الجمهورية الجزائرية الديمقراطية الشعبية
المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهد الحقوق

الرقم التسلسلي:.....

الرمـــــــــز: .....

لقسم : الحقوق

لشعبة: قانون عام.

التخصص: قانون جنائي.

الإثبات في الجريمة الإلكترونية في التشريع الجزائري

مذكرة لنيل شهادة الماستر في القانون الجنائي

إعداد الطالبتين:

- **بوحلوفة أميرة**
- **بوتارية ريان**

تحت إشراف الأستاذة

د. بعوش دليلة

أعضاء لجنة المناقشة		
اسم ولقب الأستاذ(ة)	الرتبة	الصفة
د. دعاس أحمد	(أستاذ محاضر ب)	رئيسا
د. بعوش دليلة	(أستاذة محاضر أ)	مشرفا ومقررا
د. بوكلاب سهام	(أستاذة محاضر ب)	مناقشا

السنة الجامعية 2025/2024

المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهد الحقوق

القسم : الحقوق الرقم التسلسلي:.....
الشعبة: قانون عام. الرمـــــــــز : .....
التخصص: قانون جنائي.

الإثبات في الجريمة الإلكترونية في التشريع الجزائري

مذكرة لنيل شهادة الماستر في القانون الجنائي

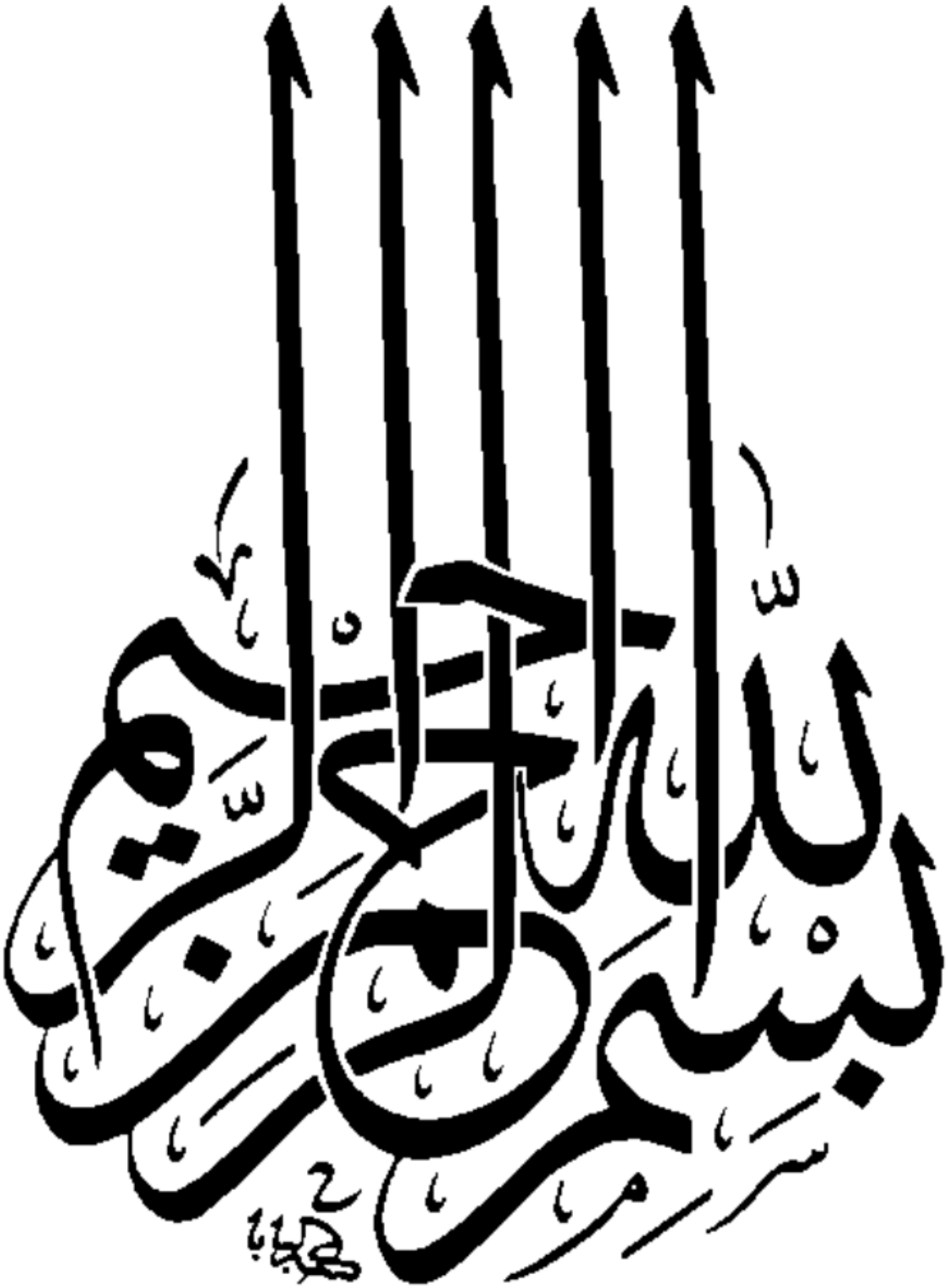
إعداد الطالبتين:
- **بوحلوفة أميرة**
- **بوتارية ريان**

تحت إشراف الأستاذة
د. بعوش دليلة

أعضاء لجنة المناقشة

اسم ولقب الأستاذ(ة)	الرتبة	الصفة
د. دعاس أحمد	(أستاذ محاضر ب)	رئيسا
د. بعوش دليلة	(أستاذة محاضر أ)	مشرفا ومقررا
د. بوكلاب سهام	(أستاذة محاضر ب)	مناقشا

السنة الجامعية 2025/2024


بسم الله الرحمن الرحيم

الشكر والتقدير

باسمك اللهم نستعين على أمور الدنيا والدين وبك آمنا وعليك توكلنا وإليك المصير

والصلاة والسلام على من بلغ الرسالة وأدى الأمانة ونصح الأمة، نبي الرحمة ونور العالمين

سيدنا محمد صلى الله عليه وسلم

هي كلمة أبت إلاّ الحضور، هي كلمة شكر وتقدير لله-عز وجلّ-فالحمد لله العلي القدير على نعمة الظاهرة والباطنة، الحمد لله الذي وفقنا على إتمام هذا العمل في أحسن الأحوال وأتمنى أن يكون سندا علميا نافعا لكل من يطلع عليه.

وفاءًا لأهل الوفاء، واعترافا بالفضل وتقديرا للجميل ونحن ننتهي من هذا العمل لا يسعنا إلاّ أن نتقدم بالشكر إلى الوالدين الكريمين الذي كان لهم الفضل في إنجاز هذا العمل المتواضع.

وسيـــرا عـــلى خطى الشاعـر الذي قـال:

قـــــم للمـــعلم وفـــيه التبـجـــيـل كـــاد المـــعلم أن يـــكون رســـولا

إلى كل من علّمنا حرفًا، أو أسدى إلينّا معروفا، وأخصُّ بالفضل الدكتورة "**بعوش دليلة**"

-حفظها الله-والتي تقبَّلتنا بصدر رحب طيلة عملنا، ولم تبخل علينا بالنصح والمشورة والتوجيهات المجيدة وتخصيصها لجزء من وقتها لمتابعة هذا العمل

إلى الأستاذين المشرفين على تأطير هذا العمل المتواضع.

كما أشكر كافة الأشخاص الذين ساعدونا في هذا العمل ولو بكلمة طيبة، سواء من قريب أو من بعيد

إهداء

بسم الله الرحمن الرحيم

"ما سلكنا البدايات الا بتيسيره وما بلغنا النهايات الا بتوفيقه وما حققنا الغايات الا بفضله فالحمد لله"

أهدي تخرجي إلى نفسي الطموحة التي لم تخذلني ابدا...

إلى الذي كلل العرق جبينه ومن علمني ان النجاح لا يأتي الا بالصبر والإصرار...

إلى النور الذي أنار دربي والسراج الذي لا ينطفأ نوره بقلبي ابدا...من بذل الغالي النفيس وإستمديت منه قوتي واعتزازي بذاتي...

...أبي الغالي...

إلى من جعل الجنة تحت اقدامها وسهلت لي الشدائد بدعائها...

إلى اليد الخفية التي أزالت التي أزالت عن طريقي العقبات...

...أمي الغالية...

إلى ضلعي الثابت وأمان أيامي...

إلى من شددت عضدي بهم فكانوا ينابيع ارتوي منها الى خيرة ايامي وصفوتها...**إلى قرة عيني...أختي وإخواني...**

لكل من كان عون وسندا في هذا الطريق...**صديقاتي ومن أحب** ...

إلى من تمنوا رؤيتي في هذا المكان...**عائلتي...**

إلى تلك الانسانة العظيمة لطالما تمنيت ان تقر عينها برؤيتي في يوم هكذا...

الى التي توسدها التراب...**جدتي رحمها الله...**

{وآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ}

أميرة

إهداء

مهما كتبت من عبارات لن أجد أصدق من قوله تعالى:" **يرفع الله الذين امنوا منكم والذين أوتوا العلم درجات**"

إلى الذي كلل العرق جبينه ومن علمني ان النجاح لا يأتي ألا بالصبر والإصرار...

إلى النور الذي انار دربي والسراج الذي لا ينطفأ نوره بقلبي أبدا...من بذل الغالي النفيس وإستمديت منه قوتي وإعتزازي بذاتي...

...أبي الغالي...

إلى من علمتني الأخلاق قبل أن أتعلمها إلى الجسر الصاعد بي الى الجنة الى اليد الخفية التي أزالت عن طريقي العقبات ومن ضلت دعواتها تحمل اسمي ليلا ونهارا...

...أمي الحبيبة...

إلى ضلعي الثابت وامان ايامي...

إلى من شددت عضدي بهم فكانوا ينابيع ارتوي منها إلى خيرة أيامي وصفوتها...

إلى قرة عيني...أخواتي وإخواني...

لكل من كان عونا وسندا لي من قريب أو من بعيد في هذا الطريق...**الأصدقاء والأوفياء ورفقاء السنين**

لأصحاب الشدائد والأزمات...

إلى من أفاضني بمشاعره ونصائحه المخلصة...

...إلى عائلتي...

أهديكم هذا الإنجاز وثمرة نجاحي الذي طالما تمنيته ها أنا اليوم أكملت وأتممت أول ثمراته بفضله سبحانه وتعالى

{وَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ}

ريان

مقدمة:

مع التطور العلمي التكنولوجي وبظهور ما يعرف بتكنولوجيا المعلوماتية التي شهدها العالم مؤخرا والتي غيرت مجرى الحياة والتي مست بشكل جذري في تغيير نمط الأفراد والمجتمعات وجميع جوانب الحياة، وعلى غرار الجانب القانوني لم يكن في منأى عن هذا التطور. حيث تميز هذا العصر بالتطور المتسارع على جميع المستويات وفي جميع المستويات وفي جميع القطاعات، ورغم ما يترتب من إيجابيات التكنولوجيا في إطار تحقيق العدالة إلا أنها تفرز بعض التداعيات وبعض الجوانب السلبية، التي تقف كحائل أمام ما تصبوا إليه العدالة الجنائية، وأمام انتشار الظاهرة الإجرامية التي ترتبط بالعالم الرقمي مما أدى إلى تدخل المشرع لتكريس واستحداث آليات تتماشى وطبيعة هذه الجرائم الخاصة والمتمثلة أساسا في الجرائم الرقمية والتكنولوجية.

كما ترتكب هذه الجرائم في بيئات رقمية باستعمال الخوادم والهواتف النقالة واعتمادا على الأنترنت ونظرا لتعقد هذه الجرائم يصعب على المحقق اكتشافها إلا أن المشرع الجزائري ضمن عدة وسائل وسبل وأدوات من أجل التحقيق في مثل هذه الجرائم وكذا ضمان طرق إثبات هذه الجرائم. ومن أهم وأبرز هذه الأدوات الدليل الرقمي الذي يعتبر واحدا من أدوات البحث الرقمي الجنائي وهو علم يختص بتتبع وتحليل الأدلة الرقمية المتعلقة بالجرائم الإلكترونية ويعتبر من العلوم الحديثة المستغلة بالتحقيق الجنائي.

ومن هذا المنطلق يمكننا القول ان الجرائم الإلكترونية لا يمكن التعامل معها من خلال الإجراءات التقليدية المعروفة بسبب استخدام الجاني الإلكتروني وسائل جديدة تختلف عن الوسائل التقليدية، حيث تعتبر هذه الوسائل أكثر تطورًا وأكثر تقنية الشيء الذي يصعب على المحقق اكتشافها أو رصدها، وفي هذا السياق يبرز الدليل الرقمي كوسيلة أساسية في الكشف عن الجرائم المعلوماتية مع الاعتماد على أدوات وتقنيات حديثة احتراما لسلامة وضمان الإجراءات وعدم التأثير على قوة الدليل.

وقد أثبتت التجربة العلمية أن الإثبات الرقمي يمثل ركيزة محورية في التصدي للجرائم المعلوماتية، وهو ما أدى إلى ظهور خلافات فقهية وقانونية بشأن مشروعية هذه الأدلة وقوتها في الإثبات وخاصة في ظل غياب نصوص قانونية بشأن مشروعية هذه الأدلة وقوتها في الإثبات وخاصة في ظل غياب نصوص قانونية واضحة تنظم استخدامها، وقد أسفر ذلك عن ظهور العديد من الإشكاليات على الصعيد الوطني والدولي، تتعلق بكيفية التوفيق بين المبادئ القانونية التقليدية والطبيعة الخاصة للجرائم المعلوماتية.

1. الإشكالية:

من خلال ما سبق ذكره نصل لطرح الإشكالية التالية:

ما مدى اعتراف المشرع بالدليل الإلكتروني في الإثبات الجنائي؟

2. الأسئلة الفرعية:

وهذه الإشكالية تتفرع عنها مجموعة من التساؤلات الفرعية كالآتي:

- ما المقصود بالجريمة الإلكترونية، وماهي الخصائص الجوهرية التي تميزها؟
- ما المقصود بالدليل الإلكتروني، وماهي أهم سماته؟
- كيف يتم التحقيق في الجريمة الإلكترونية، وماهي الآليات القانونية لجمع الأدلة الرقمية في القانون الجزائري؟
- ما القيمة للأدلة الإلكترونية في إثبات الجريمة الإلكترونية؟

3. الفرضيات:

- قد يكون التشريع الجزائري غير كاف لمواكبة التطور التقني المتسارع للجريمة الإلكترونية مما ينعكس سلبا على فعالية الإثبات.

4.المنهج المتبع:

اعتمدنا في دراستنا هذه على المنهج الوصفي، في وصف الجريمة الإلكترونية والدليل الإلكتروني الناتج عنها، بالإضافة إلى منهج تحليل المحتوى من خلال دراسة وتحليل مضمون النصوص القانونية الموضوعية والإجرائية الخاصة بإحراز الدليل الالكتروني، مع اعتمادنا في بعض الأحيان على المنهج المقارن لمعرفة موقف المشرع الجزائري في بعض المسائل المقارنة مع التشريعات الأخرى، وذلك للاستفادة من تجارب الدول الأخرى.

5.أسباب اختيار الموضوع:

إن اختيارنا لموضوع الإثبات في الجرائم الإلكترونية يرجع إلى العديد من الأسباب بعضها موضوعية وأخرى ذاتية:

- **فمن الأسباب الموضوعية:** فتتمثل في معرفة مدى مواكبة التطور التكنولوجي من طرف القضاء الجزائي الجزائري باعتبار أن هذا التطور تتبعه خطورة المجرمين الذين يستخدمون هذه التقنيات الحديثة لأغراض غير مشروعة ومخالفة للقانون، وبيان مدى القواعد اللازمة لاعتماد الدليل الإلكتروني كدليل إثبات موضوعي وموثق أمام القاضي الجزائي بصفة عامة، والقاضي الجزائي الجزائري بصفة خاصة.

-**أما الأسباب الذاتية:** الرغبة في دراسة هذا الموضوع والميول إلى المجال القضائي، وحب الاطلاع على الأدلة الإلكترونية. بالإضافة إلى نقص الدراسة في الموضوع، باعتبار انه موضوع مستحدث نسبيا. ومن جهة أخرى لنا الفضول لمعرفة مدى سلطة القاضي الجزائي في التقدير والاقتناع بالدليل الرقمي، لأنه موضوع فرض نفسه في الوقت الراهن لأنه جاء مصاحبا للتطور التكنولوجي في مجال نظم المعلومات.

6.أهمية الموضوع:

لقد قمنا باختيار هذا الموضوع وجعلناه محور دراستنا في هذه المذكرة بالنظر إلى الأهمية البالغة التي يحظى بها موضوع الإثبات في الجرائم الإلكترونية تُعد من الظواهر الحديثة والمنتشرة على نطاق واسع حاليا، كما أنها تعد من المواضيع التي أثارت جدلاً واسعا بين فقهاء القانون الجنائي. ويزداد الاهتمام بهذا الموضوع مع تطور الوسائل الحديثة، لاسيما الوسائل الإلكترونية التي أفرزت أساليب جديدة لارتكاب هذا النوع من الجرائم، مما يُلقي عبئا إضافيا على المشتغلين في مجال القانون من حيث البحث والتحقيق وإثبات هذا النوع من الجرائم، حيث أن قواعد البحث والتحقيق وأسس الإثبات الجنائي في القوانين القديمة لا تكفي، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلاءم مع طبيعتها الفنية.

وتزداد أهمية البحث في هذا المجال بالنظر إلى أن التطور العلمي أفرز العديد من وسائل الإثبات الحديثة من بينها الدليل الرقمي، مما يطرح إشكالات متعددة تتعلق بكيفية تقديره أمام القضاء الجنائي، ومدى تأثيره في إثبات الجرائم الإلكترونية. وتبرز أهمية هذا الموضوع بشكل خاص عند بحث دور القاضي الجنائي في مواجهة هذه الجرائم، التي تتطلب في الغالب خبرة تقنية ومعلوماتية، نظراً لطبيعتها المرتبطة بمسائل فنية دقيقة.

7.أهداف الموضوع:

تتلخص أهداف البحث فيما يلي:

معرفة نوع جديد من الجرائم وهو الجرائم الالكترونية، ومدى مواكبة القانون للتطور التكنولوجي رغم أنه أقل سرعة في التطور، وكيفية تعامله مع الأدلة الحديثة وبالضبط الدليل الإلكتروني، وكيفية تعامل السلطات القضائية مع هذه الأدلة من خلال الإجراءات التي يتم من خلالها حصول على هذا النوع من الأدلة. وإبراز الأعمال الإجرائية المعتمدة للوصول الى الدليل الرقمي والتعريف بهذه الإجراءات، ثم تحديد المعيار الضامن لمشروعية هذه الأعمال الإجرائية، من الواضح أن رصد الأدلة الإلكترونية وضبطها بغية الوصول الى إثبات الجريمة الإلكترونية يعد من الصعوبة للنظر في الجريمة بحد ذاتها.

8.الدراسات السابقة:

تعد الدراسات السابقة أحد أهم الأجزاء التي تحتويها الدراسة، اذ لا يمكن للبحث ان يكون بحثا علميا صحيحا متكاملا، ومن أهم المراجع التي اعتمدنا عليها في دراستنا نجد كتاب الإثبات الجنائي في الجريمة الإلكترونية للدكتور أشرف عبد القادر قنديل، إضافة الى كتاب حجية الدليل الإلكتروني في الإثبات الجنائي للدكتورة عائشة بن قارة مصطفى.

9.صعوبات الدراسة:

لا يفوتنا القول أنه تلقينا صعوبات في اختيار موضوع البحث، كون هذا الموضوع " الإثبات في الجريمة الإلكترونية في التشريع الجزائري " حديث لم يسبق بحثه بوضوح وتعمق ولو أنه هناك مراجع ومقالات تناولت هذا الموضوع، إلا أنها لم تعالجها من كل جوانبه، كما صادفنا قلة المراجع والبحوث في هذا الموضوع تحديدا وخاصة المراجع الجزائرية، بالإضافة الى الطابع التقني للموضوع، مصطلحات تقنية شكلت لنا صعوبة خلال إنجاز المذكرة حيث يتطلب هذا الموضوع فهم الباحث للشق التقني للموضوع وما يصاحب دالك من صعوبات، إضافة الى الشق القانوني.

10.حدود البحث:

يقتصر هذا البحث على دراسة "موضوع الإثبات في الجرائم الإلكترونية" في ظل أحكام التشريع الجزائري وذلك من خلال تحليل النصوص القانونية ذات الصلة، خاصة القانون رقم 09_04 وقانون الإجراءات الجزائية، كما تركز الدراسة على الجانب الإجرائي لكيفية الإثبات في الجرائم الإلكترونية وتشمل أيضا الجانب الجنائي على تحليل الأفعال المجرمة المرتبطة بالجريمة الإلكترونية، مع التطرق إلى الجانب الفني بالقدر الذي يساهم في فهم الطبيعة التقنية لهذه الجرائم وآليات ارتكابها، وتمتد الحدود الزمانية للدراسة لتشمل الفترة من 03/03/2025 إلى 19/05/2025.

11.خطة الدراسة:

وللإجابة على الإشكالية الرئيسية والتساؤلات الفرعية السابقة، ارتأينا تقسيم الخطة إلى فصلين أساسيين، وكل فصل يحتوي على مبحثين:

- **الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية والدليل الإلكتروني.**
  - **المبحث الأول:** ماهية الجريمة الإلكترونية.
  - **المبحث الثاني:** ماهية الدليل الإلكتروني.
- **الفصل الثاني: الإطار القانوني للإثبات في الجريمة الإلكترونية.**

- **المبحث الأول:** التحقيق في الجريمة الإلكترونية وإجراءات جمع الأدلة.
- **المبحث الثاني:** حجية الأدلة الإلكترونية في الوقائع المراد إثباتها.

وأنهينا بحثنا بخاتمة ضمناها أهم النتائج والتوصيات المقترحة.

الفصل الأول:

الإطار المفاهيمي للجريمة الإلكترونية والدليل

لقد شهد العالم في الآونة الأخيرة تطور ملحوظ في مجال التكنولوجيا والرقمنة، ومع الاستعمال اليومي لوسائل التكنولوجيا، الشيْ الذي ساهم في بروز وانتشار نوع جديد من الجرائم لها طبيعة خاصة حيث تتسم بالخطورة وبكونها معقدة وذات أبعاد حيث يعتبر الحاسب الآلي وشبكة الأنترنت بيئات افتراضية لارتكاب الجرائم التكنولوجيا، الأمر الذي قد ينجر عنه ارتكاب جرائم لها علاقة بهذا المجال، وهو ما يعرف بالجريمة الإلكترونية.

ان الوسط الذي ترتكب فيه الجريمة الإلكترونية يختلف من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي وعلى ضوء ذلك فإن الدليل المناسب لإثبات الجريمة الإلكترونية هو الدليل الإلكتروني كما عبرت عنه الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، فطبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها، وبإسقاط على الجريمة، فإنه يمكن أن تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها.

وفي هذا السياق سنتطرق في هذا الفصل إلى:

- **المبحث الأول: ماهية الجريمة الإلكترونية.**
- **المبحث الثاني: ماهية الدليل الإلكتروني.**

المبحث الأول

ماهية الجريمة الإلكترونية

تعد الجريمة الإلكترونية من بين الجرائم المستحدثة التي ظهرت في العصر الحديث، والسبب يرجع إلى ارتباط هذه الجرائم بوسائل التقنيات الحديثة والمتمثلة في أجهزة الكمبيوتر وشبكات الأنترنت والمواقع الإلكترونية، ولقد أدى الانتشار الكبير للتكنولوجيا الحديثة والتفشي المذهل للجريمة الإلكترونية إلى زيادة اهتمام الباحثين والمختصين من ميادين عدة كالقانون، الإعلام والاتصال، السياسة، الاقتصاد وغيرها بهذا الموضوع، مما أدى إلى تنوع تعاريفها ومسمياتها، ومن ثم صعوبة إيجاد تعريف جامع لها.

وسنحاول من خلال هذه الجزئية من دراستنا تفصيل الإطار القانوني لهذه الجريمة من خلال التطرق إلى مفهومة الجريمة الإلكترونية وخصائصها (المطلب الأول)، ثم إلى أركان هذه الجريمة وأنواعها (المطلب الثاني).

المطلب الأول

مفهوم الجريمة الإلكترونية

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك عدة تسميات لها منها الجريمة المعلوماتية، وجرائم إساءة استخدام تكنولوجيا الاتصالات، وجرائم الحاسوب والأنترنت، بالإضافة إلى الجرائم المستحدثة الناجمة عن التطورات اليقينية[1].

ويجدر التمييز بين الجريمة الإلكترونية والجرائم التقليدية، حيث تعتمد الأولى على الاعتداء على الأنظمة الحاسوبية والبرمجيات والبيانات المخزنة فيها. بينما تشمل جرائم الأنترنت عمليات نقل غير مشروعة للمعلومات، عبر الشبكات الرقمية أو باستخدام الهواتف المحمولة، ويرجع انتشار هذا النوع من الجرائم إلى التطور التكنولوجي الذي أدى إلى تداخل وتكامل المجالات الحاسوبية المختلفة والاتصالات وظهور مصطلح "cyber crime"[2] انقسم الفقهاء إلى اتجاهين في تحديد مفهوم الجريمة الإلكترونية حيث يرى البعض أنها ذات نطاق ضيق يقتصر على الجرائم المتعلقة بالحاسوب والأنترنت، حيث يعتقد آخرون أن مفهومها أوسع، ليشمل أي فعل إجرامي يتم باستخدام التكنولوجيا الحديثة.

[1] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة 2008، العدد 7، ص112.

[2] مفتاح بوبكر المطرودي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 2012/25/23 ص13.

بناءً على ذلك سنقوم في هذا المطلب بتوضيح تعريف الجريمة الإلكترونية في (الفرع الأول)، ثم الحديث عن خصائصها في (الفرع الثاني).

الفرع الأول

تعريف الجريمة الإلكترونية

تعددت التعاريف بخصوص الجريمة الإلكترونية، وقد ذهبت أغلبها إلى الانطلاق من وسيلة ارتكاب الجريمة، إذ أن أصحاب هذا الاتجاه يعتبرون أن جريمة الكمبيوتر تتحقق باستخدام الجهاز، وهو الشيء الذي تم انتقاده على أساس أن تعريف الجريمة يستدعي الرجوع إلى العمل الأساسي المكون لها وليس فحسب إلى الوسائل المستخدمة لتحقيقه، بمعنى أنه ليس مجرد أن استخدام جهاز الحاسوب في جريمة ما يمكن أن نعتبرها من الجرائم الإلكترونية[1].

بينما يذهب اتجاه آخر في تعريفه للجريمة المعلوماتية إلى ربطها بالمعرفة الفنية باستخدام الحاسوب، حيث تعتبر المعرفة الفنية شرطا ضروريا للقول بكون جريمة ما تدخل ضمن زمرة الجرائم المعلوماتية، كمثال لأخذ التعاريف الذي قدمه هذا الاتجاه، هي: "جريمة تتطلب لاحترافها أو لارتكابها أن تتوفر لدى فاعلها معرفة بتقنية النظام المعلوماتي".

أولا: تعريف الجريمة الإلكترونية

1. التعريف الفقهي للجريمة الإلكترونية:

انقسم الفقه في تعريفه للجريمة الإلكترونية على اتجاهين، اتجاه تبنى التعريف الموسع واتجاه تبنى التعريف الضيق.

أ. الاتجاه الموسع للجريمة الإلكترونية:

يرى هذا الفريق من الفقهاء ضرورة التوسيع من مفهوم الجريمة الإلكترونية خشية حصرها في مجال ضيق فقدم عدة تعاريف منها:

"كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الجاني"[2].

---

[1] امحمد اقبلي وعابد العمراني الميلودي، "القانون الجنائي الخاص المعمق في شروح"، الطبعة الأولى، مكتبة الرشاد سلطات للنشر والتوزيع، د.ب.ن،2020، ص285.

[2] حنان مهداوي، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية جامعة محمد لمين دباغين سطيف2، المجلد 6، العدد 02،2 /2022/11، ص1060.

"كل فعل أو امتناع عمدي، ينشأ عن استخدام غير المشروع لتقنية المعلوماتية، يهدف إلى الاعتداء على الأموال المادية أو المعنوية"[1].

"كل سلوك سلبي أم إيجابي تم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت"[2].

" عمل أو امتناع عن عمل يأتيه الإنسان، إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب".[3]

تظهر التعاريف السابقة اتساعًا كبيراً في مفهوم الجريمة الإلكترونية، إذ يلاحظ أن هذا الاتساع قد يؤدي إلى وصف بعض الأفعال بأنها جرائم إلكترونية رغم أنها لا ترتبط بالضرورة باستخدام الحاسوب في تنفيذها. فقد تُرتكب بعض الجرائم، مثل سرقة الحاسوب أو الأقراص المضغوطة، دون أن يكون الحاسوب ذاته وسيلة أو أداة في الجريمة، وإنما مجرد محل للاعتداء. وبالتالي، لا يمكن اعتبار كل فعل مرتبط بالحاسوب جريمة إلكترونية إلا إذا كان هذا الارتباط له دور فعلي في تنفيذ الجريمة[4].

ب.الاتجاه الضيق للجريمة الإلكترونية:

من أهم التعريفات التي وضعها أنصار هذا الاتجاه:

" كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى"[5]. حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية.

يرى الأستاذ rosenblatt بأن الجريمة الإلكترونية هي" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقة "[6].

---

[1] عبد الحكيم مولاي براهيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة الجزائر، المجلد 2، العدد 23، 2015/06، ص213.

[2] نسرين سيد سلامة، الجرائم الإلكترونية وأثرها على المجتمع الجزائري، مجلة القاهرة للخدمة الاجتماعية، كلية الآداب جامعة المنصورة، العدد 39، 2023/06، ص404.

[3] عبد العال الديربي، الجرائم الكترونية، دراسة قانونية قضائية مقارنة، طبعة 1، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص41.

[4] حنان مهداوي، المرجع السابق ص1060.

[5] نهلا عبد القادر المومني، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، 2008، ص48.

[6] سعد فهد الدبيس المطيري، مفهوم الجرائم الإلكترونية وسماتها، مجلة متخصصة في الدراسات والبحوث القانونية، المجلد 16، العدد 5، 2023، ص1249.

يرى الفقيه الألماني Tiedemann أن " كل أشكال السلوك الضار بالمجتمع الذي يرتكب باستخدام الحاسب، فهو يرتكز في تعريفه على وسيلة ارتكاب الجريمة ".

يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب cybercrime أنها:" الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا، وارتكز كذلك في تعريفه على الوسيلة المرتكبة بها الجريمة.

"الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج دورًا أساسيا[1].

يؤخذ على هذه التعاريف أنها لم تحِط بظاهرة الإجرام الإلكتروني من جميع جوانبها، إذ ركز بعضها على الجانب الإجرامي فقط، في حين ركز البعض الآخر على الوسيلة الإلكترونية المستخدمة، بينما انتصبت تعاريف أخرى على الطابع السلوكي أو التشهيري للجريمة.

2. التعريف القانوني للجريمة الإلكتروني (تعريف المشرع الجزائري)

استخدم المشرع الجزائري في البداية مصطلح " جرائم المساس بأنظمة المعالجة الآلية للمعطيات "، وذلك بعد استحداثها بموجب القانون 04_15 المعدل و المتمم للأمر 66_156 المتضمن قانون العقوبات، بعد ذلك استعمل مصطلح " الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال " وذلك بموجب القانون 09_04[2] المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، حيث عرفها في المادة 02 منه كما يلي :" الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ".

ويلاحظ من هذا التعريف أن المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية، أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكترونية، وثانيها معيار موضوع الجريمة وهو المساس بأنظمة الآلية للمعطيات، فمن خلال النص القانوني المذكور نجد أن المشرع قد أحال إلى قانون العقوبات، وبالتالي كل الأفعال المجرمة في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات تشكل موضوعا للجريمة الإلكترونية، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات. كما اعتقد المشرع الجزائري على معيار رابع في تحديد نطاق

[1] حنان مهداوي، المرجع السابق، ص1061.

[2] القانون رقم 09_04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الجريمة الإلكترونية، كونه أقر أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجريمة الإلكترونية في القانون الجزائري[1].

وترتيبا على كل هذه التعاريف الفقهية والتشريعية، يمكننا تعريف الجريمة الإلكترونية بأنها هي كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته، يمس بالأشخاص أو الأموال أو أمن الدولة، وهو ما يبرر تجريم هذا السلوك وتقرير العقوبات المناسبة له.

أي أن الجريمة الإلكترونية على سبيل الجرائم التقليدية تعرف من خلال أركانها أي توفر القصد الجنائي لارتكاب هذه الجريمة والركن المادي للجريمة وركنها القانوني.

ثانيا: نقاط الاختلاف بين الجريمة الإلكترونية والجريمة التقليدية

يكمن الاختلاف الحقيقي بين نوعي الجريمة في بعض الخصائص التي نتفرد بها كل جريمة وهي:

– بحكم أن الجريمة ظاهرة اجتماعية، فالمتفق عليه أن هناك تشابه بين الجريمة الإلكترونية والعادية في عناصرها الثلاثية المتمثلة في وجود الجاني والضحية وفعل الجريمة، وتختلف الجريمة الالكترونية عن الجريمة العادية باختلاف البيئات والوسائل المستخدمة. وباعتبار أن الجريمة التقليدية والاعتيادية المعروفة تتم بوجود الجاني والضحية في مكان ما، فالجريمة الالكترونية عكس ذلك لأنها في الغالب تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث، وبمعنى آخر في الجرائم الإلكترونية قد لا يُوجد الجاني والضحية في مسرح الجريمة، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الاتصال الحديثة والشبكات الإلكترونية، وقد نفهم أيضا أن أداة الجريمة هنا هي الأجهزة الرقمية والمعلوماتية المتطورة، عكس الجريمة التقليدية التي كثيرا ما يلجأ الجاني أو المجرم إلى عدة أدوات تختلف باختلاف ظروف مسرح الجريمة[2].

– شخصية المجرم في الجرائم التقليدية شخص عادي قد يكون متعلم أو لا أما في الجريمة الالكترونية فهو من المتعلمين والمتعمقين في فنيات الحاسب ملما بمهارة استخدامه ومعارف تشغيله[3].

– صعوبة إخفاء الجريمة التقليدية بينما تكون الجرائم الإلكترونية مخفية ولا يمكن اكتشافها في حينها إلا أنه يمكن ملاحظة آثارها، والتخمين بوقوعها.

---

[1] نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، 24_25 مارس 2017، ص100.

[2] ندير ارتس وآخرون، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، الطبعة الأولى، المملكة المتحدة: المركز المغاربي– شرق أدنى للدراسات الاستراتيجية، 2024، ص 5.

[3] نورة قناش، مذكرة بيداغوجية في مقياس: الجرائم المستحدثة، موجهة لطلبة السنة الثانية ماستر علم اجتماع الجريمة والانحراف، جامعة سكيكدة، السنة الجامعية 2020–2021، ص 20.

– الدافع في الجرائم العادية هو الانتقام والقهر والمنفعة المادية بينما في الجرائم الالكترونية هو الربح السريع أو المغامرة وحب التحدي والمتعة وقد يكون الانتقام وإلحاق الضرر بالمعتدى عليه سواء كان شخص طبيعي أو معنوي[1].

– بالإضافة إلى ذلك تتحقق الجرائم الإلكترونية بمجرد اختراق وتتبع حسابات الغير، كما تتسم الجرائم الالكترونية بالاستمرارية، فهي جريمة دائمة التجدد طالما أنها موجودة على مواقع شبكات الحاسوب على خلاف الجرائم التقليدية التي تنتهي بوقوع الجريمة، في حين أن الجريمة التقليدية تتحقق بتواجد القصد الجنائي. وكذلك تتسم الجرائم الإلكترونية بالعالمية، حيث أن هذه الجرائم تتم باستخدام العالم الافتراضي الذي لا تقيده الحدود الجغرافية، الأمر الذي يجعل اكتشاف مرتكبها في غاية الصعوبة، فهؤلاء الجناة يمكنهم بسهولة إخفاء هويتهم الحقيقية، عكس الجريمة التقليدية التي هي ظرفية ومحددة ومكانيا[2].

– تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح. إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا يتطلب عنفا، فنقل بيانات من كمبيوتر إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

– تتميز جرائم الأنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، لأن المجرم غير ظاهر ويخفي هويته ويستخدم أدوات يصعب كشفها من جهة وغياب الدليل المادي وسهولة محو الدليل أو تدميره بعد اقتراف الجريمة مباشرة[3].

– تعتمد هذه الجرائم على قمة الذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم. إذ يصعب عليه متابعة جرائم الأنترنت والكشف عنها وإقامة الدليل عليها. فهي جرائم تتسم بالغموض، وإثباتها يتسم بالصعوبة والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية[4].

– صعوبة المطالبة بالتعويض المدني بخصوص جرائم الأنترنت.

الفرع الثاني

خصائص الجريمة الإلكترونية

[1] نورة قناش، المرجع السابق، ص 20.

[2] ندير إدريس وآخرون، المرجع السابق، ص 5.

[3] نورة قناش، المرجع السابق، ص 21.

[4] المرجع نفسه.

يرتبط مفهوم الجريمة الإلكترونية ارتباطاً وثيقاً بالحاسوب وشبكة الأنترنت، وهو ما يمنحها خصائص وسمات تميزها عن غيرها من الجرائم التقليدية. ويعود هذا التمييز إلى طبيعتها الوظيفية التي تعتمد على التكنولوجيا الحديثة، وإلى علاقتها المباشرة بالأجهزة الإلكترونية. وقد انعكس هذا الارتباط بالتقنية العالية على السلوك الإجرامي المرتكب[1]، وهو ما سيتم بيانه من خلال العناصر التالية:

أولا: السمات الخاصة بالجريمة الإلكترونية

تتسم الجريمة الإلكترونية بجملة من الخصائص وهي كالآتي:

1. جريمة عابرة للحدود:

إن تعبير جرائم عابرة للدول أو جرائم عبر وطنية هي تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعرف بالحدود الجغرافية للدول كجرائم تبييض الأموال، والمخدرات، وغيرها.

وفي عصر الحاسب الآلي ومع انتشار شبكة الاتصالات العالمية (الانترنت)، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والاتصال فيما بينها أمرا سهلا، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، سواء تم ذلك بطرق مشروعية أو غير مشروعة.[2]

وفي هذه البيئة يمكن أن توصف جرائم التقنية بأنها جرائم عابرة للدول، إذ غالبا ما يكون الجاني في بلد، والمجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، وعليه تعتبر جرائم التقنية شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية[3].

2. صعوبة الكشف عنها وإثباتها:

تتميز الجريمة الإلكترونية بكونها لا تترك آثارًا مادية لما بعد ارتكابها، وصعوبة الاحتفاظ الفني بآثارها إن وجدت، إذ ليس هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات لذا نجد أن معظم جرائم الأنترنت تكتشف بالمصادفة، أو بعد فترة طويلة من ارتكابها.

3. جريمة هادئة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الإلكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس

[1] نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع الجزائري منها، رسالة لنيل شهادة الماجيستر في القانون الجنائي، جامعة الجزائر 1، يوسف بن خدة، 2016-2017، ص 92.

[2] أسامة أحمد المناعسة، وجلال محمد الزغبي "جرائم تقنية نظم المعلومات الإلكترونية"، الطبعة الأولى، دار الثقافة والنشر والتوزيع، عمان (الأردن)، 2010، ص 27.

[3] المرجع نفسه.

القائم على معرفة تقنية الكمبيوتر. وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيديرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف.[1]

4. الجرائم الإلكترونية جرائم الأذكياء:

إن مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ومهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب وكيفية تشغيله، وكيفية تخرين المعلومات والحصول عليها، في حين أن مرتكب الجريمة التقليدية في الغالب شخص أمي بسيط متوسط التعليم.[2]

5. خصوصية مجرم المعلومات:

المجرم الذي يرتكب الجريمة المعلوماتية يطلق عليه تسمية المجرم الإلكتروني أو المعلوماتي يتسم بخصائص المجرم الذي يرتكب الجريمة المعلوماتية يطلق عليه تسمية المجرم الإلكتروني أو المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (الجرم التقليدي)، فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الأنترنت.[3]

6. جريمة مستحدثة:

الجريمة الإلكترونية تعتبر من الجرائم المستحدثة، بل إنها أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، بحيث ظهرت تبعا للتطور الهائل في مجال التقنية العالية، وهو ما جعل أمر تحديد هذا النمط من الإجرام وإدراجه ضمن طائفة الجرائم التقليدية المعروفة تكتنفه صعوبات ترجع إلى الطبيعة الخاصة بها باعتبارها تطال المعلومات.[4]

7. جريمة تعتمد في تنفيذها على الحاسوب:

إذ يعد الحاسوب فيها أداة رئيسية لارتكاب العمل الإجرامي نظرا لما يحتويه من معلومات وأصول، فالحاسب الآلي هنا ليس مجرد وسيلة لتشغيل النتيجة الإجرامية أو مضاعفة جسامتها. بل يمكن القول ان

[1] نعيمة داودي، المرجع السابق، ص، ص 48 49.

[2] اسمهان بوضياف، المرجع السابق، ص ص 356 357.

[3] نهلا عبد القادر المومني، المرجع السابق، ص، ص 57 58.

[4] امحمد اقبلي وعابد العمراني الميلودي، المرجع السابق، ص 287.

المعلومات والبيانات التي يحتويها تشكل الباعث على ارتكاب الجريمة، كما هو الشأن في حالة التحويل غير المشروع من حساب بنكي لآخر، فاستخدم حاسوب متصلب وحده للاتصال يعد ضروري لتنفيذ هذا العمل الإجرامي.[1]

ثانيا: السمات الخاصة بالمجرم الإلكتروني:

- **المجرم الإلكتروني:** هو شخص يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة المعلوماتية[2].

لقد تنوعت الدراسات التي تحدد المجرم، وشخصيته ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة. فهناك سمات خاصة بالمجرمين ويمكن إجمال تلك السمات فيما يلي:

1. صغير السن:

حيث تتراوح أعمار مقترفي الجريمة الإلكترونية بين (18_46) سنة، والمتوسط العمري لهم(25) سنة وهذا مؤشر على أن المجرم الإلكتروني يكون من صغار السن لان كبار السن لم يألفوا التعامل مع الحاسب الآلي. كما ان حداثة الطفرة الإلكترونية الهائلة التي يشهدها العالم المعاصر كانت عاملا في بلورة هذه السمة[3].

2. المعرفة والذكاء:

تميز المعرفة مجرمي تكنولوجيا المعلومات حيث يستطيع مجرم التقنية أن يكون تصوراً كاملاً لجريمته، ويرجع ذلك إلى أن المسرح الذي تمارس فيه جريمة تكنولوجيا المعلومات هو نظام الحاسب الشامل. أما الوسيلة فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته، فمجرمو تكنولوجيا المعلومات يتميزون بالقدرة على الحصول على ما يحتاجون إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي[4].

---

[1] احمد اقبلي وعابد العمراني الميلودي، المرجع السابق، ص 287.

[2] إسراء جبريل رشاد مرعي، الجريمة الإلكترونية "الأهداف –الأسباب–طرق الجريمة ومعالجتها"، مجلة الدراسات الإعلامية، المركز الديمقراطي، العدد 1، 2018، ص 429.

[3] عادل يوسف عبد النبي الشكري، المرجع السابق، ص 117.

[4] سعد فهد الدبيس المطيري، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية، العدد 2، ص 1269.

يوصف الإجرام الإلكتروني بأنه إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم الإلكتروني إنسان على مستوى من الذكاء، إضافة إلى أنه مجرم متكيف اجتماعيا لا يناصب العداء للمجتمع[1].

3. السلطة:

يقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم في جريمة تكنولوجيا المعلومات والتي تمكنه من ارتكاب جريمته، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى نظام المعالجة الآلية، وقد تتمثل هذه السلطة في الحق في استعمال الجهاز الذي يحوي مزايا المعلومات الإلكتروني[2].

4. مجرم محترف:

لابد ان تتوفر لدى الجناة مرتكبي الجرائم المعلوماتية قدر من المعرفة المعلوماتية، ولكن هذه السمة ليست عامة ومطلقة وإنما تقتصر على الجرائم التي يستلزم ارتكاب التعامل مع الحاسب الالي ومعالجة المعلومات، للتغلب على العقبات التي اوجدها المختصون لحماية أنظمة الحاسوب كما في البنوك أو المفاعلات النووية والمؤسسات العسكرية[3].

5. مجرم متخصص:

له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته فب اختراق الشبكات كسر كلمات المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل غالٍ وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات[4].

6. مجرم يعود للإجرام:

يتميز المجرم الإلكتروني بأنه يعود للجريمة دائما فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهاراته في الاختراق[5].

---

[1] عادل يوسف عبد النبي الشكري، المرجع السابق، ص 117.

[2] سعد فهد الدبيس المطيري، المرجع السابق، ص 1269.

[3] عادل يوسف عبد النبي الشكري، المرجع السابق، ص 117.

[4] إسراء جبريل رشاد مرعي، المرجع السابق، ص 429.

[5] المرجع نفسه.

المطلب الثاني

أركان الجريمة الإلكترونية وأنواعها

تتخذ الجريمة المرتكبة عبر الأنترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، والمجرم يقوم بهذا الفعل، كما يمكن تصور الجريمة الإلكترونية من زاويتين بحسب اختلاف الزاوية التي ينظر منها إزالة الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي فمن ناحية قد يكون هذا الأخير نفسه موضوع الجريمة الإلكترونية، ومن ناحية أخرى قد يكون النظام المعلوماتي هو أداة الجريمة الإلكترونية و وسيلة تنفيذها.

بناءا على ذلك سنقوم في هذا المطلب بتبيان الأركان التي تقوم عليها الجريمة في (الفرع الأول)، ثم الحديث عن أنواعها في (الفرع الثاني).

الفرع الأول

أركان الجريمة الإلكترونية

إن أركان الجريمة عموما هي تلك العناصر التي لا يوجد للجريمة بدونها، وتتمثل الأركان العامة في الركن القانوني(الشرعي)، وهو النص الجزائي الذي يحوي النموذج القانوني للفعل أو الامتناع المجرم، ثم العناصر المكونة للركن المادي وأخيرا الركن المعنوي القائم على العلم والإرادة، أما الأركان الخاصة فهي ما يورده المشرع من عناصر في النص لقيام الجريمة بالإضافة إلى الأركان السابقة، وما يميز الجريمة الالكترونية عن غيرها من الجرائم أن وجود نظام المعالجة الآلية للمعطيات يعد بمثابة الشرط الأولي أو الركن الخاص الذي يجب تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام[1] وفيما يلي نفصل في مختلف الأركان التي تقوم عليها الجريمة الالكترونية.

أولا: الركن الشرعي

يقوم الركن الشرعي على النص التشريعي المجرم للسلوك والمحدد للعقوبة المقررة له تطبيقا لمبدأ شرعية الجرائم والعقوبات، لا جريمة ولا عقوبة إلا بناءا على نص تشريعي تضعه السلطة المختصة بالتشريع[2]، ولقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن

[1] عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجيستر في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012-2013، ص 62.

[2] عائشة بوخبزة، المرجع نفسه، ص 62.

قانون العقوبات وهو القسم السابع مكرر الذي يشتمل على تسعة مواد تهتم بذكر كل أنواع الاعتداءات على الأنظمة المعلوماتية[1].

إن الركن الشرعي للجريمة هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسيين:

- مطابقة الفعل لنص التجريم.
- ألا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة[2].

ثانيا: الركن المادي

تتخذ الجرائم الالكترونية عدة أشكال وذلك بتعدد وتنوع صور الاعتداء الواقع على نظام المعلوماتية بحد ذاته، ويمكن تلخيص هذه الصور كما يلي:

1. جريمة الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات:

يقصد بفعل الدخول ذلك الدخول المعنوي أو الإلكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي، ولا يعد فعل الدخول في حد ذاته سلوكا غير مشروع، وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص[3]، وهو ما أشار إليه المشرع الجزائري في المادة 394 مكرر من قانون العقوبات التي نصت على ما يلي: " يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة مالية من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...". أما فيما يخص فعل البقاء غير المشروع في نظام المعالجة الآلة للمعطيات فيقصد به استمرارية التواجد داخل النظام دون إذن من صاحبه أو من له حق السيطرة عليه، أي أنه بقاء شخص داخل نظام للمعالجة يكون ملكا للغير وذلك بعد الدخول إليه خطأ أو صدفة رغم علمه أن بقاءه فيه غير مرخص[4].

---

[1] المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات.

[2] بلعيات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص ص 94 95.

[3] حنان مهداوي، المرجع السابق، ص 1064.

[4] أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستر في القانون، كلية الحقوق، جامعة الجزائر، 2001، ص 44.

وبالرجوع إلى نص المادة 394 مكرر من قانون العقوبات يمكن القول أن المشرع الجزائري قد أورد ظرفين لتشديد عقوبة الدخول والبقاء دون ترخيص في نظام المعالجة الآلية للمعطيات، يتحقق الظرف الأول إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام، ويتحقق الظرف الثاني عندما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة و إعاقته عن أداء وظيفته، فالفقرة 2 من المادة 394 مكرر سالفة الذكر تنص على ما يلي: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب في نظام اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج.[1]

2. جرائم الاعتداء على المعطيات الموجودة داخل نظام المعلوماتية:

نص المشرع الجزائري على هذا النوع من الجرائم في المادتين 394 مكرر 1 و394 مكرر 2 من قانون العقوبات حيث جاء فيهما ما يلي:

المادة 394 مكرر1: " يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل نت أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال عدل بطريق الغش المعطيات التي يتضمنها".

المادة 394 مكرر2: "يعاقب بالحبس من شهر إلى 3 سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن يرتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

ويتضح من هاتين النصين أن جرائم الاعتداء على المعطيات الموجودة داخل نظام المعلوماتية تتخذ صورتين، الصورة الأولى هي جريمة التلاعب بالمعطيات والصورة الثانية هي جريمة التعامل في المعطيات. بالنسبة لجريمة التلاعب بالمعطيات فإنها تتحقق طبقا لما ورد في المادة 394 مكرر1 بارتكاب إحدى الصور الثلاث التالية:

– الإدخال بطريق الغش لمعطيات في نظام المعلوماتية.

– المحو بطريق الغش لمعطيات في نظام المعلوماتية.

[1] حنان مهداوي، المرجع السابق، ص 1065.

– التعديل بطريق الغش لمعطيات في نظام المعلوماتية.

أما بالنسبة لجريمة التعامل في معطيات غير مشروعة، فإنها تتحقق طبقا لما ورد في المادة 394 مكرر2 بارتكاب إحدى الصورتين التاليتين:

- **التعامل في معطيات صالحة لارتكاب جريمة:** يقصد بالتعامل كل سلوك يكشف عن وجود صلة معينة بين شخص ومعطيات غير مشروعة، هذه الصلة تتمثل في القيام بأحد أنواع السلوك، بدءا بتصميم هذه المعطيات والبحث في مضمونها وتجميعها وصولا إلى جعلها في متناول الغير، وتصل ليد الجاني وتكون تحت تصرفه ليرتكب بها جريمته وذلك بتوفيرها أو نشرها أو الإتجار فيها[1].
- **التعامل في معطيات متحصلة من جريمة:** يتحقق هذا السلوك المجرم بالقيام بأحد الأفعال التي نصت عليها المادة 394 مكرر2 وهي الحيازة، الإفشاء، النشر والاستعمال للمعطيات المتحصل عليها من جريمة الدخول أو البقاء بطريق الغش أو من جريمة التلاعب بالمعطيات.

ثالثا: الركن المعنوي

الركن المعنوي هو المسلك النفسي للجاني باعتباره محور القانون الجنائيين وذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية من علم وإرادة آثمة وقصد جرمي مع إفراز العقاب الذي يبنى على هذه المقومات، لذلك يمكن تعريف الركن المعنوي بأنه العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وهذه العلاقة يطبق عليها القانون والعقاب الذي يقرره[2]. يتكون هذا الركن من عنصرين هما العلم والإرادة. فالعلم هو إدراك الأمور على نحو مطابق للواقع يسبق الإرادة. أما الإرادة فهي اتجاه لتحقيق السلوك الإجرامي.

ويتخذ القصد الجنائي صورتين، القصد العام والقصد الخاص. فالقصد الجنائي العام هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة، أي لا يمتد بعدها. أما القصد الجنائي الخاص فهو ما يتطلب توافره في بعض الجرائم، فلا يكفي مجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك لأنه يبحث في نوايا المجرم[3]. أما فيما يتعلق بالجريمة المعلوماتية فإنها تعد من الجرائم العمدية أي تكفي لقيامها توفر القصد الجنائي العام المتمثل في علم الجنائي بعناصر الجريمة واتجاه إرادته إلى

[1] عائشة بوخبزة، المرجع السابق، ص 82.

[2] حسني نجيب محمود، النظرية العامة للقصد الجنائي، الطبعة السابعة، الإسكندرية، دار النهضة العربية، 1974، ص 90.

[3] حنان مهداوي، المرجع السابق، ص 1066.

إلحاق الضرر بالنفس أو المال أو البيانات المخزنة في الحاسوب[1]، ولكن هذا لا يمنع من القول ان هناك بعض الجرائم الإلكترونية تتطلب توفر القصد الجنائي الخاص مثلا جرائم تشويه السمعة عبر الأنترنت.

يرى الباحث 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 الإلكترونية وكجرائم مستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي لقيام الجريمة[2].

الفرع الثاني

أنواع الجريمة الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة، اختلف الفقه الجنائي حول تقسيم الجرائم الإلكترونية، حيث قد يكون النظام المعلوماتي هو نفسه موضوع أو محل الجريمة الإلكترونية ومن ناحية أخرى قد يكون النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها.

1. الجرائم الواقعة بواسطة النظام المعلوماتي:

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غي مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة.

أ. الجرائم الواقعة على الأشخاص:

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، حيث أن الهدف الأول والأسمى من وضع القوانين هو حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها سواء في أبدانهم كالقتل أو الجرح أو الضرب أو إعطاء مواد ضارة، كما يمارس بعضها على الجنين في رحم أمه كجريمة الإجهاض ومنها ما يمس عرض الإنسان وحياءه كالاغتصاب.[3]

أما فيما يتعلق بالجريمة الإلكترونية (المعلوماتية) فهناك العديد من الأفعال تدخل في نطاق هذا النوع من الجرائم والتي تستهدف الأشخاص في حياتهم وتشويه سمعتهم وكذلك التحريض عن القتل عبر الأنترنت

[1] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان، 2021، ص 91.

[2] اسمهان بوضياف، المرجع السابق، ص 355.

[3] محمود نجيب حسني، شرح قانون العقوبات (القسم الخاص)، الطبعة الأولى، دار النهضة العربية، مصر، 1988، ص317.

والتهديد والتحرش والمضايقة عبر وسائل الاتصال والملاحقة عبر وسائل تقنية وأنشطة اختلاس النظر والاطلاع على البيانات الشخصية.

- **جرائم القدف والسب:** عرف المشرع جريمة القذف في المادة 296 من قانون العقوبات الجزائري وعرف السب في المادة 297 من نفس القانون كما أن هذه المواد لم تشر إلى الوسيلة الإلكترونية لنشر ذلك الادعاء أو الإسناد.[1]

تعتبر جريمة القذف والسب من أكثر الجرائم شيوعا عبر شبكة الأنترنت حيث توجد هناك مواقع متخصصة تعمل على إبراز سلبيات الشخص المستهدف وإفشاء أسراره من أجل تشويه شرفه وسمعته.

وتعتبر شبكة الأنترنت مسرحا غير محدود لارتكاب تلك الجرائم، وتتم وجاهيا عبر خطوط الاتصال المباشر أو يكون كتابيا، وذلك عبر المبادلات الإلكترونية (بريد الكتروني، صفحات الويب غرف المحادثة).[2]

وهنا لابد من القول ان الجاني في مثل هذه الجرائم غالبا ما يستعمل البرامج التي تساعده على إخفاء هويته أثناء القيام بمثل هذه الأفعال عند إرسال البريد أو تصفح المواقع، الهدف من ذلك هو الخوف من تعرضهم للمساءلة القانونية أو الخجل من التصرفات الغير لائقة التي يقومون بها. وفي المادة 144 مكرر والمادة 146 من قانون العقوبات نجد أن القذف والسب الموجه لرئيس الجمهورية أو الهيئات سواء قضائية أو أمنية أو أي هيئة أخرى قد تكون بأية آلية لبث الصورة أو الصوت أو بأي وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

- **جرائم الاعتداء على حرمة الحياة الخاصة:** تعد فكرة الحياة الخاصة مسألة دقيقة جدا، وذلك لأنها تحكمها معايير المجتمع وعاداته وتقاليده. وعلى هذا فإن جريمة الاعتداء على حرمة الحياة الخاصة في مجال المعلوماتية هي كل اعتداء على البيانات الأسمية عبر الأنترنت وذلك عن طريق التمركز في موقع معين داخل شبكة الأنترنت والعمل على تسجيل وحفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية.[3]

[1] أنظر المادة 286 من قانون العقوبات الجزائري.

[2] عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات، الطبعة الأولى، دار الأوراق للطباعة والنشر والتوزيع، لبنان، 2004، ص312.

[3] برمش مراد، خصوصية الجريمة الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 1، 2020-2021، ص72.

– **جريمة التهديد:** وهي التي يتم من خلالها إرسال بعض الصور أو الكتابات على الشخص المراد تهديده او ابتزازه بغية حمله على القيام بفعل معين أو منعه من القيام به[1]، ويتم إرسال مثل هذه الكتابات إلى البريد الإلكتروني أو في وسائل الحوارات الآنية المختلفة على شبكة الأنترنت مثل الفايسبوك والواتساب... الخ.

– **انتحال شخصية الغير والاستدراج:** يتم ذلك من خلال استخدام الجرم الإلكتروني لشخصية الضحية أو المجني عليه بغرض الاستفادة من سمعته أو سلطته أو ماله أو غيره من الأسباب. فقد تتم بواسطة انتحال شخصية المجني عليه أو انتحال شخصية ما. ويكثر استخدام هذا النمط في الوسط التجاري. أما الاستدراج فغالب ضحاياه هم صغار السن، حيث يهومون من قبل المجرم الإلكتروني برغبته في تكوين صداقة عبر الشبكة تتحول إلى لقاء واقعي بينهما، وقد تتم الجريمة في إقليم الدولة الواحدة. وقد تكون مخترقة حدود الدولة أي أن المجرم الإلكتروني في دولة والضحية موجود في دولة أخرى.[2]

– **نشر الإباحة:** يقصد بنشر الإباحة كل إرسال أو نشر عمل إباحي أو بإعداد أو حفظ أو معالجة أو عرض أو نشر أو ترويج أنشطة أو أعمال إباحية أو اتصل بالدعارة. ويتم ذلك من خلال المواقع الإلكترونية الموجودة على الشبكة، والتي تستخدم بغرض الإثارة الجنسية من خلال قيام المجرم الإلكتروني بنشر صور جنسية فاضحة وأفلام جنسية، وكثيرا ما تستهدف الأطفال والشباب لأن هذه الفئة أقل تحصينا.

ب. الجرائم الواقعة على الأموال:

لقد صاحب ظهور شبكة الأنترنت تطورات كثيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما انجر عنه تطور وسائل الدفع والوفاء وأضحت جزء من هذه المعاملات، وفي خضم هذا التداول المالي عبر الأنترنت انتهز بعض المجرمين الفرصة من أجل السطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار السطو والسرقة، والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة. في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية وما أنجز عنه من تطور وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الأنترنت[3]، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها:

---

[1] لينا محمد الأسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار حامد، الأردن، دون سنة النشر، ص 45.

[2] نعيمة دوادي، الجريمة الإلكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها)، مجلة مهد اللغات، جامعة على لونيسي– البليدة (الجزائر)، المجلد 2، العدد 1، 2020، ص49.

[3] اسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، مسيلة، 2008، ص 358.

- **جريمة غسيل الأموال عبر الأنترنت:** من الجرائم المعاصرة تمارس عبر الأنترنت، حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل الأموال، بتوفير السرعة، وتفادي الدود الجغرافية، والقوانين المعيقة لغسيل الأموال، وكذا لتشفير عملياتهم وسهولة نقل الأموال واستثمارها لإعطائها الصبغة الشرعية.[1]

- **جريمة الإتلاف المعلوماتي:** الإتلاف هو تخريب الشيء محل الجريمة وذلك بإتلافه أو التقليل من قيمته مما جعله غير صالح للاستعمال أو تعطيله. وجريمة إتلاف المعلومات تتخذ إما صورة إجراء تعديلات غير مشروعة لها أو تدميرها أو الإدخال غير مشروع للمعلومات داخل أنظمة الحاسبات الآلية وهذا الجاني يكون على دراية وعلم بأن الأموال التي يتعدى عليها بالإتلاف ملك للغير وأن فعله من شأنه أن يتلف الشيء أو يجعله معطل أو يجعله غير صالح للاستعمال أو ينقص من قيمته.[2]

- **جريمة الاحتيال الإلكتروني:** الاحتيال المعلوماتي أو الغش المعلوماتي هي كل فعل أو مجموعة من الأفعال غير المشروعة والمعتمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شيء ذي قيمة ويكون نظام الحاسوب لازما لارتكابها أو إخفائها.

- وقد يسعى البعض إلى استغلال المعلومات للحصول على كسب مادي غير مشروع، من خلال الدخول إلى معطيات الحاسوب والتلاعب بها وتحويل الأموال إلى حسابه الخاص مما يسبب الضرر للآخرين.

- **تجارة المخدرات عبر الأنترنت:** تتعلق بالترويج للمخدرات وبيعها، والتحريض على استخدامها، وصناعتها بمختلف أنواعها.

ج. الجرائم الواقعة على أمن الدولة:

تقع هذه الجرائم باستعمال النظام المعلوماتي سواء لإفشاء الأسرار التي تخص مصالح الدولة ونظام الدفاع الوطني، أو الإرهاب، التجسس. نصت عليها المادة 394 مكرر2:" تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد.[3]

- **الإرهاب:** تعد جريمة الإرهاب من الجرائم البالغة الخطورة التي تواجه العالم بأسره، فهو يرتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجية، حيث أصبحت هذه الأخيرة أحد العوامل الاستراتيجية التي تمكن

[1] سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، جامعة جيلالي ليابس سيدي بلعباس الجزائر، العدد 1، 2018، ص 244.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، 2018، ص420.

[3] أنظر المادة 394 مكرر2 من الأمر 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

التنظيمات الإرهابية وأنصارها من أول استخدام الانترنت استخداما متزايدا في مجموعة واسعة ومتنوعة الأغراض تشمل التجنيد والتمويل، والدعية والتحريض على ارتكاب أعمال إرهابية.

– ويقوم الإرهابيون باستخدام الأنترنت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية، والاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر فيروسات، وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة والاستخدام والتي يمكن تحميلها مجانا.

– **التجسس:** يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية أو الدولية، وتستهدف خاصة التجسس العسكري، الساسي، والاقتصادي، وذلك باستخدام التقنية المعلوماتية، وتمارس من قبل دولة على دولة، أو من شركة على شركة ... وذلك بالاطلاع على المعلومات الخاصة المؤمنة في جهاز آلي، وغير مسموح بالاطلاع عليها، كأن تكون من قبيل أسرار الدولة.[1]

– **الجريمة المنظمة:** تعرف الجريمة المنظمة بأنها تعبير عن المجتمع الإجرامي يعمل خارج إطار الشعب والتعقيد والحكومة ويضم بين طياته آلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة، يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، فالجريمة المنظمة بسبب تقدم وسائل الاتصال والتكنولوجيا، أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان بل أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية.[2]

2. الجرائم الواقعة على النظام المعلوماتي:

إضافة إلى الجرائم المعلوماتية 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.[3]

وهذا ما سنتطرق إليه بشيء من التفصيل في النقاط التالية:

أ. الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الإتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، مما يترتب

[1] سورية ديش، المرجع السابق، ص 246.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 87.

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

عليها خسارة كبيرة، ولقد حدث هذا النوع من الجرائم في فرنسا، وأدى الى إتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية وقد قدرت الخسائر ب 5 ملايين فرنك فرنسي.[1]

ب.الاعتداء على برامج النظام المعلوماتي:

ويتوجب هنا معرفة ودراية ذات درجة عالية في مجال البرمجة، وتقع هذه الجرائم إما على البرامج التطبيقية أو برامج التشغيل.

– **البرامج التطبيقية:** وهنا يقوم الجاني بتحديد البرامج ثم التلاعب فيه للاستفادة منه ماديا، وذلك بتعديل البرنامج ويكون الهدف من تعديل البرامج اختلاس النقود، حتى ولو كان باستقطاع مبالغ قليلة لكن لفترات زمنية طويلة لتحقيق الفائدة، بدون إثارة الشبهات.[2]

– أما **التلاعب:** فيأخذ عدة أشكال، فقد يكون عن طريق زرع برنامج فرعي في البرنامج الأصلي مثلا يسمح له بالدخول غير المشروع في العناصر الضرورية للنظام المعلوماتي، حيث يصعب اكتشاف هذا البرامج لدقته وصغر حجمه.

– **برامج التشغيل:** وهي البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام، وتأخذ شكلين هما المصيدة وتصميم برنامج وهمي.

ج.الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

للمعلومة المعالجة آليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتية ولما لها من قيمة اقتصادية، وبهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها أو إتلافها أو حذفها أو تغييرها.[3]

– يكون **التلاعب** في المعلومات الموجودة على النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فيتم **التلاعب المباشر** عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم، الإبقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية، أو عن طريق تحويل لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك، وتسجيلها وإعادة ترحيلها وإرسالها لحساب آخر في بنك آخر، بهدف اختلاس الأموال.[4]

أما **التلاعب غير المباشر** فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين، أو التلاعب عن بعد بمعرفة أرقام وشفرات الحسابات، قصد التلاعب في الشرائط الممغنطة،

[1] المرجع نفسه، ص 359.

[2] سورية ديش، المرجع السابق، ص 246.

[3] اسمهان بوضياف، المرجع السابق، ص 360.

[4] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994، ص 82.

أو باستخدام الجاني كلمة السر أو مفتاح الشفرة، وإمكانية تسلل الجاني إلى المعلومات المخزنة والحصول على المنفعة المالية.[1]

- **إتلاف المعلومات:** في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحواسب وشبكاته، وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، ويكون الاتلاف العمدي للبرامج والبيانات كمحوها أو تدميرها إلكترونيا، أو تشويهها على نحو يجعلها غير صالحة للاستعمال[2].

[1] سورية ديش، المرجع السابق، ص ص247 248.

[2] سوية ديش، المرجع السابق، ص ص 247 248.

المبحث الثاني

ماهية الدليل الإلكتروني

إن ظهور أشكال مستحدثة من الجرائم المعلوماتية أدى بطبيعة الحال إلى ظهور أدلة مستحدثة وفي اثبات الجاني تختلف عن الأدلة التقليدية وتعرف بالدليل الإلكتروني وهذا الأخير هو كل دليل مأخوذ من جهاز الكمبيوتر محل الجريمة أو يكون في شكل بيانات وملفات مخزنة بداخله وقد يكون عبارة عن ملفات ناجمة عن اتصالات بين الجاني والمجني عليه من خلال مواقع الأنترنت، وهو ما يساعد القاضي على توضيح موقفه من القضية ومنها إصدار حكم آليات في القضية المعروضة أمامه.

وسنحاول من خلال هذه الجزئية من دراستنا التفصيل في ماهية الدليل الرقمي من خلال التطرق إلى مفهوم الدليل الإلكتروني (المطلب الأول)، ثم إلى نطاق الدليل الإلكتروني ونطاقه (المطلب الثاني).

المطلب الأول

مفهوم الدليل الإلكتروني

من المشكلات التي تتعلق بالدليل الإلكتروني أنه دليل غير مرئي، حيث تكون الأدلة الناتجة عن الناتجة عن الجرائم المرتكبة في الوسط الافتراضي عبارة عن بيانات غير مرئية لا تفصح في الغالب عن شخصية الجاني، وتكون مسجلة إلكترونيا، وفي الغالب مشفرة على وسائط تخرين ضوئية أو ممغنطة لا يمكن للإنسان قراءتها، وإن كان ذلك ممكنا للآلة، والتلاعب أو التعديل الذي يحدثه الجاني فيها لا يحدث أثرًا، مما يقطع صلة المجرم بالجريمة، ويحول دون كشف شخصيته في الغالب[1].

بناءا على ذلك سنقوم بتقسيم هذا المطلب بتعريف الدليل الإلكتروني في (الفرع الأول)، ثم التطرق إلى خصائص ومميزات الدليل الإلكتروني في (الفرع الثاني).

[1] وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقا للتشريع الجزائري، المجلة الجنائية القومية، كلية الحقوق، جامعة بجاية، المجلد 7، العدد 2، جويلية 2014، ص 69.

الفرع الأول

تعريف الدليل الإلكتروني

أولا: التعريف اللغوي

الدليل في اللغة هو المرشد وما يستدل به وجمعه أدلة، كما يقصد به كذلك تأكيد الحق بالبينة، والبينة هي الدليل أو الحجة أو البرهان[1].

وقد جاء في القرآن الكريم معنى الدليل بقوله تعالى: " ألم تر إلى ربك كيف مد الظل ولو شاء لجعله ساكنا ثم جعلنا الشمس عليه دليلا"[2].

بالنسبة لكلمة "الرقمي" فهي اسم منسوب للدليل وأصلها "رقم"، وهي علامات الأعداد المعروفة 1،2،3...، وينصب معناها أيضا إلى كلمة عدد، وجمعها أعداد.

وينتمي الدليل الرقمي إلى بيئة تتكون من نبضات إلكترونية يتم معالجتها، باستخدام لغات برمجة رقمية، فتقوم بتحويلها إلى أشكال متنوعة من المعلومات، تعرض في شكل نصوص وصور وجداول وغيرها، كما أنها تمكن المستخدم من اختيار إحدى اللغات الحية في تعامله مع الجهاز الرقمي، وتتنقل هذه الأشكال المبرمجة من خلال وسائل الاتصال الرقمي لشبكات النظم الرقمية[3].

ثانيا: التعريف القانوني

لم يتعرض المشرع الجزائري إلى تعريف الدليل الإلكتروني ونفس الشيء بالنسبة للمشرع الفرنسي، ولهذا سأقوم بعرض التعريفات التي أتى بها فقهاء القانون الجنائي.

فقد عرفه البعض بأنه هو الدليل المأخوذ من أجهزة الكمبيوتر في شكل موجات ونبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها بواسطة برامج تطبيقات وتكنولوجيات خاصة، وهي مكون رقمي لتقديم

[1] جميل صليبا، المعجم الفلسفي المصطلحات القانونية، الجزء الأول، دار الكتاب اللبناني، بيروت، الطبعة الأولى 1982، ص 564.

[2] الآية 45 من سورة الفرقان.

[3] أسامة حسين محي الدين عبد العال، حجية الدليل الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والاقتصادية، العدد 76، جوان 2021، ص 639.

معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الرسوم من أجل اعتماده أمام أجهزة تطبيق القانون[1].

كما يُعرّف بأنه الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة أو هو تلك المعلومات التي يقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة ما او المجني عليه[2]. كما يمكن تعريف الدليل الإلكتروني بأنه ذلك الدليل الذي يتضمن بيانات إلكترونية مخزنة بالحاسب الآلي ولها وجود في الوسط الافتراضي والتي من خلالها يتم الكشف عن الجريمة أو إثبات العلاقة بين حدوث الجريمة وفاعلها.

كما عرفه البعض بأنه يشمل جميع البيانات الرقمية التي يمكن أن تثبت بأن هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني، أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة[3].

ومن وجهة نظرنا فإن الدليل الرقمي Digital Evidence هو ذلك الدليل المشتق من النظم المعلوماتية، أو أجهزة ومعدات الكمبيوتر، أو شبكات الاتصالات، بعد تحليلها علميا وفنيا وتفسيرها في شكل نصوص مكتوبة، أو رسومات أو أصوات، لتقديمها لهيئات العدالة لإثبات وقوع الجريمة من عدمها.

المعلومات المخزنة أو المنتقلة في شكل ثنائي فيمكن أن تعتمد عليها المحكمة، وهو نفس التعريف المقدم من قبل الفريق العملي العامل على موضوع الأدلة الرقمية (SWGDE) باعتبار هذا الأخير أنشئ من أجل توحيد الجهود التي تقوم بها المنظمة الدولية لأدلة الحاسوب(IOCE)، وتطوير مختلف التخصصات والمبادئ التوجيهية من أجل استرداد، المحافظة، ودراسة الأدلة الرقمية بما فيها الصوتية والمصورة.

اتجهت كذلك بعض التعريفات إلى إضفاء صفة الدليل الإلكتروني على تلك الأدلة المستخلصة من الوسط الافتراضي، وبمفهوم المخالفة فإن تلك المعلومات التي لازالت لم يتم فصلها عن الحاسوب وهي شكل مجالات أو نبضات مغناطيسية أو كهربائية لا تصلح لأن توصف بالدليل الرقمي وهو قول غير دقيق، إضافة انها حصرت الدليل الإلكتروني على ذلك الذي يتم استخراجه من الحاسب الآلي، ولا شك أن ذلك فيه

[1] عيدة بلعابد، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق علمية، جامعة سعيدة، المجلد 11، العدد 1، 2019، ص 137.

[2] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015، ص ص123 124.

[3] وهيبة لعوارم، المرجع السابق، ص 70.

تضييق لدائرة الأدلة الرقمية، فهي كما يمكن أن تستخلص من الحاسب الآلي فمن الممكن أيضا الحصول عليها من أي وسيلة تقنية أخرى كالهواتف النقالة الذكية وآلات التصوير والبطاقات الذكية.

الفرع الثاني

خصائص الدليل الإلكتروني

إن دليل الإثبات في القانون ليس له أي طابع موحد أو نموذجي، وذلك يتصف الدليل عامة بطابع التنوع نظرا لما تتمتع به طبيعته من ضرورة توافقه من الواقعة الإجرامية وهي البيئة الافتراضية أو العالم الافتراضي، هذه البيئة ممثلة في أجهزة الحاسب الآلي بكل مكوناته المادية، المتمثلة في الأجهزة والمعدات والأدوات المادية Hardware، ومكوناته المعنوية المتمثلة أيضا في البرامج الحاسوبية Software، وعليه فهذه البيئة

الافتراضية قد انعكست على طبيعة هذا الدليل، فأصبح يتصف بعدة خصائص وهو ما سنتطرق إليه فيما يلي:

أولا: الخصائص المتعلقة بطبيعة الدليل الإلكتروني

1. الدليل الإلكتروني دليل علمي:

إن الطبيعة الخاصة بالدليل 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 إلكترونية، حيث إن العام 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 الالكتروني بهذه الخاصية بأنه دليل علمي، فاستخراج الدليل الرقمي يحتاج إلى بيئة مشابهة للبيئة التي نتج عنها، لذا يتطلب الاستعانة بأجهزة وأدوات التقنية واستخدام برامج حاسوبية ملائمة، للاطلاع عليه أو استخراجه في هيئة ملموسة أو مادية وهي تعد أساليب علمية[1].

2. الدليل الإلكتروني تقني:

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

يقصد بالتقنية العلم التطبيقي لوسائل وأدوات تم اختراعها من أجل تسهيل حياة الفرد والمجتمع[1]، وهي تقوم على أساس علمي، مثلها مثل الدليل الإلكتروني الذي هو كذلك دليل علمي، لذا يمكن استنتاج أن الدليل الإلكتروني يتميز بأنه دليل تقني، استنادا للمصدر الذي جاء منه وهو البيئة الرقمية أو التقنية، مثلما هو دليل علمي استنادا 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 لمأموري الضبط القضائي وسلطات التحقيق أن يبنوا عملهم على أساس الخبرة في التقنية، فلدى بعض الدول المتقدمة يكون لسلطات 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 يتحقق الفصل بين سلطة التحقيق والخبرة، حيث إن الخيرة تقوم بدور في التحقيق لمساعدة سلطة التحقيق لإثبات الجريمة والدليل التقني[3].

3. الدليل الإلكتروني دليل متنوع ومتطور:

مع توسع قاعدة الدليل الإلكتروني، يمكن لهذا الأخير أن يشمل أنواعا متعددة من المعلومات والبيانات الرقمية والتي بدورها تصلح أن تكون دليلا جنائيا بإدانة المتهم أو براءته، وأما ميزة التطور التي يختص بها الدليل الإلكتروني، فهي نتيجة تزايد استخدام تقنية المعلومات الرقمية، بعد أن أصبح كل من الحاسب الآلي

[1] حازم محمد حنيفي، الدليل الإلكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1988، ص 17.

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

[3] مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس 9، العدد 3، أكتوبر 2018، ص 198.

وشبكة الأنترنت يشكلان موطئا هاما للبيانات والمعلومات الرقمية، ومن وجهة أخرى نجد أن تطورها اليومي جاء لتلبية احتياجات المستخدمين الشيء الذي أدى إلى ظهور أنواع جديدة من هذه الأدلة[1].

4. الدليل الإلكتروني يصعب التخلص منه:

من أهم ما يميز الدليل الإلكتروني أنه يصعب إتلافه أو التخلص منه، ففي حالة محاولة إزالة ذلك فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوي ذلك الدليل، بل مجرد محاولة محو الدليل تعد في حد ذاتها دليل لأنه في حال القيام بعملية المحو يتم تسجيلها في ذاكرة الآلة ويتم استخراجها كدليل ضد من قام بالفعل، كما يمكن أيضا عرض الدليل الإلكتروني على تطبيقات وبرامج معروفة ما إذا كان قد تعرض للعبث أو التحريف[2].

5. الدليل الإلكتروني ذو طبيعة ثنائية:

تعتبر الطبيعة المزدوجة التي يختص بها الدليل الإلكتروني امتدادا للطبيعة العلمية والتقنية التي يتمتع بها، وأيضا امتدادا للبيئة الافتراضية التي تكون فيها كما سبق ذكره، لذا فالمعلومات والبيانات التي تشكل لنا دليلا جنائيا رقميا تكون في الأصل شكلاً ثنائياً أو رقمياً، ومردّ ذلك أن الحاسوب الآلي أو أي جهاز آخر له نفس خصائصه يقوم باستقبال هذه البيانات والمعلومات وتحويلها إلى أرقام ثم معالجتها[3].

فمضمون الطبيعة المزدوجة للدليل الإلكتروني هو اختزال البيانات أو المعلومات كالنصوص أو الصور أو الصوت أو أي معلومة أخرى إلى رموز ثنائية، وهذه الرموز الثنائية تتكون من سلسلة من رقم الصفر(0) ورقم واحد (1)، ومثال ذلك (أ) يقابله في البيئة الافتراضية (11000110)، وهكذا يتم من خلال طرق الترميز نقل وتمثيل البيانات المختلفة لتكون صالحة للتعامل معها داخل الحاسب الآلي وكذا الأجهزة الرقمية، بحيث أن لغة التعامل بين تلك الأجهزة هي النظام الثنائي الرقمي والتي تسمى في الأصل لغة الآلة[4]

ثانيا: الخصائص المتعلقة بمرونة الدليل الإلكتروني

1. دليل قابل للنسخ:

---

[1] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجيستر في العلوم القانونية، جامعة الحاج لخضر –باتنة، كلية الحقوق والعلوم السياسية، 2013، ص 124.

[2] أوشن حنان، وادي عماد الدين، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2015، ص ص 98 .99

[3] سليمان غازي، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، رسالة ماجيستر، جامعة نايف للعلوم الأمنية، السعودية، 2010، ص 25.

[4] أسامة حسين محي الدين عبد العال، المرجع السابق، ص 644.

يمكن استخراج نسخ من الأدلة الإلكترونية مطابقة للأصل ولها نفس القيمة العلمية وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق النسخ طبق الأصل من الدليل بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة[1].

2. دليل سهل الإخفاء:

إن التخلص من الدليل الإلكتروني قد يقابله مسألة أخرى ذات علاقة بمسألة التطوير المستمر في تكنولوجيا المعلومات، وهي أن الدليل الإلكتروني نتيجة لمرونته وضعفه، فإنه يسهل فقدانه أو إتلافه بالتالي يمكن التخلص منه بشكل آخر غير الحذف أو الإلغاء[2].

3. دليل متنوع ومتطور:

مع توسع قاعدة الدليل الإلكتروني، يمكن لهذا الأخير أن يشمل أنواعا متعددة من المعلومات والبيانات الإلكترونية والتي بدورها تصلح أن تكون دليلا جنائيا بإدانة المتهم أو براءته، وأما ميزة التطور التي يختص بها الدليل الإلكتروني، فهي نتيجة تزايد استخدام تقنية المعلومات الرقمية، بعد أن أصبح كل من الحاسب الآلي وشبكة الأنترنت يشكلان موطئا هاما للبيانات والمعلومات الرقمية، ومن وجهة أخرى نجد أن تطورها اليومي جاء لتلبية احتياجات المستخدمين الشيء الذي أدى إلى ظهور أنواع جديدة من هذه الأدلة[3].

المطلب الثاني:

تقسيمات الدليل الإلكتروني ونطاقه

الأدلة الجنائية هي كل ما يقود إلى برهان صحة الواقعة أو الوقائع موضوع التحقيق ويتم تصنيف الأدلة الجنائية إلى أربعة أنواع رئيسية هي: الأدلة القانونية تلك التي حددها المشرع وعين حالات استخدامها ومدى حجية كل منها، والأدلة الفنية تلك التي تنبعث من رأي الخبير الفني حول تقدير أو تقديم دليل مادي أو قولي وفق معايير ووسائل علمية معتمدة، والأدلة المادية الناتجة من عناصر مادية ناطقة بنفسها وتؤثر

[1] ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه مقدمة لنيل شهادة دكتوراه علوم في القانون، جامعة مولود معمري–تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، 23 جانفي 2019، ص 43.

[2] المرجع نفسه.

[3] نعيم سعيداني، المرجع السابق، ص 124.

في اقتناع القاضي بطريق مباشر، والأدلة القولية ويقصد بها تلك التي تنبعث من أشخاص أدركوا معلومات مفيدة للإثبات بإحدى حواسهم كالاعتراف وأقوال الشهود[1].

ويرى البعض أن الأدلة الجنائية الإلكترونية ماهي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان إلى الاستعانة بجميع ما يبتكره العلم من أجهزة مخبرية ووسائل التقنية العالية ومنها الكومبيوتر محور الأدلة الإلكترونية.

بناءا على ذلك سنقوم في هذا المطلب بدراسة تقسيمات الدليل الإلكتروني في الفرع الأول، ثم دراسة نطاق العمل به في الفرع الثاني.

الفرع الأول

تقسيمات الدليل الإلكتروني

تختلف الجريمة الإلكترونية عن الجريمة التقليدية في كون الأولى تتم في بيئة غير مادية عبر نظام حاسب آلي أو شبكة المعلومات الدولية –الأنترنت–حيث يمكن للجاني عن طريق نبضات إلكترونية رقمية لا ترى أن يعبث في بيانات الحاسوب أو برامجه وذلك في وقت قياسي قد يكون جزءا من الثانية، كما يمكن محوها في زمن قياسي قبل أن تصل يد العدالة إليه إذا ما استخدمت برامج خاصة في ذلك، مما يصعب الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوافر. إلا أن لهذا الأخير ميزة التنوع فلا يأتي على صورة واحدة بل يوجد له العديد من الصور والأشكال، وفي هذا الصدد نجد نوعين من التقسيمات للأدلة الإلكترونية بالإضافة إلى تقسيمات أخرى سنتطرق إليها فيما يلي:

أولا: التقسيمات الفقهية للدليل الإلكتروني.

لم يتطرق فقهاء القانون إلى دراسة الدليل الإلكتروني بشكل واسع، وهذا راجع إلى الحداثة النسبية لهذا الدليل من جهة، والتطور المتلاحق من جهة أخرى، ومن المحاولات الفقهية أنه تم تقسيم الدليل الإلكتروني إلى أربعة أقسام هي:

الأدلة الإلكترونية الخاصة بأجهزة الكمبيوتر وشبكاتها، الأدلة الإلكترونية الخاصة بالأنترنت، الأدلة الإلكترونية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، الأدلة الإلكترونية الخاصة بالشبكة العالمية للمعلومات.

وما يلاحظ على هذا التقسيم أنه يتطابق مع التقسيم الفقهي للجريمة عبر الكمبيوتر، على النحو التالي:

[1] وهيبة لعوارم، المرجع السابق، ص 74.

1. الأدلة الإلكترونية الرقمية المتعلقة بجهاز الكمبيوتر وشبكاته

وهي سلوك غير إنساني يشكل فعل غير مشروع على أجهزة الكومبيوتر، سواء وقع الأمر على المكونات المادية له أو المكونات المعنوية، أو قواعد البيانات الرئيسية، مثل تخريب مكونات الكمبيوتر كالطابعة[1].

2. الأدلة الإلكترونية الرقمية المتعلقة بالشبكة العالمية للمعلومات.

وهي سلوك إنساني يكون فعل غير مشروع قانونا يقع على أي وثيقة أو نص موجود بالشبكة مثل قرصنة المعلومات وسرقة أرقام بطاقات الائتمان، وانتهاك الملكية الفكرية للبرامج وغيرها فهذا النوع من الجرائم يتطلب اتصال بالأنترنت[2].

3. الأدلة الإلكترونية الرقمية المتعلقة بالأنترنت.

وهي سلوك إنساني يشكل فعل غير مشروع قانونا، يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات، مثل جرائم الدخول غير المشروع لمواقع يمنع الدخول إليها، واستخدام عناوين IP غير حقيقية للولوج إلى الشبكة العالمية للمعلومات وغيرها[3]

4. الأدلة الإلكترونية الرقمية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

تشمل هذه الأدلة الجرائم التي ترتكب عبر بروتوكولات الشبكة باستخدام الحاسوب، وتعتبر الأفعال المرتكبة ضمن هذا السياق جرائم قائمة بذاتها، بدون الحاجة إلى الاعتداء على معلومات محددة، وقد تستخدم هذه الوسائل الإجرامية لتسهيل جرائم أخرى مثل تهريب المخدرات أو غسيل الأموال دون وجود أثر مادي مباشر مما يعقد عملية الإثبات الإلكتروني.

ثانيا: التقسيمات التشريعية والقضائية للدليل الإلكتروني

[1] أسامة حسين محي الدين، المرجع السابق، ص 655.

[2] المرجع نفسه.

[3] نبيل عبد المنعم، جرائم الحاسب الآلي، بحث منشور، ندوة المواجهة الأمنية للجرائم المعلوماتية، دبي، مطبعة بن دسمال، عام 2005، ص 128.

برزت عدة تشريعات حول تقسيم الدليل الإلكتروني وإحاطة كل ما يتعلق به، وكان للقضاء أيضا دور في معالجة موضوع الدليل الإلكتروني وكذا العمل على إعطاء تقسيمات، إلا أن تشريع الولايات المتحدة الأمريكية كان من السباقين الذين تطرقوا للدليل الإلكتروني ولهذا ستكون كنموذج لدراستنا مع إبراز تقسيم المعتمد من قبلها لهذا الدليل، سواء كان هذا الأمر على مستوى التشريع أو القضاء.

فهي تعتبر ثاني دولة بعد السويد في إصدار قوانين خاصة بها تجرم هذا النوع المستحدث من الإجرام، ومن أهم هذه القوانين قانون تقرير الأشخاص الصادر في عام 1970، أيضا قانون الخصوصية الصادر في 31 ديسمبر 1986 وغيرها من القوانين.

ومنه سنبرز منة خلال ما يلي تقسيمات وزارة العدل الأمريكية للدليل الرقمي 2002 حيث تم تقسيمه إلى ثلاث مجموعات هي:

1. السجلات المحفوظة في الحاسوب:

عبارة عن بيانات يتم تخزينها إلكترونيا باستخدام الحاسوب، وتشمل جميع الحروف أو الأرقام أو الرموز أو الإشارات المثبتة بطريقة إلكترونية رقمية أو ضوئية أو بوسيلة أخرى تُظهر دلالتها بشكل يمكن التحقق منه. ومن أمثلتها البريد الإلكتروني، الذي يُعرف على أنه: "طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات"[1].

ففكرة البريد الإلكتروني تقوم على تبادل الرسائل الإلكترونية والملفات والرسوم والصور أو البرامج وغيرها، عن طريق إرسالها من المرسل إلى شخص أو أكثر وهذا باستعمال البريد الإلكتروني للمرسل إليه، عبارة عن صندوق تتواجد به كل الرسائل المرسلة على صاحب البريد والتي سبق له إرسالها والملغاة وغيرها من الأمور التي يحتوي عليها البريد الإلكتروني[2].

وهناك أيضا ملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الأنترنت.

2. السجلات المحفوظة جزئيا في الحاسوب:

يتم إنشاء هذا النوع من السجلات بواسطة الحاسوب، فهي تعتبر مخرجات برامج الحاسوب أي أنه لم يتم لمسها من قبل الأشخاص مثل files، log، وسجلات الهاتف، وكذا فواتير أجهزة السحب الآلي ATM.

3. السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب:

[1] محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، مصر، 2006، ص 272.

[2] أسامة حسين محي الدين عبد العال، المرجع السابق، ص 658.

ومن أمثلة هذا النوع من الأدلة الإلكترونية أوراق العمل المالية التي تحتوي على مدخلات يتم تحويلها إلى أوراق عمل مثل (EXCEL)، ثم تمت معالجتها بإجراء العمليات الحسابية.

وهذا التقسيم هو نفسه الذي أخذ به القضاء الأمر فسجلات الأمريكي، فسجلات الحاسوب المقبولة أمام القضاء الأمريكي، هي التي تكون في شكل نصوص وهذا إما في هيئة سجلات الحاسوب المتوالدة، أو سجلات الحاسوب المخزنة، والفرق بينهما يكمن فيما إذا كان الشخص هو المنشئ لمحتوى هذه السجلات أو الآلة، فسجلات الحاسوب المخزنة تشير إلى الوثائق التي تحتوي على كتابات شخص، أو بعض الأشخاص في شكل إلكتروني مثل: رسائل البريد الإلكتروني، أما فيما يخص سجلات الحاسوب المتوالدة فالكمبيوتر هو الذي يصدرها فهي تحتوي على مخرجات برامج الحاسوب مثل سجلات الدخول على الأنترنت ومصدرها مزود خدمة الأنترنت، بالإضافة إلى نوع ثالث من السجلات الذي يجمع بين التدخل الإنساني ومعالجة الكمبيوتر، مثلا كما لو أدخل متهم بيانات معينة ويطلب من الكمبيوتر معالجتها للوصول إلى نتائج يسمح بها البرنامج المستخدم كالشخص الذي يتهرب من الضرائب فيسجل بيانات غير صحيحة عن دخله وربحه طالبا من الكمبيوتر حساب الضريبة المستحقة[1].

إلا أن ما يؤخذ على هذه التقسيمات أنها ليست شاملة للدليل الإلكتروني، بل اقتصرت على نوع واحد، وهو سجلات الحاسوب المحتوية على نص بالرغم من أن الدليل الإلكتروني يشمل كافة البيانات الإلكترونية الممكن تداولها إلكترونيا، كالصور والأصوات والرسوم وغيرها فنجد حاليا بروتوكولات الاتصالات والتطبيقات المعلوماتية التي تستخدم في تحقيق الجرائم الإلكترونية ويعتبر نظام TCP/IP من أكثر البروتوكولات المستخدمة في شبكة الأنترنت، فهي جزء أساسي منه فهي تدل بصفة يقينية عن مصدر الجهاز الذي استخدم في الجريمة، كما تحدد الأجهزة التي أصابها الضرر من هذا الفعل الإجرامي.

ومنه نقول ان التقسيم الذي جاء به كل منة التشريع الأمريكي وكذا القضاء الأمريكي فيه جانب من الصحة، باعتبار أنه تحدث عن نوع مهم من الأدلة الإلكترونية والتي تعتبر أدلة قوية.

إلا أن هذا التقسيم ناقص ولا يشمل كل الأدلة الرقمية، حيث نستطيع القول إنه حصر تقسيمه في الأدلة الإلكترونية المكتوبة فقط في حين أن هناك أدلة أخرى فهو لم يخرج في تقسيمه هذا عن السجلات المتعلقة بالحاسوب فقط.

ثالثا: تقسيمات أخرى للدليل الإلكتروني

[1] عائشة بن قارة مصطفى، المرجع السابق، ص ص 74 75.

هناك تقسيمات فقهية أخرى للدليل الإلكتروني فقد أعطى الفقهاء احتمالات عديدة للدليل الإلكتروني، وهذا ما سنحاول إيضاحه من خلال ما يلي:

1. تقسيم الدليل الإلكتروني تبعا لمكوناته:

تنقسم إلى ما يلي:

أ. الأشرطة المغناطيسية:

وهذا الشريط هو عبارة عن شريط بلاستيكي مغطى بمادة قابلة للمغنطة، قد يكون ملفوفا على بكرة مثل التي تستخدم في أجهزة التسجيل الصوتي، وقد يكون داخل علبة على هيئة شريط فيديو مثلا، وكل الأشرطة الممغنطة بها رأس للقراءة والكتابة ويسجل البيانات على شكل نقطة مغناطيسية على الشريط بشفرة خاصة تدل على البيانات المستخرجة من داخل الحاسوب، كما يستطيع هذا الرأس من الإحساس بوجود هذه النقطة ويقوم بإرسال النبضات الكهربائية المقابلة لشفرة البيانات داخل الحاسوب، والشريط المغناطيسي يستخدم في تخزين البرامج والملفات المتتالية أي اللازمة لقراءة البيانات فيها قراءة الشريط من بدايته وتنظم المعلومات فيه على شكل وحدات خاصة، تسمى كل وحدة منها حزمة وحجم الحزمة يحدده مستخدم الجهاز، لذا تعامل الحزمة كوحدة متكاملة، وذلك عند تخزينها أو إخراجها من الشريط[1].

ب. الأقراص المغناطيسية:

تعتبر الأقراص المغناطيسية من أفضل وسائط الخزن، حيث يمكن استخدامها للتخزين المباشر أو العشوائي، وذلك لقدرتها الاستيعابية العالية، ومن أهم خواصها هي إمكانية القراءة أو التسجيل على قطاع من السطوح وكذلك يمكن تغيير أو تعديل أي ملف عليها دون الحاجة إلى إنشاء ملف جديد إذ يتم تعديل السجل وهو في موضعه، وهناك عدة أنواع نذكر منها: القرص المرن، القرص الصلب، قرص الخرطوش أو قرص الكارت ريدج، المصغرات الفيلمية[2].

2. تقسيم الأدلة الرقمية بحسب مكان وجودها:

تنقسم إلى ما يلي:

- **أدلة ورقية:** مثل مخرجات الحاسوب والتقارير والرسوم البيانية.
- **أجهزة الحسابات:** وهي التي تحتوي على ملحقات الحاسوب من شاشات وغير ذلك.

[1] أسامة حسين محي الدين عبد العال، المرجع السابق، ص 661.

[2] أسامة محي الدين عبد العال، المرجع السابق، 661.

- **الأقراص المونة والصلبة:** تعتبر من أهم الأدلة لاحتوائها على بيانات وكلمات مرور وصور وتقارير وخطط ارتكاب الجريمة وغيرها.

- **أشرطة تخزين المعلومات:** تستخدم لحفظ النسخ الاحتياطية.

- **القطع الإلكترونية:** مثالها أجهزة الإرسال التي يجب أن تفحص للتأكد من طبيعتها خاصة في قضايا التجسس.

- **أجهزة المودم:** والتي تستخدم في نقل المعلومات ويمتاز بعضها بإمكانية أن يعمل كجهاز الرد على رسائل الهاتف، ويجب تسجيل الكابلات المتصلة به عند ضبطه.

- **البرامج:** وهي التي تمثل الأدوات الرئيسية التي يستغلها المجرم في ارتكاب جريمة نظم المعلومات.

- **الطابعات والأجهزة الخاصة:** بتصوير المستندات وما قد تحتويه من أوراق مطبوعة ومصورة أو ما هو مخزن في ذاكرتها من معلومات.

يمكن القول ان هذه التقسيمات قد ألمت بجانب كبير ومهم منة الأدلة الإلكترونية التي تعتبر من الأدلة القاطعة، ففي تقسيم الدليل الرقمي لابد من الأخذ في عين الاعتبار التطور المستمر الذي يطرأ على هذا النوع من الأدلة من جهة، وعلى البيئة الافتراضية من جهة أخرى، فهي أدلة متطورة بطبيعتها، كما تتطور وسائل الحصول عليها والتي يجب مراعاتها قانونيا حتى يكون من الإمكان الاعتماد عليها كدليل إثبات في مختلف القضايا.

الفرع الثاني

نطاق الدليل الإلكتروني

إن البحث في مجال الدليل الإلكتروني يضع الباحث أمام عدد كبير من التساؤلات المتعلقة بهذا الدليل. خاصة عندما تتداخل الأساليب مع المعايير المستخدمة في رصده. وتكمن الصعوبة في كيفية التعامل مع الدليل الإلكتروني، خصوصا إذا أخذنا في الاعتبار أن مصطلح "الدليل الرقمي" يحمل دلالة مختلفة عن تلك التي يتمتع بها الدليل المادي، الذي يعتمد على الطرق التقليدية المعروفة في القانون للحصول على ما يثبت الإدانة أو يضمن حقوق العدالة بشكل عام، سواء كان ذلك حق المجتمع في الإدانة أو حق الفرد في إثبات براءته، في المقابل فإن استخدم الدليل الرقمي يثير تساؤلات حول قيمته كدليل يتماشى مع المفاهيم القانونية للأدلة. رافق التطور التكنولوجي السريع وزيادة استخدام الحواسيب بشكل ملحوظ، ظهور الإنترنت الذي أدى إلى ارتفاع عدد الجرائم المرتكبة باستخدام هذه الوسائل. ونظرا لإن الدليل الرقمي يعتبر الأكثر فعالية في إثبات هذا النوع من الجرائم، نظرا لطبيعة البيئة التي حدثت فيها، فإن الاهتمام المتزايد بهذا

الدليل يعود إلى انتشار التقليدية. من المهم أن نوضح أن الدليل الإلكتروني لا يقتصر على إثبات الجرائم الإلكترونية فحسب، بل يعتبر أيضا من أفضل الأدلة لإثباتها. بالإضافة إلى ذلك، يمكن استخدامه لإثبات الجرائم التقليدية[1].

وفي هذا السياق، يميز الفقه في الشأن بين عدة أنواع من الجرائم:

أولا: الجرائم المرتكبة بواسطة الكمبيوتر

هي الجرائم التي يستخدم فيها الكمبيوتر والإنترنت كوسيلة مساعدة لارتكاب الجريمة، مثل استخدامه في الغش والاحتيال وهذا النوع من الجرائم لا صلة له بالوسط الافتراضي إلا من حيث الوسيلة، فبالرغم من عدم اتصال هذه الجريمة بالنظام المعلوماتي إلا أن الدليل الرقمي يصلح كدليل لإثباتها، فلا يعتبر استخدام الكمبيوتر في هذه الجرائم من طبيعة الفعل الجرمي، بل تستخدم كوسيلة مساعدة لارتكاب الجريمة مثل عمليات غسل الأموال أو نقل المخدرات من مكان إلى آخر، إلا جهاز الكمبيوتر في هذه الحالة يظل محتفظا بآثار رقمية يمكن أن تستخدم للإرشاد عن الفاعل[2].

ثانيا: جرائم الأنترنت Cyber crime

هي الجرائم التي لا يكون محلها جهاز الكمبيوتر فإما أن يكون الاعتداء واقعا على الكيان المادي له، ويمكن اعتبارها في هذه الحالة جريمة تقليدية تلحق سابقتها في الإرشاد عن الفاعل، وإما أن يكون واقعا على الكيان المعنوي له أو على قاعدة المعلومات الرقمية، مثال جرائم القرصنة وهذا النوع من الجرائم هو الجرائم المعلوماتية والتي يكون الدليل الرقمي هو الأفضل لإثبات وجودها، عرفها البعض بأنها سلوك إنساني يشكل فعلا غير مشروع قانونا، تقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات ومن أمثلة هذه الجرائم جرائم الدخول غير المشروع لمواقع غير مصرح بها للدخول بها واستخدام عناوين غير حقيقية أو زائفة للولوج إلى الشبكة العالمية للمعلومات، تقنية الحماية الخاصة بالجهات المتصلة بالشبكة.

لكن يرى البعض أنه يمكن للدليل التقليدي إثبات الجريمة المعلوماتية كالشهادة رغم شدة صلتها بالدليل الإلكتروني، فلا تلازم إذن بين نطاق الدليل الإلكتروني وإثبات الجريمة المعلوماتية، بل إن الدليل الإلكتروني كما يصلح لإثبات الجريمة التقليدية المرتكبة باستعمال الآلة الرقمية يصلح لإثبات الجريمة الإلكترونية.

ثالثا: جرائم الشبكة العالمية

[1] كرام غانم بستان، نطاق الدليل الإلكتروني في الإثبات الجنائي، مجلة الجامعة العراقية، العدد 04، فيفري 2025، ص 292.

[2] وهيبة لعوارم، المرجع السابق، ص 75.

وهي أي سلوك إنساني يكون فعلا غير مشروع قانونا ويقع على أي وثيقة أو نص موجود بالشبكة، أو أنها أية جريمة يكون فيها لشبكة المعلوماتية دور في أسلوب ارتكابها أو التوقيع على إحدى وثائقها بأية طريقة كانت.

ومن أمثلتها قرصنة المعلومات وسرقة أرقام بطاقات الائتمان، وانتهاك الملكية الفكرية للبرامج والأفلام وغيرها، فهذه الجرائم تتطلب اتصالاً بالأنترنت على عكس جرائم الكمبيوتر التي قد يتصور حدوثها سواء كان هناك اتصال بالأنترنت أو لا.

رابعا: جرائم الكمبيوتر

وهي سلوك إنساني يشكل فعلا غير مشروع قانونا ويقع على أجهزة الكمبيوتر سواء وقع هذا السلوك غير المشروع على المكونات المادية أو المكونات المعنوية أو قواعد البيانات الرئيسية.

ولم يتوفر تعريف جامع يتفق عليه بسبب المتغيرات المتسارعة في مجال تقنية الكمبيوتر وتعدد أنماط الجرائم، ولكن يمكن أن نستعمل هذا المصطلح للدلالة على الجرائم الموصوفة في القوانين الحديثة لمكافحة جرائم الحاسوب أو الكمبيوتر، وهي تلك الجرائم التي تشمل سرقة خدمات الكمبيوتر، والدخول غير المشروع في نظم الحاسوب المحمية، وقرصنة البرامج وتعديل أو سرقة المعلومات المخزنة إلكترونياً، والابتزاز بواسطة الكمبيوتر، والحصول على دخول غير مصرح على سجلات البنوك أو إصدار بطاقات الائتمان أو وكلاء العملاء، والاتجار في كلمة السر، وبث الفيروسات والأوامر الهدامة، والتخريب لمكونات الكمبيوتر المادية كالشاشات أو الطابعة أو وسائط التخزين المرنة أو الصلبة، وكذلك الفيروسات وتعديل أو محو البيانات الرئيسية وغيرها[1].

أصدر المشرع الجزائري قانوناً متخصصا يعالج جرائم التكنولوجيا بما فيها التكنولوجيا الرقمية وهو قانون09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2]، وعرف تلك الجرائم أي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة الثانية منه الفقرة (أ) بأنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".

[1] عائشة بن قارة، المرجع السابق، ص 72.

[2] أنظر الى قانون 09-04.

خلاصة الفصل الأول:

ومن هنا نستخلص أن هذا الفصل يهدف إلى بناء إطار نظري لفهم موضوع الإثبات في الجرائم الإلكترونية، حيث تناولنا في البداية ماهية الجريمة الإلكترونية باعتبارها نمطا جديدا من الجرائم، يختلف عن الجرائم التقليدية من حيث الوسائل والمجال الذي تقع فيه، وهو الفضاء الرقمي.

كما تطرقنا إلى الخصائص التي تميز هذا النوع من الجرائم والصعوبات التي تطرحها على مستوى التجريم والإثبات. أما في الجانب الثاني من الفصل، فقد سلطنا الضوء على الدليل الإلكتروني من حيث طبيعته القانونية، وخصائصه التقنية، وتقسيماته الإلكترونية.

الفصل الثاني:
الإطار القانوني للإثبات في الجريمة الإلكترونية

الإثبات في الجريمة الإلكترونية هو عملية تقديم الأدلة القانونية لإثبات وقوع جريمة ارتكبت باستخدام وسائل إلكترونية أو عبر الإنترنت مثل الحواسيب أو الهواتف الذكية أو الشبكات.

يعتبر الإثبات الجنائي الأساس الذي يحقق براءة المتهم أو إدانته، كما يعد من أهم المواضيع الإجراءات الجنائية ذلك أن هدف هذه الأخيرة هو إظهار الحقيقة كما وقعت، وبالنسبة للإثبات الجنائي فهدفه هو إقامة الدليل من أجل الكشف عن الحقيقة التي وقعت بشأن الجرائم التي ارتكبت، وذلك بغية تحقيق العدالة المرجوة وهذا عن طريق الاستعانة بكافة وسائل الإثبات ومنح القاضي الحرية في تقدير الأدلة المطروحة عليه، عملا بمبدأ الاقتناع القضائي القائم على حرية الإثبات، على عكس الإثبات في المواد المدنية الذي يقوم على نظام الأدلة القانونية أو بمصطلح أحر مبدأ الإثبات المقيد.

بالرغم من الجهود المبذولة في مكافحة الجريمة الإلكترونية والدور البارز الذي يلعبه الدليل الرقمي في الإثبات، إلا أن الواقع العملي والقانوني كشف عن الكثير من الصعوبات التي تثيرها عملية الإثبات بتلك الأدلة الرقمية الحديثة.

وعليه سنتطرق في هذا الفصل إلى:

- **المبحث الأول: التحقيق في الجريمة الإلكترونية وإجراءات جمع الأدلة.**
- **المبحث الثاني: حجية الأدلة الإلكترونية في الوقائع المراد إثباتها.**

المبحث الأول

التحقيق في الجريمة الإلكترونية وإجراءات جمع الأدلة

إن طبيعة الجريمة الالكترونية من حيث عناصرها ووسائل ارتكابها قد يدفع المشرع الجزائي إلى إعادة النظر في العديد من الجوانب الإجرائية، لاسيما فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون لأن مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للأفراد.

وبما أن إثبات هذا النوع من الجرائم يتطلب دليلا ذات طبيعة تقنية تتماشي مع طبيعة الجريمة الالكترونية فان القواعد الإجرائية التقليدية لا تكون كافية لاستخلاص هذا الدليل، وهو ما استدعى المشرع لوضع قواعد إجرائية خاصة تمكن الجهات المختصة بالبحث والتحري والاعتماد عليها للوصول إلى الأدلة المناسبة لإثبات هذه الجريمة.

وعليه سيكون محل دراستنا في هذا المبحث إلى إجراءات التحقيق في الجريمة الالكترونية (المطلب الأول)، ثم إلى إجراءات الحصول على الأدلة في الجريمة الالكترونية (المطلب الثاني).

المطلب الأول

إجراءات التحقيق في الجريمة الإلكترونية

تعتبر مرحلة جمع المعلومات والمعطيات من أهم مراحل الدعوى الجزائية التي تسبق المحاكمة فمن خلالها يتم التعرف على من ارتكب الفعل وهذا ما يعرف بالتحقيق، فهو مجموعة الإجراءات التي تتخذ بعد وقوع الجريمة قصد التنقيب والكشف عن الأدلة في شان الجريمة التي ارتكبت ثم مدى كفايتها لإحالة المتهم للمحاكمة [1] ويمكن تعريفه أيضا بأنه الإجراءات التي يقوم بها مأموري الضبط القضائي عبر العالم الافتراضي لضبط الجريمة الإلكترونية والتثبت من أدلتها ومعرفة فاعلها تمهيدا لإحالتهم إلى المحكمة.[2]

وعليه سنتطرق في هذا المطلب إلى الأجهزة المكلفة بالبحث والتحري (الفرع الأول) وخصائص التحقيق والمحقق (الفرع الثاني).

[1] فلاح عبد القادر، أيت عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2019 ص1 1694.

[2] محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها، دراسة مقارنة رسالة دكتوراه كلية الحقوق، جامعة المنصورة 2005، ص 234.

الفرع الأول

الأجهزة المكلفة بالبحث والتحري في الجريمة الإلكترونية

نظرا للخصوصية التي تتميز بها الجريمة الإلكترونية كان الأمر لازما لتوفير أجهزة مختصة تقوم بعملية البحث والتحري على الجريمة الإلكترونية، إما على مستوى جهاز الضبطية القضائية أو على مستوى مركز الوقاية من جرائم الإعلام الآلي.

أولا: الضبطية القضائية

تعد الضبطية القضائية الجهة ذات الاختصاص العام في مجال البحث و التحري عن الجرائم نظرا لقدرتها العالية على كشف الجرائم التي تقع ضمن نطاق اختصاصها، وتعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في كل الجرائم بما فيها الجريمة الإلكترونية [1] وهدا حسب ما ورد في المادة 12 من قانون الإجراءات الجزائية، ومن اجل إشراك مزودي خدمات الإنترنت و الاتصالات الثابتة ، و المتنقلة في محاربة الجرائم الإلكترونية يلزم القانون 9-4 هؤلاء بتقييم المساعدة للسلطات المختصة في مجال جمع و تسجيل المعطيات المتعلقة بهذه الجرائم [2].

1. على مستوى جهاز الشرطة:

أنشأت المديرية العامة للأمن الوطني مخبر مركزي بمركز الشرطة بشوطانوف بالجزائر العامة ومخبرين جهويين بكل من قسنطينة ووهران تحتوي على فروع تقنية، من بينها خلية الإعلام وفرق مختصة مهمتها التحقيق والكشف على جرائم الإنترنت.

---

[1] أحمد بوزينة آمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم، مداخلة مشارك بها في الملتقى الوطني حول آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، 2007، ص 570.

[2] عزا الدين عثماني، إجراءات التفتيش والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، جامعة تبسه العدد 4، جانفي 2018، ص 52.

بالإضافة إلى إنشائها ثلاث مخابر على مستوى بشار ورقلة وتمنراست قيد الانجاز لأجل تعميم هذا النشاط على كافة ربوع الوطن، كما يضم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الإلكترونية[1] تحت اسم دائرة الأدلة الرقمية والآثار التكنولوجية والتي تضم ثلاث أقسام وهي:

- قسم استغلال الرقمية الناتجة عن الحواسيب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية.[2]

2. على مستوى جهاز الدرك الوطني:

يعمل جهاز الدرك الوطني على مكافحة الجريمة الإلكترونية، بواسطة المعهد الوطني للأدلة الجنائية وعلم الإجرام الكائن مقره بشاوي التابع لقيادة الدرك العام، قسم الإعلام والإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الإلكترونية، وأيضا بواسطة مديرية الأمن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية وهي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الإلكترونية[3].

3. اختصاص الضبطية القضائية:

إن أعضاء الضبطية القضائية وهم يمارسون صلاحياتهم في إجراء التحريات اللازمة بشأن الجريمة لمعرفة مرتكبيها، مقيدين في دالك بنطاق إقليمي يسمى بالاختصاص المحلي وبنوع معين من الجرائم يسمى الاختصاص النوعي.

أ. الاختصاص المحلي:

يقصد به المجال الإقليمي الذي يباشر فيه ضباط الشرطة القضائية مهامهم في البحث والتحري عن الجريمة، ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة ولذلك يتعين أن يكون مكان وقوع الجريمة أو محل إقامة المتهم محل القبض عليه. ويجيز القانون تمديد الاختصاص المحلي لضباط الشرطة القضائية في حالة الاستعجال، أو بناءا على طلب من السلطة القضائية، وهو ما نصت عليه المادة

[1] فلاح عبد القادر، أيت عبد المالك نادية، المرجع السابق، ص 1696.

[2] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة دكتوراه في الحقوق والعلوم السياسية، جامعة باتنة، سنة 2016، ص 177.

[3] فلاح عبد القادر، أيت عبد المالك نادية، المرجع السابق، ص 1969.

02/16 من قانون الإجراءات الجزائية وكذا تحديد الاختصاص المحلي لضباط الشرطة القضائية في الجرائم (06) الستة الخطيرة إلى كافة التراب الوطني[1].

ب.الاختصاص النوعي:

يقصد به اختصاص عضو الضبطية القضائية بنوع معين من الجرائم دون غيرها من الجرائم و قد ميز المشرع بين الاختصاص العام لبعض الفئات أعضاء الضبطية القضائية أي الاختصاص بالبحث و التحري بشان جميع الجرائم، دون تحديد نوع معين من الجرائم دون الأنواع الأخرى و هي الفئات المنصوص عليها في المادة 15 من قانون الإجراءات الجزائية فلهم الاختصاص العام بالبحث و التحري في جميع الجرائم أما الفئات الأخرى من الضباط المحددين في الفقرة 7 من المادة 15 و المواد 21 27 28 من قانون الإجراءات الجزائية فإنهم ذو اختصاص خاص و ليس عام يتحدد بنطاق جرائم معينة.[2]

ثانيا: مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية عن طريق المرسوم الرئاسي رقم 15-261 ومقره بئر مراد رايس وهو تابع لمديرية الأمن للدرك الوطني، وقد حددت المادة الأولى منه تشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وتمارس هذه الهيئة العديد من المهام في مجال التصدي للجريمة الإلكترونية وورد النص عليها في المادة 14 من القانون 9-4 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهي:

- ضمان المراقبة المستمرة لشبكة الإنترنت.
- القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني.
- المشاركة في عمليات البحث والتحري عن الجرائم الإلكترونية.
- إدارة وتنسيق العمليات الوقائية من الجرائم الالكترونية[3].

الفرع الثاني

خصائص التحقيق والمحقق في الجريمة الإلكترونية

إن التحقيق في الجريمة الالكترونية يختلف عن التحقيق في الجريمة التقليدية ببعض المميزات الخاصة وكدا المحقق الجنائي وهذا نظرا للطبيعة التقنية التي تتمتع بها هذه الجرائم.

---

[1] أنظر المادة 16 من الأمر 155/66، من قانون الإجراءات الجزائية، في 8 يونيو 1966، يعدل ويتمم القانون 22/06 في 20 ديسمبر2006، الجريدة الرسمية، عدد 84 بتاريخ 24/ 12/ 2006.

[2] المرجع نفسه.

[3] فلاح عبد القادر، أيت عبد المالك نادية، المرجع السابق، ص 1696

أولا: خصائص التحقيق في الجريمة الإلكترونية

إن التحقيق الجنائي هو علم ينطوي تحت لواء العلوم الأخرى، فهو له قواعد ثابتة راسخة تحدد منهجيته سواء من حيث القواعد القانونية أو الفنية أو العلمية، وتكمن أهمية هده القواعد في تعزيز مصداقية الإثبات القانوني. ويعد التحقيق الجنائي نشاطا يتطلب مهارات عالية تتجاوز مجرد إتباع الإجراءات الشكلية، إذ يعتمد بدرجة كبيرة على قدرة المحقق في التحليل والاستنتاج. إضافة إلى توفره على رصيد من التجربة و المعرفة كما أن نجاح التحقيق في الجرائم المعقدة، و على وجه الخصوص الجرائم ذات الطابع ألمعلوماتي يستوجب تجديد الفكر التحقيق و تطوير آلياته، حيث لم تعد الأساليب التقليدية كافية ومن هنا برزت أهمية تفكير المحقق بأساليب مرنة تتماشي مع الطبيعة المتجددة لأساليب الجريمة الإلكترونية.

1. أسلوب التحقيق الابتدائي في الجريمة الإلكترونية:

التحقيق مجموعة إجراءات يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة، ومعرفة مرتكبها تمهيدا لتقديمهم إلى المحاكمة وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كالبصمات الرقمية، أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام الإلكتروني.

والهدف من التحقيق الابتدائي:

- التأكد أولا من وقوع الجريمة يعاقب عليها القانون.
- معرفة نوع هذه الجريمة.
- معرفة الجاني والمجني عليه.
- معرفة الوسائل التي استعملت في ارتكابها.

ويكون ذلك في الجريمة الإلكترونية وفقا لمنهج تحقيق يختلف عن غيره بالنسبة للجرائم الأخرى[1].

أ. تشكيل فريق التحقيق:

التحقيق الابتدائي في الجرائم الإلكترونية يكون غالبا من ان يتولاه شخص واحد بمفرده، حتى لو كانت المضبوطات هي مجرد حاسب شخص واحد ولذلك فانه يفضل أن يقوم بتعاون عدة محققين في القيام بمهمة التحقيق والعثور على دليل[2].

[1] نعيم سعيداني، المرجع السابق، ص 110.

[2] عبد الله حسين محمد، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 26-28 أفريل 2003 ص 612.

ويكون تشكيل فريق التحقيق من فنيين وأخصائيين دوي الخبرة في مجال الأنترنت، والحاسوب ويتميزون بمهارات التحقيق الجنائي بشكل عام والتحقيق الإلكتروني بشكل خاص ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة.

وبذلك يكون تشكيل فريق خاص بالتحقيق في هدا النوع من الجرائم، أمرا ضروريا ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم الإلكترونية من:

- المحقق الرئيسي ويكون ممن لهم الخبرة في التحقيق الجنائي.
- خبراء الأنترنت والحاسوب الدين لديهم الخبرة وكيفية التعامل مع هده الجرائم.
- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الدين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي[1].

2. الأسس الإجرائية المعتمدة في التحقيق الابتدائي للجريمة الإلكترونية:

يقصد بها تلك الإجراءات التي تقوم بها جهات التحقيق خلال تنفيذ أساليب التحري، والتي تهدف لإثبات وقوع الجريمة وتحديد هوية مرتكبها وتوجد إجراءات، وتدابير معينة من اختصاص الضبطية القضائية يجب القيام بها قبل البدء وأثناء مباشرتها في التحقيق الابتدائي.

ب. الإجراءات الواجب اتخاذها قبل الشروع في التحقيق:

- القيام بتحديد نوع نظام المعالجة للمعطيات هل هو كمبيوتر معزول أو متصل بشبكة معلومات.
- القيام بوضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.
- يجب حصر طرفيات الاتصال إذا وقعت الجريمة على شبكة لمعرفة الطريقة التي تمت بها عملية الاختراق.
- مراعاة صعوبة بقاء الدليل لفترة طويلة في الجريمة الإلكترونية.
- فصل التيار الكهربائي عن مواقع المعاينة أو جمع الاستدلالات.
- فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها والتحفظ على الهواتف المحمولة من قبل الآخرين الدين لا تربطهم علاقة لأنهم قد يسيئون استخدامها لطمس البيانات.
- القيام بالتأكد من أن خط الهاتف يخص الحاسوب محل الجريمة.

[1] عبد الله حسين محمد، المرجع السابق، ص 613.

– القيام بتصوير الأجهزة المستخدمة من الأمام والخلف لإثبات بأنها كانت تعمل[1].

ب–الإجراءات الواجب اتخاذها أثناء الشروع في التحقيق:

– عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ عن طريق (disk comp).

– نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

– العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

– حفظ المعدات والأجهزة التي تضبط بطريقة فنية.

– العمل على فحص البرامج وتطبيقها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلوماتي.

– أن يكون الهدف من نسخ محتوى الاسطوانة والأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.

ثانيا: المتطلبات المهنية والتقنية للمحقق في الجرائم الإلكترونية

يعد المحقق في الجريمة الإلكترونية المسؤول الأول، عن الكشف عن ملابسات الجريمة الإلكترونية وتحديد هوية مرتكبها وجمع الأدلة الرقمية، التي تدينهم أو تبرئهم بهدف تقديمها للسلطة القضائية المختصة وتكمن مهمته الأساسية في تنفيذ أحكام القانون ذات الصلة، بما يتوافق مع اختصاصه وصلاحيته المحددة قانونا[2].

وعند مباشرة المحقق التحقيق في الجريمة الإلكترونية فيجب معرفة العديد من الجوانب الفنية، ليقوم بعمله على أحسن وجه وهي كالآتي:

– معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والأنترنت والتي تتعلق بالجريمة المرتكبة دلك أن افتقار ضابط الشرطة القضائية للتأهيل الكافي، في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل على اعتبار أن جهله بأساليب ارتكاب الجريمة الإلكترونية يجعله يقع في الكثير من الأحيان في أخطاء من شانها أن

[1] نعيم سعيداني، المرجع السابق، ص ص 112 113.

[2] مصطفي محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة الطبعة الأولى، القاهرة 2008.ص253.

تؤدي إلى محو الأدلة، الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة أو أوعية المعلومات التي تخزن بها البيانات[1].

– القيام بالإجراءات الصحيحة والمشروعة من اجل الحافظة، على الأدلة الإلكترونية التي تدل على وقوع الجريمة والقيام بتخزينها في أقراص معدة لذلك لمنع حذفها.

– معرفة الأشكال المختلفة للملفات وتطبيقات الحاسوب الرئيسية، فالملفات تعتبر الوعاء الحقيقي لأدلة الإدانة في الكثير من القضايا المتعلقة بشبكة الأنترنت وبما تحتويه من معلومات[2].

– أن يكون المحقق على دراية بالأساليب المستخدمة في ارتكاب الجرائم المعلوماتية، وتقنيات الأمن المعلوماتي لأنها من الأمور التي قد تساعده في معرفة الجناة ومواقع ارتكاب الجريمة[3].

المطلب الثاني

إجراءات الحصول على الأدلة في الجريمة الإلكترونية

يعد الحصول على الأدلة في الجريمة الإلكترونية من أبرز التحديات التي تواجه الجهات القضائية نظرا لطبيعة هده الجرائم وارتباطها بالتقنيات الحديثة، وتكمن أهمية الأدلة في كونها الأساس الذي يبني عليه التحقيق ومن ثم المتابعة القضائية، وفي هذا السياق تختلف إجراءات الحصول على الأدلة بحسب طبيعتها.

وعليه سنتناول في (الفرع الأول) الإجراءات العامة المعروفة بالتقليدية لجمع الدليل الإلكتروني ثم سنتطرق في (الفرع الثاني) إلى الإجراءات الحديثة لجمع الأدلة الإلكترونية.

الفرع الأول

الإجراءات التقليدية للحصول على الأدلة في الجريمة الإلكترونية

رغم الطبيعة التقنية المعقدة للجرائم الإلكترونية إلا أن الجهات القضائية، في الجزائر لا تزال تعتمد على مجموعة من الإجراءات التقليدية المنصوص عليها في قانون الإجراءات الجزائية، وسنتطرق إلى كيفية تطبيق هده الإجراءات التقليدية في مجال الجرائم الإلكترونية.

أولا: المعاينة

[1] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجي الحديثة، دار النهضة العربية، القاهرة 2022 ص 115.

[2] خالد علي نزل الشعار، التحقيق الجنائي في الجرائم الالكترونية، رسالة لنيل شهادة الدكتورة في الحقوق والعلوم السياسية، جامعة المنصورة، ص 43.

[3] نعيم سعيداني، المرجع السابق، ص 117.

المعاينة في الجريمة الإلكترونية هي إجراء قانوني يهدف إلى جمع الأدلة الرقمية من مسرح الجريمة الإلكترونية، من خلال فحص الأجهزة الإلكترونية والأنظمة المعلوماتية والبرمجيات بهدف كشف الجريمة والمساهمة في التحقيقات الجنائية[1].والمعاينة هي: " الكشف الحسي المباشر والمادي لإثبات حالة الشيء أو المكان أو الشخص وكل ما يفيد في كشف الحقيقة "[2].

لقد أشار المشرع الجزائري إلى إجراء المعاينة في المادة 79 من قانون الإجراءات الجزائية حيث نصت على انه: " ويجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها... "[3]، ويعد هدا الإجراء جزءا من التحقيق أو الاستدلال حيث يهدف إلى إظهار الحقيقة ، من خلال إثبات وقائع معينة في أماكنها الأصلية، كما أن السلطات المختصة لا يتوقف تطبيقها على صفة من يحركها بل تعتمد على مقتضيات إجراءها بما لا يمس حقوق الأفراد، فإذا تمت المعاينة في مكان عام فإن إجرائها يعتبر استدلالا عاما أما إذا استدعت المعاينة دخول مسكن خاص ، فإن الأمر يتطلب الحصول على إذن مسبق من السلطة المختصة وفقا لما يقتضيه القانون[4] .

وبما أن المعاينة تمثل إحدى الوسائل المهمة لجمع الأدلة فإنها لا تقتصر فقط على الجرائم التقليدية، بل تشمل أيضا الجرائم الالكترونية نظرا للطابع الفني الدقيق الذي يميز هدا النوع من الجرائم وبالتالي فإن أهمية المعاينة في مجال الجرائم المعلوماتية تعادل أهميتها في الجرائم التقليدية[5].

ووفقا لما نصت عليه أحكام المواد 42 79 80 من قانون الإجراءات الجزائية فانه يجوز إجراء المعاينة من طرف قاضي التحقيق بعد إشعار وكيل الجمهورية المختص إقليميا، كما يمكن أيضا إسناد هذا الإجراء إلى جهات مختصة أخرى مثل قضاة التحقيق التابعين لمحاكم أخرى إذا دعت الضرورة لذلك.

وتجدر الإشارة إلى أنه يمكن لضباط الشرطة القضائية أيضا إجراء المعاينة إخطار وكيل الجمهورية خاصة إذا كانت الجريمة قابلة للاندثار أو اختفاء أثارها بسرعة، ونتيجة لذلك يتعين على الجهات المكلفة بالتحقيق اتخاذ إجراءات دقيقة ومراعاة المبادئ القانونية المنصوص عليها في هذا الإطار[6].

---

[1] وسام سالي، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة ماجيستير، جامعة الجزائر، 2019 ص 37.

[2] حسن الجوخدار، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 90.

[3] المادة 79 من القانون رقم 18-6 المؤرخ في 10جوان 2018 يتضمن تعديل قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 34.

[4] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص ص 219 220.

[5] خالد ممدوح إبراهيم، المرجع السابق، ص 151.

[6] وسام سالي، المرجع السابق، ص 37.

ولتحقيق المعاينة في الجريمة الإلكترونية بفعالية يجب إتباع الإجراءات والخطوات التالية:

– تصوير الأدلة الرقمية: يجب تصوير أجهزة الحاسوب والهواتف الذكية وغيرها من الوسائل التكنولوجية التي يشتبه في استخدامها لارتكاب الجريمة، مع التركيز على الأماكن التي تحتوي على أدلة رقمية كما يجب توثيق الصور بأعلى درجات الدقة مع تحديد تاريخ ووقت كل صورة.

– توثيق التوصيلات والكابلات: يجب فحص التوصيلات المادية والكابلات المرتبطة بالأجهزة الرقمية، إذ قد تحتوي على أثار رقمية يمكن مقارنتها وتحليلها لاحقا عند عرض الأدلة أمام الجهات القضائية المختصة.

– رفع الأدلة المادية يتعين جمع الأدلة المتعلقة بالجريمة سواء كانت أوراقا أو مستندات رقمية أو وسائط التخزين، مثل الأقراص المضغوطة والشرائح الالكترونية ودلك بغرض فحصها ورفع البصمات الرقمية منها[1].

ثانيا: التفتيش

يعرف التفتيش في الجريمة الالكترونية بالإجراءات التي تقوم بها السلطات المختصة بتحقيق في أنظمة المعالجة الألية للبيانات، والذي بدوره يهدف الى كشف الأنشطة الغير مشروعة التي قد تشكل جريمة أو مخالفة قانونية، ويتم ذلك عبر البحث عن أدلة تثبت الجريمة وتساعد في نسبها إلى المتهم بارتكابها[2].

1. ضمانات التفتيش:

للتفتيش ضمانات موضوعية وضمانات شكلية تتمثل فيما يلي:

أ. الضمانات الموضوعية:

وجود جريمة الكترونية تستدعي إجراء التفتيش أي لها وصف جناية أو جنحة.

– وجود أشخاص يشتبه في تورطهم في ارتكاب الجريمة الالكترونية، أو المساهمة فيها إما بوصفه فاعلا أصليا أو ثانويا.

– وجود عدة قرائن تأكد وجود عدة أدلة مادية، قد تساهم في الكشف عن حقيقة أجهزة أو مسندات الكترونية....

ب. الضمانات الشكلية:

[1] خالد ممدوح إبراهيم، المرجع السابق ص 164.

[2] مصطفي خالد حامد أحمد، المعلوماتية والمسؤولية الجزائية، مجلة الفكر الشرطي، مركز بحوث الشرطة القيادة العامة لشرطة الشارقة الإمارات، المجلد 20، العدد 79، أكتوبر 2011، ص 174.

ولصحة التفتيش يجب أن تكون هناك شروط شكلية وهي:

- إصدار أمر بالتفتيش يكون محددا من حيث نطاقه وأسبابه دون أن يكون عاما.
- في حالة الندب كتابة الإذن بالتفتيش.
- حضور الشخص المعني بالتفتيش أو اثنين من الشهود أثناء العملية.
- الالتزام بالمواعيد التي حددها القانون لتنفيذ التفتيش إذ يجرى عادة بين الساعة 5.00 صباحا إلى 20.00مساءا مع مراعاة الاستثناءات الواردة في المادة 47 (الفقرة 2) من قانون الإجراءات الجزائية.
- إعداد محضر رسمي يوثق عملية التفتيش وفقا للقانون[1].

2. أنواع التفتيش في الجريمة الإلكترونية:

إن التفتيش عن الدليل الرقمي في الوسط الافتراضي وضبط محتوياته يعتبر مشروعا حيث تتمثل أنواع التفتيش فيما يلي:

أ. تفتيش المقاومة المعلوماتية عن بعد:

يسمح القانون الجزائري بموجب المادة 09/04 بتفتيش النظم المعلوماتية عن بعد المادة 5 التي تنص على: وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكدا المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية. [2] فالتفتيش هنا يستهدف أشياء معنوية وليست مادية كالبرامج وقواعد البيانات، لأن هذه قد تكون وسيلة لارتكاب جريمة أو تخزين معلومة بشأنها لاسيما إن كانت هذه المعلومات غير مرتبطة بأية دعامة مادية، غير أن المشرع الجزائري قد أجاز إفراغ نسخ تلك المعلومات المشكوك فيها والتي من شأنها الإفادة في الكشف عن الجريمة أو مرتكبها على دعامة التخزين الإلكتروني تكون قابلة للحجز وهذا كما أشار إليه في المادة 06 من قانون 09/04[3].

ب. تمديد التفتيش من منظومة معلوماتية أو جزء منها إلى أخرى أو جزء منها:

يبدو أن المشرع الجزائري يعطي هذه التقنية أهمية كبيرة في مجال المعلوماتية ويتعلق الأمر بارتباط شبكة الحواسيب ببعضها البعض وبالتالي هناك ترابط بين الأنظمة المعلوماتية حيث يذهب المشرع إلى امتداد التفتيش إلى سجلات البيانات المحفوظة في أماكن أخرى، حيث يوجد ارتباط بينها وبين حاسب

[1] نذير ارتاس وآخرون، المرجع السابق، ص ص 119 130.

[2] المادة 05 من قانون 04/09.

[3] وهيبة لعوارم. المرجع السابق، ص 97.

المتهم في مكان واحد وهو ما يطلق عليه الشبكة المحلية، أو الموزعة ومرتبطة بواسطة خطوط الهاتف أو بواسطة الأقمار الصناعية ويطلق عليها بالشبكة الممتدة [1]

وهذا ما نستخلصه من المادة 08 من قانون 09/04 انه يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها ولكن بعد إعلام السلطة القضائية المختصة وأحد الإذن بذلك.

ج.تمديد التفتيش خارج حدود الدولة:

في الأصل لا يجوز امتداد التفتيش في الوسط الافتراضي خارج حدود الدولة احتراما لمبدأ السيادة و لكن من القواعد المتفق عليها أنه لا تلازم بين تطبيق قانون العقوبات وارتكاب الجريمة على إقليم الدولة، إذ ترتكب خارج إقليمها ومع ذلك يكون قانونها واجب التطبيق، كالاختصاص وفقا لمبدأ العينية و الشخصية و العالمية إذ يتعذر على الدولة مباشرة اختصاصها بالتحقيق خارج إقليمها لان دلك من مظاهر سيادتها فلا يسمح لها بممارسته على إقليم دولة أخرى، ولذا فمن المعتذر قانونا مباشرة الدولة المختصة بالتحقيق لأي إجراء خارج إقليمها بشان الجريمة رغم انعقاد اختصاصها بالتحقيق فيها، لذلك يتم هدا النوع من التفتيش وفق أطر قانونية محددة تعتمد على اتفاقيات و معاهدات دولية، لذلك تبدو اتفاقية الإنابة القضائية هي السبيل لتحصيل هذا الدليل مثل اتفاقية بودابست المادة 01.25 و القانون الهولندي[2].

ثالثا: ضبط (حجز) الأدلة

الضبط هو العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها وهو الغاية من التفتيش والنتيجة المباشرة والمستهدفة، ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تنطبق بشأن التفتيش، وقد يؤدي بطلان التفتيش إلى بطلان الضبط[3].

ولقد تطرق إليه القانون 09-04 في مادته السادسة منه(6) بحجز المعطيات المعلوماتية وهو الأثر الذي ينتهي به التفتيش، ويناط به وضع اليد على الأشياء والوسائل التي تم بموجبها ارتكاب الجريمة والتي من شأنها تسهيل الكشف عن الحقيقة ليتم وضع الأشياء المضبوطة في احراز مختومة وتقديمها للقضاء كدليل إثبات[4].

---

[1] يوسف صغير، التفتيش كألية لإثبات جرائم نظم المعلوماتية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، المجلد 16، العدد 04، 2021، ص ص 598 599.

[2] وهيبة لعوارم. المرجع السابق، ص 101.100.

[3] مصطفي محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة الطبعة الأولى، 2008، ص 208.

[4] نذير ارتاس وآخرون، المرجع السابق، ص 133.

وعند مباشرة التحقيق فوجود دليل رقمي تم ضبطه فإن الإجراء المتخذ بعدها الحجز كما عبر عن المشرع الجزائري بموجب المادة06 من القانون 04/09 والتي نصت على أنه:".. عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ معطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة التخزين الإلكترونية تكون قابلة للحجز ووضعها في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، يجب في كل الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية..."[1]

مع وجوب الإشارة انه في حال الاستحالة على السلطة القائمة بالتفتيش، أن تقوم بإجراء الحجز لأسباب تقنية فانه يتوجب عليها استعمال التقنيات المناسبة بهدف منع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتي. ولقد تناولته أيضا المادة 42 من قانون الإجراءات الجزائية انه يمكن للقاضي تحقيق حجز الأشياء، التي يراها ضرورية في عملية الضبط وقد تحدد طبيعة الضبط حسب الطريق التي يتم فيها وضع اليد على الشيء المضبوط إما عبارة عن إجراء تحقيق أو عبارة عن إجراء الاستدلال.

ومن بين أنواع الضبط نجد أنه يرد على عناصر معلوماتية منفصلة وعلى سبيل المثال نجد الاسطوانات الممغنطة وهنا لا نجد مشكلة قانونية عن القيام بعملية الضبط ولكن المشكلة التي تثير الصعوبة هو حالة ضبط نظام التشغيل بأكمله وذلك لاحتوائها على عناصر لا يمكن فصلها ولذلك يجب ضبطها لتضمنها على عناصر مهمة في الإثبات[2].

أما بالنسبة للعناصر المادية للحاسوب فنجد أنه لا يثير أي صعوبة فيمكن ضبط الوحدات الإلكترونية ومنها المفاتيح لوحة، نظام الفأرة، نظام القلم الضوئي، وضبط كذلك وحدات المخرجات ومنها عدة وسائل من بينها الشاشة الطابعة الرسم والمصغرات الفيلمية[3].

وبعد القيام بضبط وحجز البيانات المعلوماتية يجب أخذ ببعض الإجراءات الخاصة للحفاظ عليها وصيانتها:

- ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسختها.
- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة ولا للرطوبة.

[1] أنظر المادة 06 من القانون 09-04.

[2] خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011 ص 168.

[3] المرجع نفسه، ص 168 169.

– منع الوصول إلى البيانات التي تم ضبطها أو رفعها من النظام المعلوماتي وهذا ما قد تناولته اتفاقية بودابست ويتم اللجوء لهذا الإجراء في حالة ما إذا كانت البيانات تتضمن خطر بالمجتمع. ومن خلال هذا نلاحظ أن الضبط هو إجراء من الإجراءات المادية التي يستخلص منه الدليل الإلكتروني.

رابعا: الخبرة

الخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق أو المحكمة تحديد التفسير الفني للأدلة أو الدلائل للاستعانة بالمعلومات العلمية فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو المادي وإنما هي تقديم فني لهذا الدليل فهي في مجملها تقرير صادر عن الخبير في أمر من الأمور المتعلقة بالجريمة.

والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة والشهادة والتفتيش هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها التحليلية في الإثبات والذي يتطلب معارف علمية أو فنية خاصة لا تتوافر سواء لدى المحقق أو القاضي.

إن الخبرة التقنية في مجال الإنترنت والعالم الافتراضي لا تشمل بالضرورة تلك النوعية من الخبرة الدراسية فدراسات الحاسب الآلي و الإنترنت لا ترتبط بمنهج دراسي أو بحثي معين أو حتى مدة زمنية يقضيها المرء دراسات في الجامعات و المعاهد المتخصصة وإنما ترتبط بمهارات خاصة و بموهبة استعمال الحاسوب والإنترنت و التعامل مع تقنية المعلومات إذ أن امهر مبرمجي نظام التشغيل حتى الآن مثل bill Gates لم يكن تحصيله العلمي يتجاوز المرحلة الثانوية وذات الأمر ينطبق على الهاكرز ومخترقي الأنظمة فان أعمارهم لا تتجاوز مرحلة التعليم الثانوي و السنوات الجامعية الأولى في أحسن الأحوال[1].

1. أنواع الخبرة:

إن الخبرة في الجريمة الإلكترونية أنواع سنتطرق إليها فيما يلي:

أ. الخبرة الخاصة:

وهذه تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة، وهي تضم الخبرة الفردية التي تعد أقوي و أهم مظاهر الخبرة السائدة في مجال تكنولوجيا الأنترنت، ويكفي هنا أن نذكر أن المؤسسات الكبرى المتخصصة في الحاسب الآلي

[1] مراد فلاك، اليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، العدد الخامس، جامعة ثليجي، الأغواط، 2019، ص 213.

والأنترنت تسعى بكل جهودها إلى الاستعانة العقدية بأشخاص أثبتوا كفاءتهم في مجال الحاسوب والأنترنت، حتى عصاة القانون منهم فهناك اتجاه اقتصادي يحاول جاهدا إثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون، وإنما يلزم اللجوء إلى الحلول الاقتصادية لكي يمكن أن يضلوا عاملين في إطار الأهداف الاقتصادية، بل إن من الدول ما تسعى جاهدة إلى محاولة التعرف على قراصنة تحولوا مع مرور الوقت إلى رموز وطنية جراء تحركاتهم عبر الأنترنت.

ب. المؤسسات التعليمية:

لما كانت الأنترنت تعد أحد منتجات العلم في حركته التقنية فانه يمكن القول أن اقوي مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة في العالم الافتراضي يمكن أن تكون من خلال المؤسسات التعليمية وهذه المؤسسات تعتمد على المنهج العلمي الغير التجاري هدفها تأكيد و تطوير العلم ليقضي على المشكلات التي قد تواجه البشرية، و لقد قامت عدة مؤسسات تعليمية بتكوين دراسات الحاسب الآلي التي تتطور بشكل فائق في جامعة ستانفورد و معهد التكنولوجيا في ماساشوستس الذي قدم للبشرية خبراء على درجة عالية من التفوق.

ج. جهات الضبط القضائي:

سرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجرام عبر الأنترنت وعلى رأس تلك الدول الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الإنتربول وكأن أخر نشاط مؤسسي في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية Fbi أطلق عليه المعمل الإقليمي الشرعي للحاسوب[1].

2. أساليب عمل الخبير التقني:

للخبير التقني في سبيل تحرى الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها وهو في إطار القيام بعمله عليه أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب مالم يكن رفضها لها مسببا بشكل منطقي وإلا تعرض حكمها للنقد.

وهناك أسلوبان لعمل الخبير التقني:

- **الأول:**

القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كما هو الشأن في التهديد أو النصب أو السب أو جرائم النسخ أو بث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة

[1] مراد فلاك، المرجع السابق، ص 214.

وغيرها ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، ومن ثم كيفية التوصل إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الأنترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع[1].

- **الثاني:**

القيام بتجميع و تحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته و إنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب الجرائم و القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم والقيام بالدخول من مكان ثابت هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشتركا لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها و يقوم بالولوج إلى الأنترنت من محل إقامته كذلك يحق للخبير أن يطلع على شهادات و أقوال الجناة في الصحف و أمام الجهات الرسمية و الشعبية إذ أن كثيرا ما يكون في مثل هذه الأقوال عوامل مساعدة لخبرته فيمكن من خلالها التعرف على أسلوب عمل مرتكب الجريمة الالكترونية والتعامل معه على أساس أقواله[2].

خامسا: الشاهدة

تعرف الشهادة بأنها تقرير الشخص لما قد يكون قد رآه أو سمعه أو أدركه على وجه العموم بالحواس أما في الجريمة الالكترونية فيقصد بالشاهد بأنه الشخص الغني صاحب الخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي وشبكاته ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي تميزا له عن الشاهد التقليدي[3].

ويشمل الشاهد في الجرائم الإلكترونية عدة طوائف أهمها:

- **القائم على تشغيل الحاسب الآلي:** وهو المسؤول عن تشغيل الحاسب الآلي والمعدات المتصلة به ويجب أن تكون لديه الخبرة الكبيرة في استخدام الجهاز كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.
- **المبرمجون:** وهم الأشخاص الذين يأخذون على عاتقهم كتابة البرامج وينقسمون إلى فئتين:
- **الفئة الأولى:** هم مخططو البرامج التطبيقية ويقومون بالحصول على خصائص النظام المطلوب.

---

[1] منى الأشقر جبور، القانون والأنترنت تحدي التكيف والضبط، بيروت المكتبة المصرية، 2011، ص 78.

[2] عائشة بن قارة مصطفي، مرجع سابق ص 80.

[3] سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، الطبعة الأولى، دار الكتب القانونية مصر 2012 ص 216.

- **الفئة الثانية:** وهم مخططو برامج النظام ويقومون باختيار وتعديل وتصحيح برامج النظام الحاسب الداخلية وإدخال أي تعديلات أو إضافات لها.

- **المحللون:** وهم الأشخاص الذين تأتي على عاتقهم مهمة التحليل الخاصة ببيانات نظام معين إلى وحدات مفصلة واستنتاج العلاقة الوظيفية منها، كما يقومون كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب الالي.

- **مهندسو الصيانة والاتصالات:** وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وبمكوناته وشبكات الاتصال المتعلقة به.

- **مديرو النظام:** وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

- **طاقم عمليات البيانات:** الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها لشريط أو أسطوانة.

- **مهندس الصيانة الالكترونية:** الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة.[1]

الفرع الثاني

الإجراءات الحديثة للحصول على الدليل الالكتروني

إن تطور أساليب ارتكاب الجريمة الالكترونية وأخدها منحنى تصاعديا بين الجرائم المرتكبة في الجزائر لذلك فرض على المشرع الاعتماد على قواعد إجرائية خاصة في سبيل مكافحتها وهذا ما تطرق إليه قانون الإجراءات الجزائية والقانون رقم 09-04.

أولا: التسرب

استحدث المشرع الجزائري إجراء التسرب بموجب المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري التى تنص على: "...عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابة حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبنية في المواد أدناه ".

أورد المشرع الجزائري تعريف التسرب بموجب نص المادة 65 مكرر 12 من قانون الإجراءات الجزائرية الجزائري التي تنص على :" يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم، يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 246

الغرض هوية مستعارة و أن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه ، و لا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم "[1].

ومن هنا فالتسرب هو عملية تتسم بالتعقيد، فهو من تقنيات التحري والتحقيق الخاصة حيث تسمح لعون أو ضابط الشرطة القضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية أخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه الفاعل أو الشريك[2].

والتسرب كغيره من الإجراءات الحديثة له ضوابط وشروط شكلية وأخرى موضوعية حتى يعتد به:

1. **الشروط الشكلية:**

أ. الإذن: هو عبارة عن وثيقة رسمية صادرة عن سلطة قضائية مختصة، متمثلة في وكيل الجمهورية أو قاضي التحقيق، ويجب أن يحتوي على تاريخ صدوره أو الجهة المصدرة له والرقم الذي صدر به والموضوع الذي يحدد طبيعة الجريمة المراد كشفها والختم والتوقيع، ويتضمن هوية ضابط الشرطة القضائية المشرف على العملية والمدة الزمنية اللازمة للقيام بعملية التسرب (04) أشهر قابلة للتجديد ويمكن للجهة القضائية المصدرة للإذن أن تطلب بإيقافها قبل انقضاء المدة المحددة بالإذن[3]

ب.تنفيذ عملية التسرب: قبل البدء في عملية التسرب وطبقا للمادة 65 مكرر 13 من قانون الإجراءات الجزائية يقوم ضابط الشرطة القضائية المنتدب كمسؤول ومنسق لعملية التسرب بتحرير تقرير يضمنه العناصر الضرورية لمعاينة الجرائم أحدها بعين الاعتبار تلك الجرائم التي يمكن أن تشكل خطرا على العون أو الضابط المتسرب وكل من يتم تسخيره للعملية.

ج.الحماية القانونية للمتسرب: نتيجة لسرية عملية التسرب وخطورتها على القائم بها، فلقد حصنه قانون الإجراءات الجزائية الجزائري برعاية خاصة للحفاظ على أمنه وسلامة روحه وذلك من خلال:

- منع كشف هويته الحقيقية عند أخذه هوية مستعارة تنفيذا لعملية التسرب.
- عدم جواز سماع المتسرب شخصيا كشاهد على العملية.

---

[1] أنظر الى المادة 65 من الأمر رقم 155/16.

[2] سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة لنيل شهادة الدكتوراه قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة الجزائر، 2014، ص 42.

[3] علاوة هوام، التسرب كألية للكشف عن جرائم في القانون الجزائري، مجلة الفقه والقانون كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر – باتنة 2012، ص 3.

– عدم جعل المتسرب أن يتحمل المسؤولية الجنائية عن الجرائم التي قد يكون ارتكبها أثناء تسربه وقيامه بالمهمة الموكلة إليه قانونا شريطة ألا تكون أفعاله تحرض على ارتكاب جرائم[1].

2. الشروط الموضوعية:

أ. التسبيب:

حتى يكون قانونيا اشترط المشرع في نص المادة 65 مكرر 15 أن يكون مكتوبا ومسببا لأن التسبيب هو أساس العمل القضائي فكان لازما على رجل القضاء المختص بإصدار الإذن بالتسرب أن يسبب وذلك بإبراز الأدلة القانونية والموضوعية بعد تقدير جمع العناصر الواردة في تقرير ضابط الشرطة القضائية والتسبيب يكفي وحده للدلالة على أن الإذن مكتوب كما يسمح للقضاء ببسط رقابته على شرعية الإذن صحته.

ب.نوع الجريمة:

حينما يصدر وكيل الجمهورية أو قاضي التحقيق الإذن بالتسرب يجب أن يتضمن هذا الإذن نوع الجريمة المراد إجراء عملية التسرب فيها، على ألا تخرج على نطاق الجرائم السبعة المذكورة بنص المادة 65 مكرر 05.

تتم عملية التسرب في نطاق الجريمة الالكترونية بدخول ضابط أو أعوان الشرطة القضائية في العالم الافتراضي وذلك باختراقهم للمواقع الالكترونية والمشاركة في المحادثات مع المشتبه به وظهورهم كأنهم فاعلين أصليين وذلك باستخدام أسماء وصفات وهمية، من أجل تعلم كيف يتم اختراق المواقع وكيف يتم ارتكاب هذه الجرائم من أجل جمع الأدلة المراد إثباتها.

ثانيا: اعتراض المراسلات، تسجيل الأصوات، التقاط الصور

لقد قام المشرع الجزائري بالتطرق إلى اختراق أعراض المراسلات في الفصل الرابع من قانون الإجراءات الجزائية في المواد من 65 مكرر05 إلى 65 مكرر تحت عنوان: " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"[2].

[1] فوزي عمارة، قاضي التحقيق في قانون الإجراءات الجزائية الجزائري، رسالة لنيل شهادة دكتوراه في العلوم القانونية، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009–2010، ص 249.

[2] أنظر المادة 65 من الأمر 155/66.

ويقصد بها اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية أو اللاسلكية ، وهذه المراسلات عبارة عن بيانات قابلة للإنتاج ، والتوزيع ، والتخزين ،الاستقبال ، و العرض 2 إلى أن جاءت المادة 02 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها التي وسعت من المفهوم التقليدي للمراسلات و أدخلت الاتصالات الالكترونية في مفهومها تماشيا مع التطور التكنولوجي ، الذي تطرق إلى الاتصالات الالكترونية " أي تراسل أو إرسال أو استقبال علامات أ, إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية ...."[1].

وعليه فقد وضع المشرع الجزائري للقيام بإجراء اعتراض المراسلات وتتمثل هذه الشروط في:

- الحصول على إذن من وكيل الجمهورية، أو من قاضي التحقيق إذا تم فتح تحقيق قضائي

- أن يكون الإذن الصادر عن وكيل الجمهورية أو قاضي التحقيق مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات البحث والتحري.

- وجوب تضمنه على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوبة التقاطها والأماكن المقصودة.

- أن يكون هذا الإجراء في الجرائم المحددة بموجب المادة 65 مكرر 05، من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أما في الجريمة الالكترونية فيمكن اعتراض المراسلات من خلال المعلومات التي تحتويها حاشية رسالة البريد الالكتروني Header Maile حيث تتضمن على عنوان IP لمرسل الرسالة فعنوان IPيحتوي على معلومات تتمثل في الكومبيوتر الذي تم إرسال منه الرسالة، وأيضا الموقع الجغرافي الذي أرسلت منه و في الأخير معلومات مزود الخدمة الذي يتعامل معه مرسل الرسالة.

ثالثا: المراقبة الالكترونية

تعتبر الرقابة على الاتصالات الالكترونية أو كما يطلق عليها بمصطلح " الرقابة الالكترونية للاتصالات"

من أهم مصادر التحري التي يستعان بها في التحري على مختلف الجرائم بما في ذلك الجرائم المتصلة بالتكنولوجيا الحديثة ، خاصة في ظل أجواء الجناة إلى وسائل التقنية الحديثة للاتصال في تنفيذ مخططاتهم

[1] أنظر المادة 02 من قانون 09_04.

الإجرامية و التواصل فيما بينهم ، كما تعد مراقبة الاتصالات الالكترونية مصدرا للأدلة الرقمية [1] لذلك و بالرجوع إلى القانون رقم 09_04 الذي سبق ذكره ، نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الرقمي فقط ، بل أدرجه ضمن التدابير الوقائية من الجريمة الالكترونية بداعي حماية النظام العام و هذا ما نصت عليه المادة 04 من نفس القانون .

وعليه فقد حدد المشرع الجزائري شروط اللجوء إلى تقنية المراقبة الالكترونية وهي:

– أن يتم تنفيذ هذه التقنية تحت سلطة القضاء وبإذن منه، بحيث لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة[2].

– أن تكون هناك ضرورة تتطلب هذا الإجراء، وذلك عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات البحث أو التحقيق دون اللجوء إلى المراقبة الالكترونية، وهو ما نصت عليه المادة 04 الفقرة ج من القانون 09–04 السالف الذكر.

رابعا: حفظ المعطيات

يمكن اعتبار الحفظ على المعطيات الالكترونية بأنه قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في الأرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل قصد تمكين جهات الاستدلال من الاستفادة منها واستعمالها لأغراض التحقيق، فعملية الحفظ إذا هي من مهام مقدمي الخدمات[3].

ولقد قام المشرع الجزائري بحصر المعطيات الالكترونية الواجب حفظها من طرف مزودي الخدمة وهي المعطيات المتعلقة بحركة السير لمعطيات المرور و قد عرفتها المادة 02 من القانون 09–04 في الفقرة "ه" بأنها : " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات ، توضح مصدر الاتصال و الوجهة المرسل إليها ، و الطريق الذي يسلكه ، ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة "[4].ومن ضمن معطيات المرور التي يتعين

[1] عيدة بالعابد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، جامعة مولاي الطاهر، سكيكدة، العدد 06، 2011 ص 143.

[2] أنظر المادة 04 من القانون 04/09.

[3] جمال إبراهيمي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، فرع الملكية الفكرية، جامعة الجزائر 1، بن يوسف بن خده كلية الحقوق، الجزائر 2021/2020 ص 101.

[4] أنظر الى المادة 02 من القانون 09_04.

على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لأغراض التحقيق تلك التي حددها المشرع في المادة 11 من القانون رقم 09-04 على النحو التالي :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال كرقم تسلسلي لجهاز الاتصال ونوعه.
- الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة وقدمها.
- المعطيات التي تسمح بالتعرف على المرسل والمرسل إليه كأرقام الهواتف مثلا وكذا عناوين المواقع المطلع عليها [1]

[1] أنظر المادة 11 من القانون رقم 09-04.

المبحث الثاني

حجية الدليل الالكتروني في الوقائع المراد اثباتها

تعتبر عملية تقدير الأدلة جوهر الحكم الذي نريد الوصول إليه، ويتم ذلك بممارسة القاضي لسلطته التقديرية على الأدلة التي هي محل الوقائع، ولتقدير الدليل الالكتروني بصفة خاصة لابد من أن يتم قبوله أولا للتأكد من مدى صلاحيته كدليل لإثبات ولقبول القاضي لهذا الدليل في الإثبات لابد أن يستند على أساس لذلك قمنا بتقسيم هذا المبحث إلى مطلبين سنتناول في (المطلب الأول) سلطة القاضي الجنائي في قبول الدليل الالكتروني و(المطلب الثاني) سلطة القاضي الجنائي في تقدير الدليل الالكتروني.

المطلب الأول

سلطة القاضي الجنائي في قبول الدليل الالكتروني

يعد الدليل الالكتروني خاضعا للقواعد المقررة لباقي وسائل الإثبات، حتى وإن كانت هذه القواعد ترتبط بسلطة القاضي الجزائي في تقدير مدى قبول هذا النوع من الأدلة ونظرا للطبيعة التي يتميز بها الدليل الالكتروني لذلك سنتطرق في (الفرع الأول) إلى أساس قبول الدليل الالكتروني في القاضي الجنائي و(الفرع الثاني) قيود قبول الدليل الإلكتروني القاضي الجزائي.

الفرع الأول

أساس قبول الدليل الالكتروني في الإثبات الجنائي.

تظهر بعض القوانين المقارنة أن سلطة القاضي الجنائي في قبول الدليل الالكتروني تختلف بحسب النظام القانوني السائد في الدولة، حيث تنقسم هذه الأنظمة إلى اتجاهات من بينها حرية الإثبات، وهو ما يمنح القاضي الجنائي سلطة تقديرية واسعة في قبول مختلف الأدلة، مع الأخذ بمبدأ القناعة الشخصية حيث لا يشترط حصر الأدلة القانونية في نطاق معين، كما تختلف حرية الإثبات باختلاف المرحلة التي

تستخدم فيها سواء تعلق الأمر بمرحلة التحقيق أو الحكومة أو تحديد العقوبة مما يضفي مرونة على مبدأ حرية الإثبات[1].

أولا: مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الالكتروني.

إن القاضي له سلطة مطلقة في الأخذ بأي دليل يساهم في الإثبات في وقائع الجريمة، فليس هناك دليل مفروض عليه أن يستعين به في تكوين قناعته منه وبناء عقيدته عليه، حيث ترجع حرية القاضي في تقدير وسائل الإثبات المطروحة أمامه في الدعوى نتيجة منطقية لمبدأ القناعة الشخصية وهي نتيجة ثانية إلى جانب حرية القاضي في الاستعانة بكل وسائل الإثبات، وهو كل واقعة تؤثر على مجريات الدعوى ولا يعتد بأي دليل إلا إذا اقتنع به القاضي، وله كامل السلطة في قبول أو رفض واستبعاد أي دليل لا يقتنع به[2].

وتعتبر حرية الإثبات في المسائل الجنائية من المبادئ المستقرة في نظرية الإثبات الجنائي وذلك بخلاف المسائل المدنية حيث يحدد القانون سلفا وسائل الإثبات وقواعد قبولها وقوتها.

ومنه فقد اعتمد المشرع الجزائري في الإثبات على مبدأ حرية الإثبات كأصل ونظام الأدلة القانونية كاستثناء من الأصل[3].

لذلك نصت المادة 1/212 من ق إ ج " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك "[4].

وتطرقت أيضا المادة 213 من ق إ ج " الاعتراف شأنه كشأن جميع عناصر الإثبات يترك لحرية القاضي"[5].

ومبدأ حرية الإثبات يعد بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية والتي تم حصرها كأدلة إثبات في مواجهة الجرائم المستحدثة ومن بينها الجريمة الالكترونية، أي فتح باب لنوع من الأدلة العلمية للاستفادة من الوسائل التي يكشف عنها العلم الحديث كبصمة الصوت والبصمة الوراثية DNA والدليل الالكتروني.

---

[1] عائشة بن قارة مصطفي، المرجع السابق، ص 181.

[2] نوال شعلال، سلطة القاضي الجنائي في تقدير الأدلة، مذكرة لنيل شهادة الماجيستير، فرع قانون العقوبات والعلوم الجنائية، جامعة سكيكدة 2008. ص 84.

[3] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للنشر والتوزيع، الجزائر، 2008، ص 38.

[4] المادة 212 من الأمر 66-155 المؤرخ في 18 صفر 1386 م. الموافق ل 08 يونيو 1966 المتضمن قانون الاجراءات الجزائية المعدل والمتمم، جريدة رسمية، عدد 48، الصادرة بتاريخ 28 يونيو 1966، ص 644.

[5] أنظر الى المادة 213 من الأمر 66-155.

وبالتالي يجب التنبيه إلى أن الدليل الالكتروني لا يختلف عن الأدلة الأخرى، والتي ورد ذكرها كمثال في القانون مقبول مبدئيا في الإثبات الجزائي بصفة خاصة إذا ما تم احترام في ضابط المشروعية، ذلك أن الحرية هنا لا يقصد بها إمكان اللجوء إلى وسائل غير مقبولة قانونا فالحرية هنا يجب أن تمارس في إطار قانوني[1].

ثانيا: نتائج مبدأ حرية الإثبات الجزائي على الدليل الالكتروني.

إن أعمال مبدأ حرية الإثبات يجعل من القاضي الجزائي دور ايجابي في كشف الحقيقة الفعلية و يبدوا هذا الدور في كشف الجرائم الالكترونية من ثلاث جوانب:

- له حرية في توفير الدليل المناسب والضروري للفصل في الدعوى بما في ذلك الدليل الالكتروني.
- له الحرية في قبول أي دليل يمكن أن تتولد منه قناعته بما في ذلك الدليل الالكتروني.
- أنه يتمتع بالحرية نفسها في تقدير قيمتها الاقناعية حسب وجدانه.

1 – الدور الايجابي للقاضي الجزائي في توفير الدليل الالكتروني:

يقصد بالدور الايجابي للقاضي الجزائي عدم التزامه بما يقدمه إليه أطراف الدعوى من أدلة، وإنما له سلطة وواجب أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعلية فيها.

وتكون مظاهر القاضي الجزائي في البحث عن الحقيقة وكشفها من خلال مرحلتين أساسيتين للدعوى الجزائية مرحلة التحقيق الابتدائي ومرحلة المحاكمة، على اعتبار أن مرحلة التحقيق الابتدائي هي المرحلة التحضيرية لمرحلة المحاكمة حيث يتم فيها حشد الأدلة وتمحيصها لتحديد مدى كفايتها لإحالة المتهم على المحكمة المختصة[2].

أ. مرحلة التحقيق الابتدائي:

يتحدد الدور الايجابي للقاضي الجزائي على حسب السلطة المناط بها في التحقيق ومهمة القاضي حول التحقيق والقيام بإجراءات البحث والتحري عن الجرائم وهذا ما نصت عليه المادة 38 من قانون

[1] عائشة بن قارة مصطفى، المرجع السابق ص ص187 188.

[2] عادل مستاري، دور القاضي الجزائي في ظل مبدأ الاقتناع القضائي، مجلة المنتدى القانوني، العدد الخامس، جامعة محمد خيضر بسكرة، 2018ص 182.

الإجراءات الجزائية،[1] التي تهدف إلى الكشف عن الحقيقة وتقوم بالعديد من الإجراءات الهادفة إلى جمع الأدلة والمحافظة عليها.

ب.مرحلة المحاكمة:

يوجد العديد من النصوص التي تبين مظاهر الدور الايجابي للقاضي الجزائي نذكرهم كما يلي:

– المادة 286 من ق إ ج " له السلطة الكاملة في ضبط حسن سير الجلسة وفرض الاحترام الكامل لهيئة المحكمة واتخاذ أي إجراء يراه مناسبا لإظهار الحقيقة "[2].

– المادة 235 من ق إ ج " يجوز للجهة القضائية إما من تلقاء نفسها أو بناءا على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة ..."[3].

وتطبيقا على الجرائم الالكترونية فان القاضي الجزائي وفي سبيل الوصول إلى الحقيقة له أن يوجه أمر إلى مزود الخدمة بتقديم المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم بالاتصال وكذا عناوين المواقع ....

كما للقاضي الجزائي سلطة الأمر باعتراض الاتصالات السلكية واللاسلكية مما قدر فائدة الإجراء وجديته وملائمته لسير الدعوى وأيضا ندب الخبراء وكذا إعلانهم ليقدموا إيضاحات عن التقارير المقدمة منهم لما للخبرة في مجال المساعدة القضائية من دور كبير فهي تعد من أقوى مظاهر تعامل قاضي الموضوع مع الواقعة الإجرامية المعروضة ويملك القاضي تعيين الخبراء لاسيما أن الأصل يضل للتحقيق الذي تجربه المحكمة في الجلسة وهذا ما أكدته المادة 143 قانون إجراءات جزائية[4].

2 – الدور الايجابي للقاضي الجزائي في قبول الدليل الالكتروني:

إن مرحلة قبول الدليل الالكتروني هي المرحلة الثانية التي تلي البحث عن الدليل وتقديمه من قبل جميع الأطراف الى سلطة القاضي، وطبقا لمبدأ الشرعية الجزائية التحى يتحصل من خلالها الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل الكترونية كالكمبيوتر المحمول مثلا لا يكون الدليل المقبول ولا يكون كذلك إلا إذا كان مشروعا بأن يتم البحث عنه والحصول عليه وفقا لطرق مشروعة[5].

---

[1] أنظر الى المادة 38 من الأمر 155/66.

[2] أنظر المادة 286 من الأمر 155/66.

[3] أنظر المادة 235 من الأمر 155/166.

[4] أنظر المادة 143 من الأمر 155/66.

[5] رشيدة بوكر، جرائم الاعتداء على نزم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2012، ص ص 487 486.

ومن خلال المادة 307 من قانون الإجراءات الجزائية فان الدور الايجابي للقاضي الجزائي في توفير الدليل الالكتروني من حيث ماهيته، مظاهره وتبيين كيف أن القاضي الجزائي على خلاف القاضي المدني ولا يجوز له أن يقنع بما يقدمه له الأطراف في الدعوى من أدلة وإنما عليه أن يبحث بنفسه عن الأدلة ذات الأثر في تكوين عقيدته، وأن يستشير الأطراف إلى تقديم ما لديهم من أدلة[1].

الفرع الثاني

قيود قبول الدليل الالكتروني في القاضي الجنائي

إن قبول الدليل الالكتروني يخضع لمبدأ حرية القاضي الجنائي في قبول الأدلة الا أن هذه الحرية تخضع لمجموعة من الشروط والقيود الواجب مراعاتها من قبل القاضي الجنائي، وهذه القيود متعلقة بمشروعية الدليل الالكتروني، وهناك شروط قد وردت بنصوص خاصة وهي:

أولا: قيد المشروعية والنزاهة في الحصول على الدليل الالكتروني

يقول البعض إذا كان الإثبات الجنائي حرا فانه شرعي[2] بمعني أنه لا يكون مقبولا إلا بشرط أن يجمع ويقدم وفقا للقانون وكل إثبات تم الحصول عليه بطريقة غير شرعية ينبغي استبعاده ولا يبني عليه الاقتناع. وتعني قاعدة مشروعية الدليل الجنائي التقيد بأحكام القانون والعمل في إطاره، أما عن مبدأ النزاهة فهو أوسع من مبدأ المشروعية فهو يرتبط بالقيم الأخلاقية ويرتكز على اعتبارات العدالة وكرامة الإنسان واحترام حياته الخاصة.

ولقد تخوف الفقه والقضاء من الأدلة الالكترونية ومن مدى مشروعيتها، لأن معظم الأدلة الالكترونية يتم الحصول عليها عن طريق المساس بحقوق الأفراد وحرياتهم وتبعا لذلك لا يجوز للقاضي أن يقبل إثبات إدانة المتهم دليلا الكترونيا تم الحصول عليه من تفتيش باطل أو عن طريق إكراه المتهم على الإفصاح عن كلمة السر أو التجسس المعلوماتي.

---

[1] أنظر المادة 307 من الأمر 155/66.

[2] محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 418.

وفي هذا فان تقدير مشروعية أية وسيلة مستحدثة بما فيها الدليل الالكتروني يتوقف على عدم المساس بحياة الفرد الخاصة أو النيل من كرامته أو سلامته الشخصية، دون اعتبار للقيمة العلمية التي يمكن أن تحظى بها النتائج المتحصل عليها.

ولهذا وضعت الاتفاقيات الدولية والدساتير الوطنية والقوانين الاجرائية المختلفة نصوصا تتضمن ضوابط لشرعية الاجراءات الماسة بالحرية، ومن ثم فان مخالفة هذه النصوص في سبيل الحصول على الدليل الالكتروني، يجعل منه يتصف بعدم المشروعية، ولهذا لا يجوز للقاضي أن يقبل في إثبات ادانة المتهم دليلا الكترونيا ثم الحصول عليه من تفتيش نظام معلوماتي باطل بعد صدور اذن من جهة غير مختصة، او لم تكن الجريمة الالكترونية محل الاذن قد وقعت بعد.

وقيد المشروعية يمثل مقابل لحرية القاضي الجنائي في قبول جميع أدلة الإثبات بما فيها تلك التي لم ينظمها المشرع، فالقانون اقتصر على الإشارة على أهم وسائل الإثبات وأكثرها شيوعا في العمل وترك الباب مفتوح أمام ما قد يستجد من وسائل أخرى، حيث يكتسب القيد أهمية كبيرة بسبب التقدم الهائل في الوسائل الفنية للبحث والتحقيق، فهو منى مقتضيات العدالة من شأنها محاربة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة.

1. مدى الأخذ بالدليل الإلكتروني مراعاة للمصلحة الأولى

وهي الحالات التي يكون فيها الدليل الإلكتروني غير مشروع كالتعدي على الحياة الخاصة لأحدهم وفي نفس الوقت يعد وسيلة إثبات لجرائم تهدد أمن ونظام المجتمع الأخلاقي وهنا تكون مشكلة أي المصلحتين أولى بالرعاية.

يشكك البعض في مشروعية الدليل الإلكتروني، معتبرينه تدخلا في الحياة الخاصة، خصوصا في القضايا المتعلقة بالجرائم الجنسية التي تتم برضا الطرفين إلا أن الاعتماد على الوسائل الحديثة كشبكة الأنترنت واستخدامها كأدلة على وقوع الجرائم، مثل الإعلان عن البغاء أو نشر المواد الفاضحة، يهدف إلى حماية المصلحة العامة مما يتيح للدولة الحفاظ على النظام الاجتماعي[1].

2. قيمة الدليل الإلكتروني غير المشروع

هنا علينا أن نقوم بالتمييز والتفريق بين نوعين من الأدلة، أدلة الإدانة وأدلة البراءة.

[1] عائشة بن قارة، المرجع السابق، ص 216 217.

– **أدلة الإدانة:** القاعدة في الأصل هي الإنسان بريء، فإن المتهم يجب أن يعامل على أنه بريء في جميع مراحل الدعوى حتى يصدر بحقه حكم بات، مما يقتضي أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة[1].

وبالتالي فإن الدليل قد يتم الحصول عليه بطريقة غير مشروعة لا تكون له قيمة في الإثبات ذلك أنه إذا ما سمح بقبول الأدلة التي تكون إجراءات باطلة، فمشروعية الإثبات الجنائي تستلزم عدم قبول أي دليل كان الحصول عليه قد تم بطريقة غير مشروعة فمتى تم الحصول بإجراءات تخرج عن إطار الشرعية فإن هذه الإجراءات تكون باطلة، وبالتالي فإنه إن تم بطلان إجراء ما يجب استبعاد ما ينتج عنه من أدلة تطبيقا لقاعدة ما بني على باطل.

والنظام اللاتيني يعمل بهذه القاعدة، والتي تعمل بها مع الدليل الالكتروني. فالأدلة التي يؤسس عليها حكم الإدانة يجب أن تكون مشروعة، سواء كانت أدلة تقليدية أو ناتجة عن الوسائل الالكترونية بصفة عامة، ومن الأمثلة الغير المشروعة للحصول على الدليل الالكتروني، إكراه المتهم المعلوماتي للدخول إلى ملفات البيانات المخزنة، وأيضا أعمال التحريض على ارتكاب الجريمة الالكترونية من قبل رجال الضبط القضائي كالتجسس المعلوماتي أو المراقبة الالكترونية عن بعد بدون إذن قانوني[2].

وبالتالي فإن الحصول على الدليل الالكتروني بطريقة غير مشروعة يتم إبطاله وهذا ما تطرق إليه قانون الإجراءات الجزائية الجزائري في المواد 1، 105، 157، 191. وهذا الأمر قد شكل مسألة مهمة هي المعيار الذي يبين العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له، حتى يمتد إليها البطلان.

في الجزائر فالمعيار المعتمد عليه هو أن العمل اللاحق يعتبر مرتبطا بالإجراء السابق. فإذا كان هذا الإجراء ضروريا لصحة العمل اللاحق، فإن أوجب القانون مباشرة إجراء معين قبل الآخر بحيث يصبح الأول بمثابة السبب الوحيد الذي بني عليه.

– **دليل البراءة:** فيما يتعلق بدليل البراءة ثار خلاف بين الفقهاء حول مدى اشتراط المشروعية لهذا النوع من الأدلة وانقسمت الآراء إلى ثلاثة اتجاهات رئيسية:

– **الاتجاه الأول:** يذهب الى أن مبدأ المشروعية يجب أن ينطبق على جميع الأدلة، سواء تعلقت بالإدانة أو البراءة، انطلاقا من ان قصر هذا المبدأ على أدلة الإدانة فقط يشكل انتقاصا من حماية الفرد والمجتمع

[1] أشرف عبد القادر قنديل، المرجع السابق، ص 208 209.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص 217.

معا. كما يرى هذا الاتجاه أن إثبات البراءة ينبغي أن يخضع أيضا لشرط المشروعية، باعتباره عنصرا جوهريا لضمان صحة الاقتناع القضائي[1].

– **الاتجاه الثاني:** يرى ان لا مانع من قبول دليل البراءة حتى وان تم الحصول عليه بوسيلة غير مشروعة استنادا إلى مبدأ افتراض البراءة الذي يشكل القاعدة الاصلية وبالتالي فان المحكمة ليست ملزمة بإثباتها.

ويؤكد أن إبطال الدليل غير المشروع هدفه حماية حقوق المتهم، ومن غير المنطقي أن يستخدم هذا الإبطال ضده. فرفض دليل يثبت براءته فقط لأنه غير مشروع قد يؤدي إلى إدانة بريء، وهذا ما يقبله المنطق القانوني خاصة وأن الشك يفسر لصالح المتهم[2].

– **الاتجاه الثالث:** يدعو إلى التمييز بين كيفية الحصول على دليل البراءة، فإن تم الحصول عليه من خلال ارتكاب الجريمة، وجب استبعاده حفاظا على هيبة القانون ومنها للإفلات من العقاب أما إذا تم الحصول عليه نتيجة مخالفة قاعدة إجرائية فقط، فيجوز قبوله كدليل للبراءة لأن بطلان الإجراء يعود إلى من ارتكبه، ولا ينبغي أن يحمل المتهم تبعاته، خصوصا إذا لم يكن يدا فيه[3].

ثانيا: القيود المستمدة من النصوص القانونية

الاصل ان القاضي الجزائي حر في ان يستمد قناعته من أي دليل يطمئن اليه دون ان يتقيد بدليل معين، الا انه ترد استثناءات بحيث لا تترك للقاضي حرية اختيار الادلة التي يستمد منها قناعته، وذلك بأن يحدد له المشرع الأدلة التي تقبل في إثبات بعض الجرائم، حيث لا يجوز الإثبات بغيرها، وانه يتعين الالتزام بأدلة الإثبات الخاصة ببعض المسائل التي تملك اختصاص النظر فيها بصفة تبعية للدعوى الاصلية، والتي تكون أدلة إثباتها قانونية على عكس الجزائية، وهذا ما سنتطرق اليه:

1. حصر الأدلة في بعض الجرائم:

ان المبدأ العام في الإثبات الجنائي هو عدم حصر الأدلة في نوع معين من الجرائم، لكن بعض التشريعات خرجت على هذا المبدأ ومن بين هذه التشريعات القانون الجزائري الذي لم يترك للقاضي الجزائي حرية اختيار الادلة التي يستمد منها قناعته في إثبات بعض الجرائم وجعل لها ادلة إثبات خاصة بها كجريمة الزنا والسياقة في حالة السكر[4].

---

[1] أشرف عبد القادر قنديل، المرجع السابق، ص 210.

[2] بلولهي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة لنيل شهادة الماجيستر، قسم الحقوق والعلوم السياسية، جامعة الجزائر الحاج لحضر، باتنة، 2010–2011، ص ص 106 107.

[3] عائشة بن قارة مصطفى، المرجع السابق، ص 221

[4] بلولهي مراد، المرجع السابق، ص 80.

وفي الأدلة الالكترونية ما يهمنا هو القيد في الأدلة المعينة في جريمة الزنا، فالمشرع الجزائري حصر وسائل إثبات الجريمة، التي يعاقب عليها بموجب المادة 339 من قانون العقوبات في ثلاث أنواع من الادلة نصت عليها المادة 341 من نفس القانون وهي: محضر قضائي يحرره أحد رجال الضبط القضائي في حالة تلبس، او اقرار صادر عن المتهم ضمن رسائل أو مستندات، أو اقرار قضائي أمام المحكمة.

ويذهب غالبية الفقه والقضاء الى أن هذه الادلة ملزمة فقط لإثبات زنا الشريك مع الزوجة الزانية، باعتبار أن إثبات الزنا بوجه عام يخضع لمبدأ حرية الإثبات الجنائي، وبناءا عليه لا يجوز للقاضي الجنائي أن يستند في ادانة الشريك الا الى الأدلة التي حددها القانون، حتى وان تعلق الامر بالدليل الالكتروني كصور او مقاطع فيديو او رسائل مرسلة من الشريك الى الزوجة عبر الهاتف المحمول أو الإنترنت، سواء احتوت على اعتراف صريح أو ضمني بحدوث الزنا، او عبارات توحي بوجود علاقة غير شرعية بين الطرفين.

وبناءا على ذلك ومن اجل سد الفراغ التشريعي القائم في معظم القوانين المعاصرة، ينبغي القياس بين الكتابة الالكترونية والمكاتيب والوثائق الورقية، خاصة وان بعض المشرعين ومن بينهم المشرع الجزائري وسعو من مفهوم الكتابة، وجعلوا الكتابة الالكترونية مساوية للكتابة الورقية، بشرط التأكد من هوية مصدر الكاتبة الالكترونية، ويلاحظ على القانون انه لا يشترط توقيع المتهم على المكاتيب او الوثائق الورقية لتعد دليلا على جريمة الزنا، طالما أنه ثبت صدورها أي أنه الشريك، وتبقى مسألة تقدير حجية هذه المكاتيب والوثائق من صلاحيات القاضي الذي ينبغي أن يتمتع بثقافة معلوماتية عالية، خاصة وأنها قابلة للتعديل، وقد يستغلها البعض بانتحال شخصيات للأضرار بالغير أو الشريك.[1]

لذلك كان من الأجدر بالمشرعين، ومنهم المشرع الجزائري أن ينصوا صراحة على اعتماد الدليل الالكتروني ضمن وسائل إثبات جريمة الزنا، من أجل سد الفراغ التشريعي الواضح، لا سيما في التشريعات العربية.

2. قيد الإثبات الخاص في المسائل الغير الجنائية:

عند نظر القاضي في الدعوى الجنائية قد تعرض عليه مسائل مدنية أو تجارية أو ادارية، في هذه الحالة يجب عليه أن يتبع طرق الإثبات الخاصة بتلك المسائل، كما هو الحال في عقود الأمانة كالوديعة وعادية الاستعمال والوكالة والرهن[2].

[1] عائشة بن قارة مصطفى، المرجع السابق، ص،ص 230، 231

[2] نفس المرجع، ص 235

ولقد تطرق المشرع الجزائري بموجب القانون 10/05 من القانون المدني على أنه يعتبر الإثبات بالكتابة في الشكل القانوني كالإثبات بالكتابة على الورق، بشرط امكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها[1].

يتبين أن للدليل الالكتروني دورا بالغ الأهمية، في إثبات المعاملات الالكترونية، التي أصبحت محورا أساسيا في اقتصاد العديد من الدول، وبناءا عليه يمكن للقاضي الجنائي الاستناد الى الدليل الالكتروني لإثبات بعض المسائل الأولية لا سيما ذات الطابع المدني والتجاري نظرا لارتباط هذه المعاملات بطرق الإثبات الحديثة، يمكن القول ان قبول الدليل الالكتروني يخضع لقيود يجب على القاضي الجنائي أخدها بعين الاعتبار لهذه المسائل من تأثير مباشر في تقدير القوة الإثباتية لهذا النوع من الأدلة في المجال الجنائي.

المطلب الثاني

سلطة القاضي الجنائي في تقدير الدليل الالكتروني

لقد منح المشرع للقاضي الجزائي سلطة واسعة في تقديره للأدلة المطروحة أمامه بما في ذلك الدليل الالكتروني، فله أن يبحث و يتحرى الحقيقة بكافة الأدلة ، فهو غير ملزم بإصداره حكم الإدانة أو البراءة لوجود دليل معين طالما أنه لم يقتنع به و ذلك عملا بمبدأ الاقتناع الشخصي ، و لكن هاته السلطة ليست مطلقة ، و إنما قيدها المشرع بضوابط تعمل على حسن سير عمل القاضي و تحقيق العدالة .لذلك سنتطرق في الفرع الأول حرية القاضي الجزائي في الاقتناع بالدليل الالكتروني أما الفرع الثاني فسنتطرق إلى ضوابط الاقتناع بالدليل الالكتروني في الإثبات الجنائي .

الفرع الأول

حرية القاضي الجزائي في الاقتناع بالدليل الالكتروني

إن مبدأ حرية الاقتناع الشخصي للقاضي الجزائي من أهم عناصر الإثبات في الدعوى الجنائية، لذلك فالقاضي حر بأن يأخذ بالأدلة التي يراها مناسبة للكشف عن الحقيقة وله أن يحتوي بنفسه صدق الأدلة الرقمية وأيضا له الحق في أن يستمد اقتناعه وعقيدته في أي مصدر يطمئن إليه.

أولا: مبدأ الاقتناع القضائي

[1] أنظر الى المادة 323 من القانون 10/05 المؤرخ في 20 يونيو 2005 المعدل والمتمم للقانون المدني الجزائري

يعتبر مبدأ حرية الاقتناع الشخصي للقاضي الجزائي، من أهم عناصر الإثبات في الدعوى الجنائية، فالقاضي حر بأن يأخذ بالأدلة التي يراها مناسبة للكشف عن الحقيقة وله أن يحتوي بنفيه صدق الأدلة الرقمية، وله الحق في أن يستمد اقتناعه وعقيدته "أي مصدر يطمئن اليه ". تم تطرق المشرع الجزائري إلى مسألة مبدأ الاقتناع القضائي الجزائي في المادة 307 من قانون الإجراءات الجزائية الجزائري، والتي هي مستوحاة من المادة 353 من قانون الإجراءات الجزائية الفرنسية[1].

وتطرق المشرع الجزائري إلى مبدأ الاقتناع القضائي في نص المادة 212 من قانون الإجراءات الجزائية على أنه:" يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال الشخصية التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ..."[2].

1. أساس مبدأ الاقتناع القضائي:

لقد تناولت أغلب التشريعات المقارنة موضوع الاقتناع الشخصي للقاضي الجزائي ولتم تجسيده في قوانينها الإجرائية، وإن أهم الأحكام القضائية التي طبقت هذا المبدأ هو:

أ. الأساس القضائي لمبدأ الاقتناع القضائي:

قضت المحكمة العليا الجزائرية بهذا المبدأ في عدة أحكام منها :"من المقرر قانونا أنه لا يطلب من القضاة المشكلين لمحكمة الجنايات ، أن يقدموا حساب عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم الشخصي، ولا يرسم لهم بها قواعد يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما ، ومن تم النعي على الحكم المطعون فيه بحر القانون غير سديد مما يستوجب رفضه، و لما كان الثابت في قضية الحال أن الحكم الصادر من محكمة الجنايات بالبراءة كان بأغلبية الأصوات و أن الأسئلة قد طرحت بصفة قانونية و أن الأجوبة المعطاة كانت بحسب الاقتناع الشخصي للقضاة الذي يخضع لرقابة المحكمة العليا و من كانت كذلك استوجب رفض الطعن "[3]، و جاءت بذات المبدأ في قرار اخر ما يلي : " من المقرر قانونا أنه يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك ، و من ثم فان القضاة بما يخالف هذا المبدأ يعد خرقا للقانون ، و لما كان الثابت

---

[1] هلال أمنة، الإثبات الجنائي بالدليل الالكتروني، مذكرة مكملة من مقتضيات شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي، جامعة محمد خيضر، بسكرة ،2014، ص 28.

[2] أنظر المادة 212 من الأمر 155/66.

[3] المحكمة العليا الجزائرية، قرار صادر بتاريخ 1987/06/30 الملف رقم 50971 المجلة القضائية، العدد 3، لسنة 1991، ص 199.

في قضية الحال أن قضاة الاستئناف ناقشوا أدلة الإثبات و أوجه دفاع المتهم و اقتنعوا بعدم صحة دفاعه فيما يخص النكران للتهمة المنسوبة إليه علما أن الجريمة لم تكن من الجرائم التي ينص فيها القانون على إثباتها بنص خاص يكونوا قد طبقوا القانون تطبيقا سليما ، و من كان الأمر كذلك استوجب رفض الطعن "[1].

ب. الأساس القانوني لمبدأ الاقتناع القضائي:

حرصت الكثير من التشريعات على جعل مبدأ الاقتناع القضائي عنوان للإثبات الجنائي حيث يستند إليها القاضي في حكمه، فقد أقر المشرع الجزائري ذلك في قانون الإجراءات الجزائية على مبدأ الاقتناع الشخصي للقاضي الجزائي وجسده بنصوص واضحة وهذا ما أوردته المادة 307 من قانون الإجراءات الجزائية يتلو الرئيس قبل مغادرة قاعدة الجنايات التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان في غرفة المداومة ".

كما تطرقت إليه المادة 1/212 من نفس القانون الذي يتضمن توجيه القسم من الرئيس إلى المحلفين فيما يخص إجراءات انعقاد محكمة الجنايات،[2] كما نصت المادة 1/427 من قانون الإجراءات الجزائية الفرنسي، فيما عدا الحالات التي ينص عليها القانون خلاف ذلك تثبت الجرائم بكل وسائل الإثبات ويقضي القاضي بمقتضي اقتناعه الشخصي.

ثانيا: نطاق تطبيق مبدأ الاقتناع القضائي

ثار خلاف حول المجال الحقيقي لتطبيق مبدأ الاقتناع القضائي، سواء من حيث طبيعة القضاء أو من حيث مراحل الدعوى الجنائية.

1. بالنسبة للأولى:

يمتد تطبيق مبدأ القضاء إلى كافة أنواع المحاكم الجنائية، وإن كان المشرع الجزائري لم يحدد ذلك بصراحة في المواد المقررة لهذا المبدأ بخلاف المشرع الفرنسي فقد صرح ذلك بصراحة، حيث خصصت المادة 1/353 من قانون الإجراءات الجزائية لتطبيق المبدأ أمام الجنايات، كما نصت المادة 427 من ذات القانون على تحقيق هذا المبدأ أمام محكمة الجنح، أما المادة 536 من نفس القانون فهي مخصصة لمحاكم المخالفات[3].

[1] المحكمة العليا، قرار صادر بتاريخ 1991/01/29 الملف رقم 70690 المجلة القضائية العدد الثالث، لسنة 1991، ص 1991.

[2] محمد مروان، نظام الإثبات في القانون الوضعي، د ن، ديوان المطبوعات الجامعية الجزائر، 1999، ص 427.

[3] عائشة بن قارة مصطفي، المرجع السابق، ص 242.

2. بالنسبة للثانية:

إذا كان مبدأ الاقتناع القضائي، شرع أصلا لكي يطبق أمام قضاء الحكم، ذلك لا يعني أبدا أن نطاق تطبيقه مقصور على هذه المرحلة، بل هو يمتد كذلك ليشمل مرحلة التحقيق الابتدائي، ويستخلص ذلك في أحكام المادة 162 من قانون الإجراءات الجزائية " يمحص قاضي التحقيق الأدلة وما إذا كان يوجد ضد المتهم دلائل مكونة لجريمة من جرائم قانون العقوبات ".

حيث هذا المبدأ يطبق أما قضاة التحقيق ، فهم يقدرون مدى كفاية الأدلة و عدم كفايتها دون الخضوع لقواعد معينة ، أو لرقابة المحكمة العليا ، و لكن يخضعون في ذلك لضمائرهم و إقناعهم الذاتي ، أما قضاة الحكم فهم يقدرون مدى كفاية الأدلة أو عدم كفايتها ، دون الخضوع لقواعد معينة ، أو لرقابة المحكمة العليا، ولكن يخضعون في ذلك لضمائرهم و اقتناعهم الذاتي ، أما قضاة الحكم فهم يقدرون الأدلة من حيث كفايتها أو الإدانة و بذلك يمكننا القول أن الأولى تسمي بترجيح الظن أما الثانية إلى توكيد اليقين و يترتب على ذلك نتيجة هامة ، و هي أن تسلك في مرحلة الاتهم ضده و بينما يكون لصالحه في مرحلة الحكم[1].

الفرع الثاني

ضوابط الاقتناع بالدليل الالكتروني في الإثبات الجنائي

منح المشرع الجزائري للقاضي الجزائي سلطة واسعة في تقديره للأدلة المطروحة أمامه بما في ذلك الدليل الالكتروني، فله أن يبحث ويتحرى الحقيقة بكافة الأدلة، فهو غير ملزم بإصدار حكم الإدانة أو البراءة لوجود معين طالما أنه لم يقتنع به، وذلك عملا بمبدأ الاقتناع الشخصي.

أولا: الضوابط التي تتعلق بمصدر الاقتناع

إن الضوابط التي قد تحكم اقتناع القاضي الجنائي بالدليل الالكتروني اي الضوابط المستوحاة من هذا الدليل في حد ذاته، وهما ضابطين مهمين الأول يكون الدليل الالكتروني قد طرح في الجلسة للمناقشة.

1. ضابط أن يكون الدليل الالكتروني مقبولا

وهذا الضابط مكمل لقيد مشروعية الدليل الالكتروني المقبول في الدعوى، الذي يتم الحصول عليه بطريقة مشروعة، فالقاضي الجزائي حر في تقدير الدليل الالكتروني المقبول في الدعوى، الذي يتم الحصول عليه بطريقة مشروعة، ولهذا فان مسألة قبول هذا الدليل الالكتروني لابد أن تحظي بالأهمية

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 267.

لاعتبارها ركيزة في مبدأ حرية القاضي الجزائي في تقدير الدليل الالكتروني، لأن محل هذه الحرية هو الأدلة المقبولة، فالتطبيق الحسن للقانون يفرض على القاضي أن يكون اقتناعه من دليل الكتروني مقبول ويستبعد في المقابل جميع الأدلة الالكترونية غير المقبولة، لأنه من غير المعقول أن، تكون عنصر من عناصر اقتناعه وتقديره[1].

2. ضابط ضرورة طرح الدليل الالكتروني في الجلسة للمناقشة:

إن الأسس التي تقوم عليها الأدلة أن القاضي لا يمكن أن يباشر سلطته في تقدير هذه الأدلة، ما لم تطرح في الجلسة وبحضور الخصوم تتم مناقشتها، والغاية من هذا الضابط أن يتاح لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة ضده، وكذا يبين موقفه منها.

زيادة على ذلك من مقتضيات هذا الضابط، أن يتم عرض هذه الأدلة في جلسة المحاكمة وتطرح للمناقشات، فالشاهد يدلي بشهادته والمتهم يذكر اعترافه، وأيضا يقرأ تقرير الخبير[2].

فهذه القاعدة تعني أن القاضي لا يجوز أن يؤسس اقتناعه إلى عناصر الإثبات التي طرحت في جلسات المحكمة، وخضعت لحرية مناقشة أطراف الدعوى إعمالا لمبادئ المحاكمة الجزائية، المتمثلة في مبدأ الشفوية ويقصد بشفوية المحاكمة أو المرافعة أن يجري شفويا و بصوت مسموع للكافة كل ما يتم من إجراءات في الجلسة ومبدأ العلنية يقصد به أن تكون جلسات القضاء مفتوحة للجميع من المعنيين بالخصومة وغير المعنيين بها، فيجوز للجميع متى كانت الجلسة علنية حضور المرافعات و سماع الحكم، و هذا ما يجعل عمل القاضي يتم في شفافية ووضوح أمام الجميع وهذا ما ذهبت إليه المادة 07 من قانون الإجراءات المدنية والإدارية [3]وكذا مبدأ الوجاهية ويقصد به اتخاذ كافة الإجراءات في مواجهة الخصوم بطريق يمكنهم من العلم بها سواء عن طريق إجرائها في حضورهم أو عن طريق إعلانهم بها أو تمكينهم من الاطلاع عليها ومناقشتها إلزام يقع على الخصوم والقاضي على حد سواء أو هذه المناقشة عليها أن تأخذ بعين الاعتبار ضرورة احترام حقوق الدفاع بإعطاء فرصة للمتهم للاستفسار حول كل وسيلة من وسائل الإثبات المقدمة أمام القضاء الجزائي هذا من جهة ومن جهة أخرى يتعين توافر المناقشة الحضورية لأنها تعتبر مطلبا منطقيا وتنطوي على فحص شامل وجماعي لكل وسيلة إثبات .

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 268.

[2] فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الجزائر، 2008، ص ص 250 251.

[3] أنظر المادة 07 من قانون الإجراءات المدنية والإدارية.

ومنه فانه من القواعد الأساسية في الإجراءات، أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة ، وهو ما يسمى وضعية الدليل الجزائي بصفة عامة و الدليل الالكتروني بصفة خاصة ، والمعنى لهذا الضابط أن يكون الدليل في أوراق الدعوى و إتاحة الفرص للخصوم للاطلاع عليه و مناقشته ، وكلا الأمرين يتحتم توافرهما، ولا يختلف الأمر بالنسبة للدليل الالكتروني، سواء كان على شكل بيانات معروضة على شاشة الكمبيوتر، أو مدرجة في حاملات البيانات، أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مستخرجة في شكل مطبوعات ، كل هذا عليه أن يكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة[1]. وضابط وضعية الدليل الالكتروني يقوم على عنصرين أساسيين، يتمثل الأول في إتاحة الفرصة للخصوم للاطلاع على الدليل الالكتروني والرد عليه، والعنصر الثاني يتمثل في أن يكون الدليل الالكتروني أصل أوراق الدعوى.

1. العنصر الأول:

أنه يجب على القاضي مبدئيا أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم، وهذا حتى يكونوا على بينة مما يقدم ضدهم من أدلة تعرض تمكينهم من مواجهة هذه الأدلة والرد عليها، وهذا احتراما لحقوق الدفاع، الذي يعد أحد المظاهر الأساسية لدولة القانون والنظم الديمقراطية، ويتيح مبدأ الوجاهية تجسيد هذا الأخير، حيث يقتضي مبدأ الدفاع حضور كل خصم في الدعوى وأن يطلع خصمه على ما لديه من أدلة، وأن يواجهه بها وأن يناقش أدلة الطرف الأخر ومبدأ الوجاهية يجب أن تتوافر فيه نوعين من الضمانات:

أ. الضمانة الأولى: تكون سابقة على عملية المواجهة ذاتها بين الأطراف في الجلسة، وهو يتضمن ضرورة إحاطة المتهم علما بالتهمة المنسوبة إليه، وأن يمنح الوقت والوسائل اللازمة لتحضير دفاعه، وأن يسمح له بالاستعانة بمترجم عن الاقتضاء.

ب. الضمانة الثانية: وهي أثناء عملية المواجهة ذاتها لأنها أكثر تأثيرا في الدعوى العمومية، إذا انه يقدم كل طرف ما لديه من مستندات، ويتم سؤال الشهود والخبراء وان يطلب اتحاد اي اجراء يقدر فائدته واثارة اي دفوع او ايداع اي مذكرات، تم حق لكل طرف في مناقضة تقدير الخبير وما ورد به[2].

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 271، 269.

[2] هلال أمنة، المرجع السابق، ص 109.

ولهذا لا يجوز للقاضي الجزائي ان يبني اقتناعه على دليل قدمه أحد أطراف الدعوى الا إذا عرض هدا الدليل في جلسة المحاكمة بحيث يعلم به سائر الاطراف، اذ ان العدالة تقتضي ان يأتي حكم القاضي بعد مناقشة هادئة، ومجادلة حرة متكافئة من كل صاحب حق مشروع في الدعوى.

2. العنصر الثاني: يتمثل في ان يكون للدليل الالكتروني أصل في اوراق الدعوى، وهذا حتى يكون اقتناع القاضي الجزائي مبنيا على اساس.

ومن أجل ذلك، أوجب المشرع تحرير محضر جلسة إثبات وقائع الدعوى الجزائية، واناط بهذه المهمة القاضي الجزائي، بصفته قاضي الموضوع، أو اي شخص من الخصوم له مصلحة في الرجوع الى هدا المحضر خاصة في حال ما إذا رغبو في التأكد او طلب التوضيح بشأن ما دار من وقائع اثناء الجلسة. ويعد هدا الاجراء ضمانة فعالة من طرف القضاة الجزائيين لتكريس العدالة، وذلك بتمكين المحكمة العليا لممارسة رقابتها القانونية على الاحكام المطعون فيها، من حيث صحة التقدير والتسبيب ومدى مراعاتها للقانون[1]، ويترتب على ضابط طرح الدليل الالكتروني الجلسة لمناقشة نتائج اهمها عدم جواز ان يقضي القاضي الجزائي بناءا على علمه الشخصي أو رأي غيره.

- ضابط جواز أ يقتضي القاضي الجزائي بناءا على علمه الشخصي:

وهذا يعني أن المعلومات الشخصية التي يحوزها القاضي والتي يمنع عليه القضاء الاستناد إليها، هي معلومات تتصل بصورة أو بأخرى بالدعوى التي ينظر فيها ومن الممكن أن تتأثر على تقدير أدلتها ذلك لأنها لم تحصل بالطريق الذي رسمه القانون وهو أن يكون لها أصل في الأوراق، ويرجع أساس هذه القاعدة الى ثلاث أمور:

- أنه يترتب على حق الدفاع أي أن المعلومات الشخصية التي يستند عليها القاضي تعد في الحقيقة مفاجأة للخصوم في حالة ما إذا لم تناقش بمعرفتهم ولم يتم إثباتها في إطار اجراءات الخصومة.

- أن ما شهده القاضي أو علمه أو سمعه يتصل بوقائع الدعوى سوف يؤثر حتما في تقديره للأدلة وفي هذه الحالة يصلح لأن يكون شاهدا في أن واحد، ولهذا ينص في القانون على أن يكون القاضي الذي سبق أن شهد في قضية ما لا يصلح أن يكون فيها قاضيا[2].

- يجوز للقاضي أن يستند الى المعلومات العامة التي يفترض بالكل أن يعلم بها والتي يكتسبها القاضي من خبرته وثقافته العامة، حيث لا يلزم المحكمة قانونيا بيان الدليل عليه فما ينبغي الاشارة اليه أن هذه

[1] عائشة بن قارة مصطفى، المرجع لسابق، ص 271 272.

[2] فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة لنشر والتوزيع، الأردن،2006 ص 259

القاعدة يجب ألا تتعارض مع الدور الإيجابي للقاضي في البحث عن الحقيقة أو مع حريته في الاستعانة بكافة الوسائل للإثبات طالما أنه يقوم بطرح الأدلة المتحصل عليها للمناقشة بين أطراف الدعوى، فالحضر يقع على المعلومات التي يستقيها القاضي بصفته الشخصية، وليس بصفته القضائية هذه القاعدة يرد عليها استثناء وهو أنه يجوز للقاضي أن يحكم بما رأه وسمعه في حالة ارتكاب الجريمة في الجلسة، أي جرائم الجلسات وهذا ما نصت عليه المادة 569 من قانون الاجراءات الجزائية[1].

- **عدم جواز أن يقضي القاضي الجزائي بناءا على رأي غيره**

ان القاضي لا يبني اقتناعه على رأي غيره الا إذا كان هذا الغير من الخبراء وارتاح ضميره الى التقرير المحرر منه، فقد يقرر الاستناد اليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة أمامه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناءا عليه يكون متولدا من عقيدته هو وليس من تقرير الخبير[2].

فلا يمكن أن يعول القاضي الجزائي على رأي الغير بل يجب أن يستمد هذا الاقتناع من مصادر يستقيها بنفسه من التحقيق في الدعوى، ولا يجوز له أن يحيل الحكم في شأن واقعة الدعوى ومستنذتها الى دعوى أحرى غير مطروحة أمامه أو أن يعتمد على وقائع استقاها من محاضر قضية أخرى لم تكن ضمن الدعوى التي ينظمها، وألا يخضع الى أي تأثير خارجي مثلا تأثير رجال الصحافة أو الفقهاء ورجال الدين، لأن الاثبات في المواد الجزائية يقوم على اقتناع القاضي نفسه بناءا على ما يجري في الدعوى من تحقيق يستقي القاضي منه دعوته[3].

ثانيا: الضوابط التي تتعلق بالاقتناع بحد ذاته

1. ضابط بناء الاقتناع القضائي على اليقين:

اليقين القضائي هو اعتقاد القاضي بأن ما وصل إليه هو الحقيقة والوصول الى اليقين يتم عن طريق ما يستنتجه وسائل الإدراك المختلفة من خلال وقائع الدعوى، وما يرتبه من تصورات في ذهنه ذات درجات عالية من التأكيد[4].الأصل في الإنسان البراءة وهو شرط اليقين في أحكام الادانة شرط عام، سواء كانت هذه الأدلة تقليدية أو مستحدثة، لأن القاعدة العامة تبنى على الجزم واليقين ولا تبنى على الظن و الاحتيال، كالجريمة الالكترونية بحيث يقتنع القاضي اقتناعا يقينيا بارتكابها ونسبتها للمتهم، ويشترط على القاضي أن

[1] أنظر المادة 569 من الأمر 155/66.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص 275

[3] بلولهي مراد، المرجع السابق ص 117

[4] عائشة بن قارة مصطفى، المرجع نفسه، ص 277

يكون مقتنعا تماما بالدليل المقدم ولا يبقى لديه أي شك معقول في صحة القرار وهذا ما أكدته المادة353 من قانون الاجراءات الجزائية التي تنص على: "يجب على المحكمة أن تكون مقتنعة بالدليل المقدم لكي تتخذ قرارها "[1].

2.ضابط ملائمة الاقتناع القضائي لمقتضيات العقل والمنطق:

ان هذا الأمر مشروط بأن يكون استنتاج القاضي للحقيقة الواقعة وما كشف عنها من أدلة لا يخرج عن مقتضيات العقل والمنطق عند تقييم الأدلة واتخاد القرار، ومع ذلك تجدر الاشارة الى تقيد القاضي الجنائي عند تقديره لضوابط معينة سواء كانت متعلقة بالدليل ذاته أو متعلقة بالاقتناع، وتكمن الاهمية من هذا الضابط هو ضمان العدالة وتعزيز الثقة في القضاء، وهذا حسب المادة 353 من قانون الإجراءات الجزائية.

خلاصة:

ومن هنا نستخلص من هذا الفصل أن المشرع قد حاول تكييف القواعد العامة للتحقيق مع خصوصية هذا النوع من الجرائم، التي تتسم بالتعقيد التقني وسرعة طمس الأدلة. فقد تم منح الضبطية القضائية صلاحيات خاصة في هذا المجال، تمكنها من تتبع أثر الجريمة وجمع الأدلة الإلكترونية وفق إجراءات دقيقة مع مراعاة للضمانات القانونية.

[1] أنظر الى المادة 353 من الأمر 155/66.

أما فيما يخص حجية الأدلة الإلكترونية فإن المشرع لم يفرد لها تنظيما خاصا شاملا، بل أدمجها ضمن الإطار العام لقواعد الإثبات، ممالا يطرح إشكالات علمية تتعلق بمدى قبولها أمام القضاء ومدى قوتها في الإثبات مقارنة بالأدلة التقليدية.

خاتمة

خاتمـة:

بعد إتمام هذه الدراسة بفضل الله وتوفيقه حول موضوع " **الإثبات في الجريمة الالكترونية في التشريع** فيها صعب المنال، لاعتبار أدلتها الرقمية حفية وغير مرئية، حيث ظهر قصور كبير في النصوص الجنائية الموضوعية لذلك وجد الكثير من الإشكالات في التطبيق خاصة جانب التحقيق والإثبات فهناك مشاكل متعلقة بجمع الأدلة ومشاكل متعلقة بالقانون.

لذلك فقد اهتم المشرع الجزائري على مواكبة النهضة التكنولوجية والمعلوماتية، فسعى لسد الفراغ التشريعي بقانون العقوبات الجزائري وذلك بتعديله بموجب قانون رقم 04_15 وتعديل قانون الإجراءات الجزائية بموجب قانون 06_22واصدار قانون خاص والمتمثل في قانون رقم09_04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالرغم من هذه المحاولات يبقى المشرع الجزائري بعيد عن التطور القانوني على المستوى العالمي.

وعليه وبناء على ما سبق، تطلب الأمر أن نتقدم بنتائج ما وصلنا إليه من خلال هذا الجهد المتواضع الذي قمنا به في سبيل التصدي لموضوع شديد الحساسية وفي حاجة دائمة للدراسة والتحليل بفعل ارتباطه بالتطور المستمر لتكنولوجيا المعلومات، ويمكن بلورة هذه النتائج فيما يلي:

النتائـج:

- إن الجرائم الإلكترونية ظاهرة جديدة وخطيرة وهي تمثل الوجه السلبي للثورة المعلوماتية والتطور التكنولوجي كونها تتخذ نظام الحاسوب كوسيلة لها. وأن صعوبة الحصول على الدليل في الجريمة الإلكترونية يظل من الصعوبة بمكان وأن الإجراءات التي أقرها المشرع الجزائري في هذا المجال بموجب أحكام القانون 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تعد غير كافية.

- ارتباط الجريمة الإلكترونية بالتقنية المعلوماتية، جعل منها جرائم ذات طبيعة خاصة تتميز عن غيرها من الجرائم التقليدية، سواء من حيث الماهية أو من حيث مرتكبها أو من حيث ضحاياها.

- تبين أن البحث عن الدليل الإلكتروني عبارة عن معلومات ذو طبيعة ديناميكية فائقة السرعة تتنقل من مكان لآخر عبر شبكات الاتصال المتعددة، ومن السهولة أن يتم إتلافه في أي لحظة.

- وجود عدة عوائق لإثبات الجريمة الإلكترونية، منها ما يتعلق بالجريمة ذاتها ومنها ما يتعلق بأدلتها ومنها ما يتعلق بالعامل البشري.

– إن إثبات الجرائم الإلكترونية، أصبح يستدعي إعداد البرامج التدريبية المتخصصة والكفيلة بتلقين الجهات القائمة على إثبات الجريمة الإلكترونية. كفنيات البحث والتحري، التحقيق والحكم في هذا النوع المستحدث من هذه الجرائم.

– ضبط وتحرير الآثار الجنائية الرقمية ونقلها بالطريقة العلمية الصحيحة وهذا ما يستلزم التعاون الكامل بين رجال الضبط القضائي وقاضي التحقيق والخبير من أجل نجاح عملية ضبط الجريمة.

– الشك في الدليل الإلكتروني لا يتعلق بمضمونه كدليل، وإنما يتعلق بعوامل مستقلة تؤثر في حجيته.

التوصيات:

وعلى ذلك يمكن القول أن مجمل ما توصل إليه من خلال هذه الدراسة، أن قواعد الإثبات التقليدية قاصرة على إثبات الجرائم الإلكترونية، وأن الفكر الأمني والقضائي غير ملائم لعملية الإثبات، بل أصبح الأمر يحتاج إلى رجل أمن معلوماتي، ومحقق معلوماتي، وقاضي معلوماتي. لهذا سنقوم بختم هذه الدراسة بمجموعة من التوصيات، لعلها تساهم ولو بقدر ضئيل في جل بعض المشكلات التي استنتجناها من هذه الدراسة.

وتتمثل هذه التوصيات فيما يلي:

– وجوب الاهتمام والعمل على تكوين الخبراء والمحققين والقضاة من أجل التعامل مع الجرائم الإلكترونية.

– التركيز على تطوير الوسائل التقنية باستمرار للتمكن من التحليل الجيد والنسخ المناسب للمحتويات من الأقراص وتخزين البيانات.

– وجوب النص صراحة على الأدلة الإلكترونية كأدلة إثبات في المجال الجنائي والاعتراف لها بجدية قاطعة باعتبارها استثناء على سلطة القاضي الجنائي في تقدير الدليل.

– تطوير النظرة الاستشرافية في مكافحة الجريمة الإلكترونية من خلال تفعيل التعاون الدولي لمواجهة هذه الجرائم بالأخص من خلال ربط الاتفاقيات والمعاهدات الدولية التي تجرم صور هذه الجرائم وبصفة هذه الجرائم وبصفة موحدة ليسهل اتخاذ موقف موحد منها.

– الاستفادة من تجارب وخبرات الدول المتطورة في مجال مكافحة الجرائم الإلكترونية أو العمل على استعمال الآليات الوقائية قبل وقوع الجريمة، خاصة عندما يتعلق الأمر ببعض الجرائم الإلكترونية التي تهدد أمن الدولة مثل الإرهاب الإلكتروني أو التجسس الإلكتروني.

– على المشرع الجزائري الإشارة أو وضع استثناء خاص بوقت التفتيش ضمن القانون رقم 09_04، وعليه إدراج تفتيش الأشخاص وتحديد كيفية وشروط إجرائه ضمن قانون الإجراءات الجزائية.

– على المشرع الجزائري أيضا إدراج إجراء الاعتراف والشهادة والاستجواب ضمن قانون 09_04 من أجل اعتماد القاضي عليها الفصل في الدعوى بالرغم من أن لهذه الإجراءات دور ضئيل في مجال المعلوماتية.

– توجيه الجهود نحو التوعية بمخاطر الجرائم الإلكترونية، مع إبراز الأساليب التي يعتمدها المجرمون في ارتكابها، من خلال استخدام وسائل الإعلام المختلفة.

– تشجيع التعاون الدولي مع الدول المتقدمة في مجال الجرائم الإلكترونية لتبادل الخبرات والتقنيات، والاستفادة من النظم القانونية المتقدمة.

– تنظيم دورات تدريبية وتأهيلية للكوادر القضائية والأمنية لتطوير مهاراتهم في التعامل مع الأدلة الرقمية والتقنيات الحديثة.

وهكذا يكون البحث قد اكتمل بحمد الله، فإن كان فيه الحسن والصواب فهو من الله سبحانه وتعالى، وإن كان فيه النقص فهو منا، ولما لا فنحن بشر نجتهد ونخطأ ونصيب، فإن أصبنا فأجرنا على الله وإن أخطأنا فندعوه ألاّ يحرمنا أجر المجتهدين.

تم بحمد الله.

قائمة المراجع

أولا: المصادر

1. القرآن الكريم

- الآية 45 من سورة الفرقان.

2. النصوص القانونية

أ. النصوص التشريعية:

- **الأوامر والقوانين:**

1. الأمر رقم 66_156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 الذي يتضمن قانون العقوبات المعدل والمتمم.

2. الأمر رقم155/66 من قانون الإجراءات الجزائية المؤرخ في 8 يونيو 1966، يعدل ويتمم القانون 22/06 المؤرخ في 20 ديسمبر 2006 الجريدة الرسمية عدد 84 في تاريخ 2006/12/24.

3. القانون رقم 09_04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

4. القانون رقم 10_05 المؤرخ في 5 رمضان عام 1431 الموافق 15 عشت سنة 2010 يعدل ويتمم الأمر رقم 03_03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بالمنافسة.

5. القانون رقم06_18 المؤرخ 25 رمضان 1439 الموافق ل 10 يونيو سنة 2018 يعدل ويتمم 66_15 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

ب. الأحكام والقرارات القضائية:

1. قرار المحكمة العليا الجزائرية صادر بتاريخ 1987/06/30 الملف رقم 50971 المجلة القضائية العدد الثالث، سنة 1991.

2. قرار المحكمة العليا صادر بتاريخ 1991/01/29 الملف رقم 70690 المجلة القضائية العدد الثالث سنة 1991.

ثانيا: المراجع

1. الكتب:

1. ارتاس نذير وآخرون، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، الطبعة الأولى المركز المغاربي – شرق أدنى للدراسات الاستراتيجية، 2024.

2. الأسدي لينا محمد، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار حامد، الأردن، د س ن.

3. الأشقر منى، القانون والأنترنت تحدي التكيف والضبط، بيروت المكتبة المصرية، 2011.

4. اقبلي امحمد والعمراني الميلودي عابد، "القانون الجنائي الخاص المعمق في شروح"، الطبعة الأولى، مكتبة الرشاد سلطات للنشر والتوزيع، د.ب.ن،2020.

5. أوشن حنان، وادي عماد الدين، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2015.

6. بلعيات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007.

7. بن عبد الله السند عبد الرحمن، الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات، ط1، دار الأوراق للطباعة والنشر والتوزيع، لبنان، 2004.

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

9. بوكر رشيدة، جرائم الاعتداء على نزم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2012

10. الجوخدار حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع الأردن 2008.

11. الحلبي خالد عباد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011.

12. حنيفي حازم محمد، الدليل الإلكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1988.

13. الشوا محمد سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994.

14. صليبا جميل، المعجم الفلسفي المصطلحات القانونية، الجزء الأول، دار الكتاب اللبناني، بيروت، الطبعة الأولى، 1982.

15.عبد الباقي الصغير جميل، أدلة الاثبات الجنائي والتكنولوجي الحديثة، دار النهضة العربية، القاهرة 2022.

16.فقي حسين سامي جلال، الأدلة المتحصلة من الحاسوب وحجبتها في الاثبات الجنائي، دار الكتب القانونية مصر 2012.

17.قنديل أشرف عبد القادر، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية 2015.

18.محمد زيدان، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة لنشر والتوزيع،

19.محمود حسني نجيب، النظرية العامة للقصد الجنائي، الطبعة السابعة، دار النهضة العربية، 1974.

20.محمود حسني نجيب، شرح قانون العقوبات (القسم الخاص)، الطبعة الأولى، دار النهضة العربية، مصر، 1988.

21.مروان محمد، نظام الإثبات في القانون الوضعي، د. ن، ديوان المطبوعات الجامعية الجزائر، 1999

22.ممدوح إبراهيم خالد، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، 2018.

23.منصور محمد حسين، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، مصر، 2006.

24.موسى مصطفى محمد، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة الطبعة الأولى، 2008، ص 208.

25.المومني نهلا عبد القادر، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، 2008.

26.يوسف أمير فرج، الجرائم المعلوماتية على شبكة الأنترنت دار المطبوعات الجامعة الإسكندرية 2008.

ثالثا: الأطروحات والمذكرات:

1.برمش مراد، خصوصية الجريمة الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 1، 2020-2021.

2.بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، مسيلة، 2008.

3.عبد العال أسامة حسين محي الدين، حجية الدليل الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والاقتصادية، العدد 76، جوان 2021.

4.قارة أمال، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستر في القانون، كلية الحقوق، جامعة الجزائر، 2001.

5. مرعي إسراء جبريل رشاد، الجريمة الإلكترونية "الأهداف –الأسباب–طرق الجريمة ومعالجتها"، مجلة الدراسات الإعلامية، المركز الديمقراطي، العدد 1، 2018.

ثالثا: المقالات والمجلات

1. إبراهمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، فرع الملكية الفكرية، جامعة الجزائر 1، بن يوسف بن خده كلية الحقوق، الجزائر 2021/2020.

2. أمنة هلال، الإثبات الجنائي بالدليل الالكتروني، مذكرة مكملة من مقتضيات شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي، جامعة محمد خيضر، بسكرة 2014.

3. أوهايبية عبد الله، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للنشر والتوزيع الجزائر 2008.

4. بستان كرام غانم، نطاق الدليل الإلكتروني في الإثبات الجنائي، مجلة الجامعة العراقية، العدد 04، فيفري 2025.

5. بلعابد عيدة، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق علمية، جامعة سعيدة، المجلد 11، العدد 1، 2019.

6. بلعابد عيدة، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، جامعة مولاي الطاهر، سكيكدة، العدد 06، 2011.

7. بن حميد المعمري مسعود، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس 9، العدد 3، أكتوبر 2018.

8. بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه مقدمة لنيل شهادة دكتوراه علوم في القانون، جامعة مولود معمري–تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، 23 جانفي 2019.

9. بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجيستر في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012–2013.

10. حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق جامعة باتنة سنة 2016.

11. دوادي نعيمة، الجريمة الإلكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها)، مجلة مهد اللغات، جامعة على لونيسي–البليدة (الجزائر)، المجلد 2، العدد 1، 2020.

12.الديربي عبد العال، الجرائم الكترونية، دراسة قانونية قضائية مقارنة، طبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.

13.ديش سورية، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، جامعة جيلالي ليابس سيدي بلعباس الجزائر، العدد 1، 2018.

14.زيدان محمد فاضل، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى. دار الثقافة للنشر والتوزيع، الجزائر، 2008.

15.سالي وسام، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة ماجيستير، جامعة الجزائر، 2019.

16.سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة لنيل شهادة الماجيستر، جامعة الحاج لخضر–باتنة، كلية الحقوق والعلوم السياسية، 2013.

17.سلامة نسرين سيد، الجرائم الإلكترونية وأثرها على المجتمع الجزائري، مجلة القاهرة للخدمة الاجتماعية، كلية الآداب جامعة المنصورة، العدد 39، 2023/06.

18.الشعار خالد علي نزل، التحقيق الجنائي في الجرائم الالكترونية، رسالة لنيل شهادة الدكتورة في الحقوق، جامعة المنصورة

19.شعلال نوال، سلطة القاضي الجنائي في تقدير الأدلة، مذكرة لنيل شهادة الماجيستير فرع قانون العقوبات والعلوم الجنائية جامعة سكيكدة 2008.2009.

20.الشكري عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة 2008، العدد 7.

21.صغير يوسف، التفتيش كألية لإثبات جرائم نظم المعلوماتية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، المجلد 16، العدد 04، 2021.

22.عبد القادر أيت عبد المالك فلاح، نادية التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2019.

23.عبد الكريم نعمان، الجرائم الإلكترونية وموقف المشرع الجزائري منها، رسالة لنيل شهادة الماجيستر في القانون الجنائي، جامعة الجزائر 1، يوسف بن خدة، 2017/2016.

24.عبد المنعم محمد صلاح محمد، الجرائم الإلكترونية وتحدياتها، دراسة مقارنة رسالة دكتوراه كلية الحقوق، جامعة المنصورة 2005، ص 234:

25.عثماني عزالدين، إجراءات التفتيش والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، جامعة تبسة العدد 4 جانفي 2018.

26. عمارة فوزي، قاضي التحقيق في قانون الإجراءات الجزائية الجزائري، رسالة لنيل شهادة دكتوراه في العلوم القانونية، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009-2010.

27.عمارة فوزي، قاضي التحقيق في قانون الإجراءات الجزائية الجزائري، رسالة لنيل شهادة دكتوراه في العلوم القانونية، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009-2010.

28.عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان، 2021.

29.غازي سليمان، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، رسالة ماجيستر، جامعة نايف للعلوم الأمنية، السعودية، 2010.

30.فلاك مراد، اليات الحصول على الأدلة الرقمية كوسائل اثبات في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، العدد الخامس، جامعة ثليجي، الأغواط، 2019.

31.قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة لنيل شهادة الدكتوراه قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة الجزائر، 2014.

32.قناش نورة، مذكرة بيداغوجية في مقياس: الجرائم المستحدثة، موجهة لطلبة السنة الثانية ماستر علم اجتماع الجريمة والانحراف، جامعة سكيكدة، السنة الجامعية 2020-2021.

33.لعوارم وهيبة، الدليل الرقمي في مجال الإثبات الجنائي وفقا للتشريع الجزائري، المجلة الجنائية القومية، كلية الحقوق، جامعة بجاية، المجلد 7، العدد 2، جويلية 2014[1]

34.مستاري عادل، دور القاضي الجزائي في ظل مبدأ الاقتناع القضائي، مجلة المنتدى القانوني العدد الخامس، جامعة محمد خيضر بسكرة،2018.

35.مصطفى خالد حامد أحمد، المعلوماتية والمسؤولية الجزائية، مجلة الفكر الشرطي، مركز بحوث الشرطة القيادة العامة لشرطة الشارقة الإمارات، المجلد رقم 20 العدد 79، أكتوبر 2011، ص 174.

36.المطيري سعد فهد الدبيس، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية، العدد 2.

37.المطيري سعد فهد الدبيس، مفهوم الجرائم الإلكترونية وسماتها، مجلة متخصصة في الدراسات والبحوث القانونية، المجلد 16، العدد 5، 2023.

38.مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية جامعة محمد لمين دباغين سطيف2، المجلد 6، العدد 02،2 /2022/11.

39.مولاي براهيم عبد الحكيم، **الجرائم الإلكترونية**، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة الجزائر، المجلد 2، العدد 23، 2015/06.

40.هوام علاوة، التسرب كألية للكشف عن جرائم في القانون الجزائري، مجلة الفقه والقانون، العدد الثاني، كلية الحقوق والعلوم السياسية والقانون، جامعة الحاج لخضر – باتنة 2012.

رابعا: المداخلات العلمية والمؤتمرات

1.ارتس نذير وآخرون، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، المملكة المتحدة: المركز المغاربي–شرق أدنى للدراسات الاستراتيجية، 2024.

2.بوزينة آمنة أحمد، إجراءات التحري الخاصة في مجال مكافحة الجرائم، مداخلة مشارك بها في الملتقى الوطني حول آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، 2007.

3.حسين محمد عبد الله، إجراءات جمع الأدلة في الجريمة المعلوماتية مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 26–28 أفريل 2003.

4.رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، 24_25 مارس 2017.

5.عبد المنعم نبيل، جرائم الحاسب الآلي، بحث منشور، ندوة المواجهة الأمنية للجرائم المعلوماتية، دبي، مطبعة بن دسمال، عام 2005.

6.المطرودي مفتاح بوبكر، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 2012/25/23.

فهرس المحتويات

فهرس المحتويات:

فهرس المحتويات:

✍ فهرس المحتويات:

ملخص

ملخص:

تعالج هذه الدراسة موضوع الإثبات في الجريمة الإلكترونية في التشريع الجزائري، باعتباره من المواضيع الحديثة التي فرضها التطور التكنولوجي، وما رافقه من أنماط إجرامية جديدة تتطلب آليات إثبات مغايرة لما هو تقليدي. تهدف الدراسة إلى إبراز مدى فعالية النظام القانوني الجزائري في مواجهة تحديات الإثبات في الجرائم الإلكترونية، ومدى كفاية الوسائل التقنية والقانونية المعتمدة. اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال تحليل النصوص القانونية ذات الصلة، ودراسة التطبيقات القضائية والفقهية. تم جمع البيانات من خلال المصادر التشريعية، والاجتهادات القضائية، والدراسات الأكاديمية المتخصصة. وتوصلت الدراسة إلى أن المشرع الجزائري لا يزال في حاجة إلى تطوير الإطار القانوني للإثبات في الجرائم الإلكترونية، بما يضمن التوازن بين حماية الحقوق والحريات وضمان فعالية الملاحقة الجزائية.

الكلمات المفتاحية: الجريمة الإلكترونية، الإثبات الرقمي، التشريع الجزائري، الإطار القانوني، الإجراءات الجزائية، التطور التكنولوجي، التطبيق القضائي.

Abstract:

This study addresses the issue of evidence in cybercrime under Algerian legislation, as one of the contemporary topics imposed by technological advancement and the emergence of new types of crimes that require different evidentiary mechanisms from traditional ones. The aim of the study is to highlight the effectiveness of the Algerian legal system in confronting the challenges of evidence in cybercrimes, and to assess the adequacy of the adopted technical and legal tools.

The study adopts a descriptive and analytical approach by analyzing relevant legal texts and examining judicial and scholarly applications. Data were collected from legislative sources, judicial precedents, and specialized academic studies. The study concludes that the Algerian legislator still needs to develop the legal framework for evidence in cybercrime cases, in a way that ensures a balance between the protection of rights and freedoms and the effectiveness of criminal prosecution.

Keywords: Cybercrime, digital evidence, Algerian legislation, legal framework, criminal procedure, technological development, judicial practice