي، طبيعة الدليل الرقمي.

Abstract:

Like other traditional crimes, cybercrime requires special methods of research and investigation due to its special nature, which has led the legislator to develop exceptional procedures and methods to prove the latter adopting this different policy of evidence, it is necessary to know the extent of the authority of this evidence in the evidence and to form the conviction of the judges, because this evidence encounters difficulties during its evaluation because it is new.

Keywords: Cyber-crime, Authentic digital guide, Research methods, Judge's conviction, Digital evidence, extraction procedures, The nature of digital evidence.