الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التكوين العالي والبحث العلمي
جامعة إبن خلدون - تيارت -
كلية الحقوق والعلوم السياسية

مذكرة لنيل شهادة الماستر في شعبة الحقوق
التخصص: القانون الجنائي

بعنوان:

الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية

من إعداد الطالبة:
- قاسم عائشة حنان

تحت إشراف:
د. بوسماحة الشيخ

أعضاء اللجنة	لجنة المناقشة	الصفة
الدكتورة حمر العين مقدم	أستاذ التعليم العالي	رئيسا
الدكتور بوسماحة الشيخ	أستاذ التعليم العالي	مشرفا مقررا
الدكتور كاسيلي أحمد محمد	أستاذ التعليم العالي	عضوا مقررا
الدكتور مبطوش الحاج	أستاذ التعليم العالي	عضوا مقررا

السنة الجامعية: 2025/2024

الإهداء

أهدي ثمرة جهدي إلى التي لا يمكن للكلمات أن توفي حقها، وإلى التي لا يمكن للأرقام أن تحصي فضائلها وإلى من جعل الجنة تحت أقدامها إلى من كانت ملجئي في هذه المرحلة إلى من أبصرت بها طريق حياتي واعتزازي بذاتي إلى من دعمتني في أصعب أوقاتي وعلمتني أن هذه الحياة كفاح وسلاحها العلم والمعرفة إلى أمي التي ربتني وأنارت دربي وأعانتني بالصلوات والدعوات وإلى أبي العزيز رحمه الله واسكنه فسيح جناته والذي عمل بكد في سبيلي وعلمني الكفاح وأوصلني إلى ما أنا عليه، إلى منبع المحبة والحنان وسندي في الحياة زوجي العزيز الذي كان لي نعم الرفيق في مشواري الجامعي وإلى إبنتي قرة عيني أسيل حفظها الله ورعاها وإلى إبنتي الصغيرة سوار الجنة رحمها الله والتي رافقتني منذ بداية مشواري الدراسي وتركتني في آخره وإلى إخوتي وأخواتي وإلى الأصدقاء، إلى أساتذتي الكرام في الكلية وكل عزيز على القلب ولم يذكره اللسان وإلى كل من يبحث للارتقاء بالعلم في كل مكان .

شكـــر وتقديـر

الحمد لله الذي أنار لي درب العلم والمعرفة وأعانني على أداء هذا الواجب ووفقني إلى انجاز هذا العمل، وأمدني بالصبر حتى أتجاوز الصعوبات أمامي ووفقني لانجاز هذه المذكرة.

كما أتقدم بكل معاني التقدير والعرفان بالجميل للأستاذة البروفيسورة طفياني مخطارية كرئيسة والتي قدمت كل الدعم خلال فترة الدراسة وعلى إشرافها على هذا البحث، أسأل الله تعالى أن يجعل لها ذلك في ميزان حسناتها ويجازيها عنا خير الجزاء كما أتقدم بالشكر الخالص والتقدير الفائق إلى الأستاذ الدكتور بوسماحة الشيخ كمشرف والسادة أعضاء اللجنة العلمية الموقرة على تفضلهم بقبول المناقشة،واشكر كل من ساهم و بذل جهدا ولو بالقليل في انجاز هذه المذكر ،وقبل أن نمضي نقدم أسمى آيات الشكر و الامتنان و التقدير و المحبة إلى الذين حملوا أقدس رسالة في الحياة إلى الذين مهدوا لنا طريق العلم و المعرفة إلى جميع أساتذتنا الكرام.

مقدمة

يسعى الإنسان منذ نعومة أظافره إلى الوصول إلى المعرفة والحقيقة اليقينية، هذا كون الضروريات والحاجات ومتطلبات الفرد لا تعرف السكون وهكذا هو طبع الإنسان منذ بداية العصور مرورا بكل مراحل التطور والازدهار وكذا مراحل الانحطاط والتدهور، حيث دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الفكري والمعرفي الهائل غير المعهود.

وذلك بفضل الثورة العلمية التكنولوجية والرقمنة في جميع المجالات خاصة منها مجال الاتصالات والمعلومات التي اقتحمت بقوة هذه المرحلة التي وفرت مناخا خصبا لنهضة علمية تكنولوجية شاملة غير مسبوقة في كافة مجالات الحياة الاقتصادية، الاجتماعية، الثقافية والعلمية، تهاوت أمامها الحدود السياسية والحواجز بين الدول والشعوب ،وضاقت معها الأماكن وتقلصت فيها المسافات، واختزلت وطوت فيها الأبعاد.

بما تتميز به من عنصري السرعة والدقة، مما أهل الحقبة الجديدة بالغة الأهمية أحدثت تأثيرا في بنية المجتمع وذلك لاكتساح جميع النواحي التي تتطلبها الحياة البشرية، مما جعل منها مصدرا أساسيا للأشخاص وكذا المؤسسات للاعتماد عليه في كافة شؤونهم نظرا للسرعة والدقة في تخزين المعلومات ومعالجتها في وقت قصير، حيث في هذه الفترة عرفت المعلوماتية تطورا مذهلا .

كما ساعد اقترانها بالتكنولوجيات أخرى على تعميم استعمالها وتعدد وظائفها، فالحديث اليوم لم يعد عن الحاسوب وقدراته في اختزال الوقت وتخزين المعلومات أو انجاز العمليات المعقدة وإنما عن تكنولوجيا الإعلام والاتصال والفضاء الافتراضي الذي نشا نتيجة ارتباط المعلومات بمختلف المواصلات السلكية واللاسلكية، حيث أصبحت هذه الوسيلة ليست حكرا فقط على الدول المتقدمة، وإنما تعدت إلى غيرها من الدول النامية مما زاد من أهميتها، حيث عرفت بما يسمى بعصر المعلومات الذي أضحت فيه الكرة الأرضية قرية صغيرة تسبح في فضاء الكتروني، وهو ما دعا بالكثير إلى وصف الثورة المعلوماتية، بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في أواخر القرن التاسع عشر.

فهدف الثورة الثانية هي إحلال الآلة محل النشاط الذهني للإنسان لما توفره من الوقت والجهد والتكلفة عن الإنسان لتسهيل حياته اليومية، الأمر الذي أدى إلى تضاعف الطلب على التقنيات المتمثلة في الحواسيب الآلية والشبكات المعلوماتية وتوسع ميادين استعمالها وازدياد الاعتماد عليها بشكل مفرط في كل القطاعات، إلا أن الاستخدام المتنامي لهذه التقنيات انطوى على بعض الجوانب السلبية التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع لسوء استخدام هذه التقنية واستغلالها على نحو غير مشروع حيث أصبحت تلحق الضرر بمصالح الأفراد والجماعات والمؤسسات الأمر الذي أدى بأصحاب النوايا الإجرامية إلى الاستعمال غير المشروع للمنظومة المعلوماتية من أجل ارتكاب أعمالهم الإجرامية المختلفة والتملص من المسؤولية الجزائية حيث ظهر شكل جديد من الإجرام والذي يعرف بالجرائم المعلوماتية التي تعتبر من اخطر وأعقد الجرائم الجديدة المنظمة.

فخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث حداثة أساليب ارتكابها والبيئة التي تجري فيها وخصوصية مرتكبيها ووسائل كشفها فهي جريمة تنشأ في الخفاء وفي بيئة افتراضية دون أن تخلف أي أثار، وهذه الجريمة يرتكبها مجرمون أذكياء يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات وخبرات تقنية عالية.

وهذا ما أدى إلى وضع أطر قانونية ملائمة جديدة، وإدخال تعديلات على القوانين بما يتلائم مع الوضع الجديد، لتحديد شروط استعمال هذه الوسائل في مختلف المعاملات، من خلال نصوص جزائية لحماية الأنظمة المعلوماتية و ردع إساءة استعمالها، كما امتدت التعديلات إلى نطاق القانون الجنائي الإجرائي والجزائر باعتبارها واحدة من الدول التي تعرضت لهذا النوع من التطور التكنولوجي فهي معنية بالمكافحة ومسايرة التطور .

فكان لابد من إيجاد إطار قانوني مناسب لسد الفراغ الإجرائي لذلك وضعت مجموعة من الإجراءات عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة ومنها إجراءات تطبق فقط على الجريمة المعلوماتية التي تم النص عليها في القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته فهذا القانون يعد الإطار التشريعي الأساسي لمكافحة الجرائم المعلوماتية في الجزائر حيث يحدد أنواع الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال كاختراق أنظمة المعلومات والاعتداء على البيانات ونشر المحتويات غير القانونية .

تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جريمة جديدة لابد من إثباتها في القانون الجنائي طالما كان من المستحيل قانونا إدانة شخص دون أن تثبت مساهمته في الفعل الإجرامي ودون اجتماع كافة العناصر المكونة لهذه الجريمة، فالإثبات الجزائي هو الوحيد الذي لا تنقطع المحاكم عن تطبيقه في كل ما يعرض عليها من القضايا وذلك بالاستعانة بوسائل تعيد أمامها رواية وتفصيل ما حدث وهذه الوسائل هي أدلة الإثبات، وتقوم العملية الإثباتية التي تستهدف إقامة الأدلة على منهجية منتظمة ترتكز على قواعد أساسية يمكن اعتبارها بمنزلة معطيات تتشابك فيما بينها في مختلف مراحل الدعوى منذ قيام الجريمة إلى غاية صدور حكم نهائي فيها، وبهذا يعد الإثبات من أهم الركائز التي يقوم عليها صرح العدالة الجنائية كما يعتبر الهدف الجوهري الذي تدور حوله قواعد الإجراءات الجزائية والتي تسعى إلى إثبات الواقعة التي وقعت وذلك برسم الطرق التي تمكن من كشف الجريمة وصولا للقناعة الوجدانية للقاضي تتم من خلال الأدلة المتوافرة.

وبناءا على ذلك نطرح إشكالية الدراسة **كيف يتم الإثبات الجنائي للجرائم المعلوماتية بالأدلة *الرقمي؟***

ساهم التقدم الهائل الذي أضحى واضحا في المجال التكنولوجي، وزيادة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة، من أشخاص أو هيئات وأشخاص معنوية، كل ذلك أسهم في ظهور فئة جديدة من الإجرام مرتبطة بالتكنولوجيا، ومنها الجرائم المعلوماتية، ونظرا لتزايد نسب ارتكاب هذه

الجريمة في الآونة الأخيرة أدى إلى إنعكاسها على مضمون الأنظمة والقوانين، حتى تتماشى مع طبيعة الجريمة ومعطياتها، وأثارها.

ومن هذه الإشكالية الرئيسية، تتفرع عدة تساؤلات فرعية تقف مع الإشكالية الرئيسية لتقيم بنيان البحث وهي كالتالي:

- ماهية الجريمة المعلوماتية ؟ وماهي أنواعها ؟
- ماهية الدليل الرقمي ؟ وماهي مراحله ؟
- ماهي طرق الحصول على الدليل الجنائي الرقمي ؟
- وماهي حجية الدليل الرقمي أمام القضاء الجنائي ؟

من بين الأسباب التي دفعتني إلى إختياري لهذا الموضوع:

- إنتشار ما يعرف بالجرائم المعلوماتية مما جعلها هاجسا وخطرا على المستوى العالمي، لما تلحقها هذه الجرائم من أضرار على إقتصاديات الدول.

- إن الجريمة المعلوماتية ورغم أهميتها وخطورتها على المجتمع لم تتم معالجتها بالشكل الكافي وإنما بطرقة سطحية من قبل الباحثين وصنفت كباقي الجرائم الأخرى، لذا كان من الضروري إعطاء توضيح شامل لها، سواء بالنسبة للدارسين أو الجهات القضائية.

تهدف الدراسة إلى التعرف ودراسة العديد من النقاط وهي:

- التعرف على الجريمة المعلوماتية.
- التعرف على أسباب إرتكاب الجريمة المعلوماتية.
- التعرف على الهيئات المختصة لمكافحة الجريمة المعلوماتية.
- التعرف على إجراءات التحقيق والمحاكمة في الجريمة المعلوماتية.

إستخدمنا في هذا البحث المنهج الوصفي والتحليلي، الذي يقوم على أساس تحديد خصائص المشكلة محل البحث، ووصف ماهيتها وأسبابها، ثم تحليل هذه المشكلة والتعرف على أنواعها وذلك للوصول لمعالجة المسؤولية الجنائية عن الجريمة المعلوماتية في التشريع الجزائري، وهو المنهج الذي ساعدنا في الوصول إلى مجموعة من النتائج الدقيقة.

- رسالة دكتوراه: "الأسرار المعلوماتية وحمايتها الجزائية" جامعة أبو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية قسم الحقوق، عزيزة رابحي، 2017-2018.

- مذكرة ماستر: "مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية"، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية قسم الحقوق، يوميلا إبتسام، 2020-2021.

- مذكرة ماستر: "خصوصية التحقيق في الجريمة المعلوماتية"، جامعة طاهر مولاي، سعيدة، كلية الحقوق والعلوم السياسية، قسم الحقوق، عبد العزيز أحمد، 2021-2022.

ومن الصعوبات التي واجهتني في إعداد المذكرة المتمثلة أساسا في:

- قصر الوقت المخصص لتحضيرها.
- صعوبة التنقل بين المكتبات ومكان الإقامة نظرا لتواجدها في أماكن مختلفة.
- صعوبة إيجاد المراجع بسبب الوعكة الصحية (الحمل).
- الصعوبات المالية.
- صعوبة الإتصال بالمشرف

ولمعالجة هذا الموضوع والإجابة على الإشكالية والتساؤلات المطروحة تم تقسيم البحث إلى فصلين الفصل الأول بعنوان الجرائم المعلوماتية وأهمية الأدلة الرقمية وقد تم تقسيمه إلى مبحثين الأول بعنوان مفهوم الجرائم المعلوماتية وقد تم تقسيمه إلى ثلاث مطالب والمبحث الثاني بعنوان مفهوم الأدلة الجنائية الرقمية وقد تم تقسيمه إلى ثلاث مطالب.

أما الفصل الثاني بعنوان طرق إثبات الجرائم المعلوماتية بإستخدام الأدلة الرقمية وقد تم تقسيمه إلى ثلاثة مباحث، المبحث الأول كان بعنوان إجراءات إستخلاص الدليل الرقمي وقد تم تقسيمه إلى ثلاثة مطالب، والمبحث الثاني كان بعنوان طرق الحصول على الدليل الرقمي والصعوبات التي يواجهها، وقد تم تقسيمه إلى ثلاثة مطالب، والمبحث الثالث بعنوان حجية الدليل الرقمي في الإثبات أمام القضاء الجنائي وقد تم كذلك تقسيمه إلى ثلاثة مطالب.

الفصل الأول : الاطار المفاهيمي للجريمة المعلوماتية.

الفصل الأول : الجرائم المعلوماتية وأهمية الأدلة الرقمية.

تعد الجريمة المعلوماتية من أكبر التحديات التي نواجهها في عالمنا المعاصر إن لم تكن أكبرها على الإطلاق، فعصر التكنولوجيا الرقمية أو عصر المعلوماتية إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الإنجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة، ويبدو بالفعل أن تكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة وأن المعلومات في حد ذاتها هي المادة الخام الأساسية للإنتاج الذي يعتمد المجتمع على إنتاجها وإيجادها والإستفادة منها، وفي الواقع إن هذا الوجه المشرق لتقنية المعلومات له جانب مظلم والذي يتمثل في الإجرام المعلوماتي[1] ولذلك كان لابد من تواجد ما يسمى بالأدلة الرقمية التي تعد من العناصر الحيوية في العديد من المجالات نظرا لأهميتها الكبيرة في تقديم المعلومات الدقيقة والموثوقة للكشف عن الجريمة المعلوماتية ومنه نتطرق إلى دراسة المبحث الأول عن مفهوم الجرائم المعلوماتية والمبحث الثاني عن الأدلة الجنائية الرقمية في الجرائم المعلوماتية.

المبحث الأول: مفهوم الجرائم المعلوماتية .

تعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا واتساعا وقد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، فلقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا كبيرا من أجل الوصول إلى تعريف مناسب يتلائم مع طبيعة الجريمة المعلوماتية، إلا أن كثيرا من هذه المحاولات قد باءت بالفشل، فالمحاولات التي بذلت من أجل تعريف الجريمة المعلوماتية متعددة إن كانت لا تخرج جميعها عن أحد الإتجاهين، الإتجاه الأول يضيق من مفهوم الجريمة المعلوماتية[2] بحيث تقل الحالات التي يمكن أن يتصف فيها النشاط الإجرامي بها والاتجاه الثاني يوسع من مفهوم هذه الجريمة حتى أنه يمكن القول أنه يدخل في عدادها في كثير من الأحيان.

المطلب الأول: تعريف الجريمة المعلوماتية.

بداية لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن إستغلال تقنية المعلومات وإستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي والبعض الآخر يطلق عليها جريمة الإختلاس المعلوماتي أو الاحتيال المعلوماتي وآخرون يفضلون تسميتها بالجريمة المعلوماتية[3].

الفرع الأول: تعريف المعلوماتية.

هي التي اشتقت كلماتها في اللغتين الانجليزية والفرنسية (informatics-informatique) من المقطع الأول من كلمة معلومات information والمقطع الأخير من كلمة آلي (automatics -automatique) وذلك لتعبر عن المعالجة الآلية للمعلومات وهي تعبر في مجملها

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط1، الأردن، 2010، ص 46

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، ط1، مصر، منشورات الحلبي الحقوقية، كلية الحقوق، جامعة حلوان، جمهورية مصر العربية، 2005، ص26-27.

[3] نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص46.

عن الإدماج والتزاوج بين تلك المستحدثات التقنية المتقدمة للتحكم في المعلومات وجمعها ثم معالجتها وإختزانها وإسترجاعها وتحسين الانتفاع بها كالحاسبات والأقراص الليزرية ووسائط الإدخال ويتضح من ذلك أن هذا المصطلح يضم في جانبيه مصطلحين مهمين وهو النظام المعلوماتي والمعلومات ونظرا لتعلق هذين المرادفين بالدليل الجنائي الرقمي فإنه يقع لزاما إراد تعريف لكل منهما[1].

أولا: تعريف النظام المعلوماتي .

عرفت اتفاقية بودابست الدولية لمكافحة الجرائم المعلوماتية التي وقعت في 23 نوفمبر 2001 تهدف إلى مكافحة الجرائم المرتكبة عبر الانترنت والشبكات المعلوماتية وتعتبر هذه الاتفاقية أول معاهدة دولية تسعى إلى معالجة الجرائم السيبيرانية من خلال توحيد التشريعات الوطنية، وتعزيز التعاون الدولي وتشمل هذه الاتفاقية مواد تتعلق بتجريم أفعال مثل الوصول الغير مصرح به إلى الأنظمة المعلوماتية، وإعتراض البيانات، والتدخل في الأنظمة، كما تتناول الاتفاقية الإجراءات الواجب اتخاذها على الصعيد الوطني مثل تبني السلطات المختصة للصلاحيات والإجراءات اللازمة للتحقيق في الجرائم المعلوماتية وتوفير آليات للتعاون الدولي الفعال والسريع بين الدول الأعضاء[2].

فلقد عرفت اتفاقية بودابست النظام المعلوماتي بأنه: " كل جهاز بمفرده أو مع غيره من الأجهزة المتصلة والتي يمكن أن يقوم واحد منها أو أكثر تنفيذ برنامج معين بأداء المعالجة الآلية للبيانات".

كما عرفته أيضا الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات التي تم إقرارها من قبل مجلس وزراء الداخلية، والعدل العربي في عام 2010 تحت مظلة جامعة الدول العربية وتم تبني الاتفاقية خلال الاجتماع المشترك لمجلس وزراء العدل الداخلية العربية بتاريخ 21 ديسمبر 2010 بالقاهرة، مصر، ويمكن العثور على نص الاتفاقية في الموقع الرسمي لجامعة الدول العربية وعبر الجريدة الرسمية للدول التي صادقت عليها.

ولقد عرفت الاتفاقية العربية النظام المعلوماتي بأنه:" مجموعة برامج وأدوات المعدة لمعالجة وإدارة البيانات والمعلومات ".

أما بخصوص التشريعات الوطنية فقد عرفه المشرع الجزائري 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها وقد صدر بتاريخ 05 أوت 2009 هذا القانون عن الجمهورية الجزائرية الديمقراطية الشعبية وهو منشور لجريدة الرسمية حيث يحدد الأحكام الخاصة بمكافحة الجرائم المعلوماتية وحماية نظم المعلومات.

---

[1] بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة الدكتوراه، كلية الحقوق، جامعة الجزائر1، 2015، ص26

[2] أهم ما جاء في اتفاقية بودابست:" - تجريم الجرائم الإلكترونية كالاحتيال عبر الانترنت وانتهاك حقوق الملكية الفكرية .
- تمكين السلطات من جمع الأدلة الرقمية والاحتفاظ بها .
- منح صلاحيات للتحقيق والمراقبة في حالات الجرائم الالكترونية.
- التعاون الدولي وتبادل المعلومات بين الدول لمكافحة الجرائم الالكترونية .
- تسهيل تسليم المجرمين المرتبطين بالجرائم السيبيرانية.
- المساعدة القانونية المتبادلة في التحقيقات والملاحقات القضائية."

ثانيا: تعريف المعلومات .

في أوائل السبعينات من القرن المنصرم ازدهرت صناعة جديدة أطلق عليها صناعة المعلومات وأصبحت تشكل مصدرا للثروة والثراء ولأهميتها أصبحت المعلومة في الوقت الحاضر سلعة تباع وتشترى، وقد تناولت العديد من التشريعات العربية مفهوما للمعلومات، كما وقد عرفها المشرع الأمريكي في قانون المعاملات التجارية الالكترونية لسنة 1999 في الفقرة العاشرة من المادة الثانية على أنها "تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات وما شابه ذلك[1]."

أمان القانون الفرنسي رقم 82-652 الصادر في 26 جوان 1982 فعرف المعلومة بأنها "صوت أو صورة أو مستند أو معطيات أو خطابات أيا كانت طبيعتها" .

كما عرفها الفقه بأنها:" مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال والتفسير والتأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة حيث يمكن تغييرها وتجزئتها وجمعها ونقلها بوسائل وأشكال مختلفة[2]".

وعليه من خلال ما سبق يمكن تعريف المعلومات بأنها: "كل ما يصلح لتقديمه فائدة أو كل ما يصلح أن يكون محلا للتبادل أو التصرف فيه إلكترونيا سواء للتخزين أو الإرسال بأي شكل كان من رموز أو الصور أو بيانات يتم إرسالها وتبادلها عبر النظام المعلوماتي الذي يهدف إلى أمر معين ويكون ذا قيمة علمية، ثقافية، مالية، إجتماعية".

الفرع الثاني: تعريف الجريمة المعلوماتية.

لقد تضاربت الآراء في تعريف الجريمة المعلوماتية فمنهم من يعرفها بأنها فعل غير مشروع يرتكب باستخدام التكنولوجيا الرقمية، سواء عبر أجهزة الحاسوب أو شبكات الانترنت أو أي وسيلة الكترونية أخرى بهدف الإضرار بالإفراد أو المؤسسات أو الدول من خلال الاختراق، الاحتيال، التشهير، التجسس أو أي سلوك إجرامي رقمي آخر ويشمل هذا التعريف الجرائم التي تستهدف البيانات أو الأنظمة الالكترونية أو تستخدم التقنية كوسيلة لتنفيذ الجريمة وهناك من يعرفها بأنها ليست هي التي يكون النظام المعلوماتي أداة ارتكابها بل هي التي تقع على النظام أو داخل نطاقه وظهرت أيضا عدة تعريفات منها :

أولا: التعريف الفقهي للجريمة المعلوماتية.

عرفها الفقيه الألماني تيدمان بأنها:" كل أشكال السلوك غير مشروع الذي يرتكب باستخدام الحاسب".

كما عرفها مكتب التقنية في الولايات المتحدة الأمريكية بأنها:" الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا ".

---

[1] خالد ممدوح إبراهيم، جرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009، ص50.

[2] نفس المرجع ص52.

كما عرفها كل من الفقيهين Hard Castle،Richard Totty "بأنها تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسب".

وعرفها الأستاذ Astar Solarz "نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات وهو يشابه التعريف الذي أتى به الباحث ".

David Thompson بأنها :"جرائم يكون متطلبا لاقترافها أن يتوفر لدى الفاعل معرفة بتقنية الحاسب".

أما الفقيه Meowe فقد عرفها :"بأنها ذلك الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي الذي يرتكب باستخدام المعالجة الآلية للبيانات".

كما عرفها الأستاذ rosenbalt " بأنه نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة أو التي تحول عن طريقه".

وكذلك عرفها الأستاذ john forester "هو فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"[1].

ونشير أيضا إلى أن جانبا من الفقه والمؤسسات ذات علاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية أن الجريمة تنسب لفاعلها الأصلي[2] .

كما عرفها أيضا الفقيه parker "على أنها كل فعل غير مشروع يكون باستعمال تكنولوجيا الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى غير أن اتجاها من الفقه أعطى للجريمة المعلوماتية معنى واسع لتشمل كل أشكال السلوك أو الفعل الغير مشروع والذي يرتكب بواسطة الحاسوب[3].

ثانيا: التعريف القانوني للجريمة المعلوماتية.

تبنى المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح "المساس بأنظمة المعطيات" معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات محل الجريمة تمثل المعالجة الآلية للمعطيات والشرط الأول الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة.

فالمشرع الجزائري جرم الاعتداء على أنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية وظهور أشكال جديدة من الجرائم وهو ما دفعه إلى تعديل قانون العقوبات الذي عالج

---

[1] بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، مرجع سابق، ص 52- 53

[2] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية العلوم الاقتصادية والتجارية، جامعة قاصدي مرباح ورقلة، 2019، ص3-4,

[3] بن دراح علي إبراهيم، محاضرة في الجرائم المعلوماتية، ماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، المركز الجامعي، أفلو، الأغواط، 2020-2021، ص5.

القسم السابع منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات الذي تضمن مواد من 394 مكرر إلى غاية 394 مكرر7[1] ".

وفق المشرع في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة بالتشريعات المقارنة بحيث اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات.

وما يمكن استخلاصه هو أن استعمال المشرع لمصطلح "أنظمة المعالجة الآلية للمعطيات" للدلالة على كلمة المعلومات والنظام الذي يحتوي عليها ويخرج بذلك من نطاق التجريم لتلك الجرائم التي يكون فيها النظام المعلوماتي وسيلة ارتكابها وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي أي الجرائم التي يكون النظام المعلوماتي محلا لها[2].

الفرع الثالث: خصائص الجريمة المعلوماتية .

في ظل الثورة الرقمية والاعتماد المتزايد على التقنيات الحديثة، برزت الجريمة المعلوماتية كظاهرة معقدة ومتعددة الأوجه، تتسم هذه الجرائم بخصائص فريدة تجعل من تتبع مرتكبيها مهمة شاقة، حيث يعتمد المجرمون على التقنيات الرقمية لإخفاء هوياتهم والتسلل عبر الشبكات العالمية دون التقيد بالمكان أو الزمان ومن أهم خصائصها ما يلي :

أولا: الجريمة المعلوماتية جريمة مستحدثة .

تعتبر من أبرز الجرائم الجديدة التي أفرزتها ثورة التكنولوجيا، كما أنه لا يوجد أي مفهوم أو تعريف أو مصطلح قانوني موحد للدلالة على هذا النوع من الجرائم إذ اختلفت التسميات بشأنها كما سبق ذكره وهذا راجع أساسا إلى تطور هذه الجريمة تزامنا مع التطور التكنولوجي[3].

ثانيا: صعوبة الكشف عن الجريمة المعلوماتية وإثباتها .

تتميز الجريمة المعلوماتية بصعوبة إكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة حيث يبدو من الواضح أن عدد الحالات المكتشفة قليلة، مقارنة بالجرائم التقليدية ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشافها إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، كما أن الجاني يمكنه ارتكابها في دول وقارات أخرى، ويمكنه تدمير دليل الإدانة في أقل من ثانية واحدة.

ثالثا: جريمة عابرة للحدود الوطنية .

أي أنها ذات طابع دولي هذه الخاصية ناجمة من أن المجتمع المعلوماتي لا يعترف بالحدود الجغرافية أو المكانية أو الزمانية مما طرح مشكلة الإختصاص القضائي، وهنا ظهرت الحاجة لضرورة صياغة تشريع قانوني دولي لمكافحة هذا النوع من الجرائم.

---

[1] تعديل قانون العقوبات بموجب قانون رقم 04-15 الصادر في 10-11-2004 المتمم للأمر رقم 156- 66 المتضمن قانون العقوبات

[2] عيادي فريدة، الجريمة المعلوماتية في التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، ص229- 230

[3] سويسي فتيحة، تكييف القانوني للجرائم المعلوماتية والإشكالات العملية المترتبة عنها، مداخلة مقدمة خلال الندوة البحثية، مركز البحوث القانونية والقضائية، 2022، ص08.

رابعا: جريمة تتطلب خبرة فنية والتحكم في التكنولوجيا المعلوماتية أثناء التحقيق والمتابعة .

نظرا للطبيعة التقنية للجريمة لابد أن يكون المحققين أو عناصر الضبطية القضائية متخصصين بهذا النوع من الجرائم والتعامل باحترافية ومهارة أثناء مرحلة البحث والتحري، كما تتطلب المتابعة المستمرة للتطورات التكنولوجية ومعرفة الوسائل التقنية والإجرائية لمواجهة الجرائم المعلوماتية، وكذلك ضرورة التدريب المستمر وتبادل الخبرات بينهم في هذا المجال سواء على المستوى الدولي أو الوطني، وكذا تفعيل دور التعاون لإكتساب المهارات والخبرات من الدول المتقدمة، كما تساعد الخبرة العلمية والتقنية في الكشف عن الدليل الالكتروني وتحديد خصائصه كالمستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور.....الخ[1].

خامسا: جريمة تتسم بخطورة بالغة من شأنها المساس بالاقتصاد الوطني والدولي وتتسبب في خسائر مالية كبيرة .

حسب دراسة حديثة أصدرها مركز الدراسات الإستراتيجية والدولية تم التوصل إلى أن الجرائم الإلكترونية تكلف الإقتصاد العالمي نحو 445 مليار دولار سنويا.

سادسا: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص .

تتميز الجريمة المعلوماتية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت، يقوم بالجانب الفني من المشروع الإجرامي شخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

سابعا: خصوصية مجرمي المعلوماتية .

المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة عامة، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب ومن يرتكبها عادة يكون من ذوي الإختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على إستعمال جهاز الحاسوب والتعامل مع شبكة الانترنت، فعلى سبيل المثال فإن الجرائم ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير مشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جدا من قبل مرتكبيها[2].

الفرع الرابع: تعريف المجرم المعلوماتي وخصائصه .

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثر على تمييزها عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثر أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين، فمجرمو المعلوماتية ليسوا دائما مجموعة من النوابغ الذين لا يمكن التنبؤ بهم أو معرفتهم[3].

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق ، ص 53

[2] سويسي فتيحة، تكييف القانوني للجرائم المعلوماتية والإشكالات العملية المترتبة عنها، مرجع سابق، ص09.

[3] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، مرجع سابق ص56.

أولا: تعريف المجرم المعلوماتي .

خطورة هذه الجرائم تكمن بصفة أساسية في المجرم الذي يقوم بتنفيذ الجريمة حيث أنه يتميز بالذكاء والدراية في التعامل في مجال المعالجة الآلية لمجال المعطيات والإلمام بالمهارات والمعارف التقنية، فسمات المجرم المعلوماتي في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء، حيث أن كل من هؤلاء المجرمين قد يكون من ذوي مناصب رفيعة المستوى ومن ذوي التخصصات والكفاءات العالية ويتمتعون بالذكاء وبالقدرة على التكيف الاجتماعي في المحيط الذي يعيشون فيه، بل أن بعضهم يتمتع بإحترام وثقة عالية من الأشخاص المحيطين بهم في مجال العمل[1].

ثانيا: خصائص المجرم المعلوماتي .

1- الذكاء والمهارة في مجال التعامل مع التقنية المعلوماتية :

لقد قام الباحثون بإختيار عينة من الأشخاص المختصين في مجال الجريمة المعلوماتية فوجدوا أن هناك مجموعة من الأفراد لديهم ملامح إجرامية توحي لشخصية المجرم المعلوماتي الذي يتمتع بالذكاء والمهارة في مجال إستخدام والتعامل مع التقنية المعلوماتية، فهو يتميز بالقدرة على إختراق النظم المعلوماتية، شبكات الإتصال والتلاعب بأنظمتها، ويبتكر أساليب متطورة لإرتكاب أفعاله ولديه القدرة الفائقة على المعالجة الإلكترونية للنصوص والتعامل مع البرامج[2].

2- المجرم المعلوماتي يبرر إرتكاب جريمته :

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في تعداد الجرائم أو بمعنى أخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص، الأمر الذي يعدونه غاية اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم [3].

3- خوف المجرم المعلوماتي من كشف جريمته :

يتصف مجرمو المعلوماتية بالخوف من كشف جرائمهم وافتضاح أمرهم، صحيح أن هذه الخشية إنما تصاحب المجرمين على اختلاف أفعالهم الإجرامية إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب على افتضاح أمرهم من ارتباك مالي وفقد للمركز الوظيفي في كثير من الأحيان ويساعد مجرمي المعلوماتية على الحفاظ على سرية أفعالهم، فان أكثر ما يعرض المجرم إلى اكتشاف أمره أن تطرأ أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحاسبات الآلية سواء كانت المحل الذي يرد عليه السلوك الإجرامي أو الوسيلة المستخدمة لتنفيذه إنما تؤدي عملها بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى وهو ما يساعد على عدم كشف الجريمة طالما أن جميع خطوات التنفيذ معروفة مسبقا ولقد لخص الأستاذ parker من خلال دراسته لأنماط مجرمي معلوماتية أن أغلبهم غير قادرين على اقتراف الجرائم التقليدية وخاصة

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص59.

[2] ربيعي حسن، المجرم المعلوماتي شخصيته وأصنافه، مجلة العلوم الإنسانية،عدد40، جوان2015، ص288- 298.

[3] نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص78.

تلك التي تتطلب مواجهة مع المجني عليه، فالمجرم المعلوماتي لا يستطيع الاعتداء على المجني عليه بطريقة مباشرة [1].

4- المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي:

يقصد بالسلطة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي التي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة معلومات محل الجريمة وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة، كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها وقد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة [2].

ثالثا: دوافع المجرم المعلوماتي :

إذا كان من الصعب توحيد نموذج المجرم المعلوماتي بالنظر إلى تباين شخصية كل مجرم عن الأخر من حيث مدى ذكائه ومركزه وإمكاناته والاكتفاء بالملامح الرئيسية لتلك الشخصية، فإن أمر تحديد الدوافع والحوافز التي تحرك المجرم المعلوماتي في إطار إتمام فعله يبدو أمرا أقل صعوبة من خلال إشتراك مختلف الطوائف والمجرمين المعلوماتيين في دوافع قد تكون مشتركة غالبا فالدافع أو الباعث أو الغرض أو الغاية تعد تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي تتصل بما يعرف بالقصد الخاص في الجريمة، وللجريمة المعلوماتية عدة دوافع لارتكابها فبعضها يرجع لدوافع شخصية والبعض الآخر دوافع خارجية وكل هذه الدوافع يكون مصدرها الرغبة الإجرامية [3].

1-الدوافع الشخصية :

1-1- العبث أو اللهو: من الصعب التفريق بين دافع العبث واللهو، وتحقيق المصلحة الخاصة، فهما وجهان لعملة واحدة، فوجود الأولى يعني وبالضرورة وجود الثانية، واللهو والعبث يعتبران من الدوافع المتوفرة في أغلب الجرائم المعلوماتية البسيطة، فيجد المجرم المعلوماتي فيها الإحساس بشعور الاعتراف الاجتماعي، وبأنه أكثر شجاعة وقيمة وعادة ما يتطور هذا اللهو والعبث من دافع شخصي إلى جماعي مشترك.

1-2- الرغبة في الانتقام: الانتقام من الغرائز البشرية التي تؤدي بالشخص إلى إرتكاب الجريمة المعلوماتية فنجد منهم من يفصلون من مناصب عملهم تعسفيا ومن دون وجه حق، فتجده حائزا على معلومات متعلقة بسير النظام المعلوماتي، فتجده يرتكب جريمته رغبة منه في الانتقام من الشركة التي فصلته ليجعلها تتكبد الخسائر المالية الكبيرة .

1-3- تحقيق الربح المادي: تعتبر غاية تحقيق الربح المادي من الدوافع الرئيسية لدى مجرمي المعلوماتية، فإكتشاف ثغرة في النظام المعلوماتي هو السبيل المباشر لغرض تحقيق منفعة مالية كتحويل الأموال، فحسب رأي كل من الأستاذين lamer et rose :" إن المجرم المعلوماتي وانطلاقا

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، مرجع سابق ص60.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص80.

[3] غريبي بشرى، خصوصية المجرم المعلوماتي، مجلة نوميروس الأكاديمية، جامعة أبو بكر بلقايد، المجلد2، العدد2، 2021، ص109.

من حافز تحقيق الربح المادي فهو يطبق نظرية اقتصادية، فهو يبحث عن أكبر قدر ممكن من الأرباح مقابل أقل قدر ممكنة من الخسائر".

وقد يتحقق غرض الربح المادي بأسلوب التهديد والابتزاز، فحسب تقرير السيد Mikko hypomen مدير مركز البحوث لدى شركة (f.secure) فإن بعض المجرمين المعلوماتيين يعمدون إلى إرسال رسائل إلكترونية لضحاياهم مسبقا، يخبرونهم فيها بأمر اكتشاف ثغرات أمنية على أنظمتهم المعلوماتية وبأنهم سيقومون بمحو بياناتهم وتدميرها كليا في حال عدم تحويل أموال إلى حساباتهم، وهذا ما حدث بالفعل لشركة Google في شهر ماي 2004 أين قام Bradly Michel بإرسال تهديدات لهذه الشركة بضرورة دفع مبلغ 100,000 دولار وإلا سيقوم بنشر فيروس وبرنامج غامض من شأنه أن يتسبب في تعطيل نظامها المعلوماتي الخاص بتحصيل عائدات الإشهار من الصفحات المدعمة من قبلها.

2-الدوافع السياسية :

دافع الإرهاب: يمكن أن يتحول الدافع الإيديولوجي والسياسي إلى توجها آخر وهو الإرهاب بشكله الالكتروني، من خلال شبكة الانترنت التي يمكن أن تأوي مواقع خاصة بجماعات إرهابية، تمارس نشاطها من خلال التحريض على القتل والتمرد والعصيان المدني، وتهدف إلى ترويع المواطنين والأفراد من خلال نشرها لصور وفيديوهات على كيفية صنع المتفجرات والقنابل والإشادة بأعمالها الإجرامية، زيادة على ذلك فإنها عادة ما تستهدف النظم المعلوماتية الحكومية بغرض تعطيلها وتدميرها[1].

المطلب الثاني: تطور الجرائم المعلوماتية.

خلال سنة 1966 سجلت أول قضية في الولايات المتحدة الأمريكية تتعلق بارتكاب أفعال إساءة استعمال الحاسوب أين تمت محاكمة مهندس يعمل في البنك من أجل قيامه بالتحايل على برنامج الإعلام الآلي لإختلاس مبلغ مالي كما تم تسجيل عدة قضايا مماثلة تتعلق بالدخول خلسة إلى الأنظمة المعلوماتية للاطلاع على محتواها وكان القضاء يتعامل مع هذه القضايا على أساس قضية سرقة بالإكراه وأحيانا يعتبرها إخلال بالالتزامات المسؤولية العقدية[2].

أما اليابان سجلت أول قضية خلال سنة 1970 تتعلق بالمساس بالأنظمة المعلوماتية على اثر اكتشاف عملية سرقة ونشر معطيات شخصية لزبائن شركة تجارية، ونظرا لصعوبة التعامل مع هذا النوع من الجرائم بسبب خصائص البيئة المعلوماتية الافتراضية، تبلورت فكرة ضرورة وضع نصوص قانونية خاصة وبادرت عدة دول إلى إصدار تشريعات تجرم إساءة استعمال الكمبيوتر ونذكر على سبيل المثال :

الولايات المتحدة الأمريكية في سنة 1970 صدر أول قانون خاص بحماية البيانات وحق الوصول إليها ثم في سنة 1977 أصدرت أول تشريع فيدرالي خاص بجرائم الحاسوب[3]، أما في

---

1. ربيعي حسن، المجرم المعلوماتي شخصيته وأصنافه، مرجع سابق، ص291-292-294.
2. سويسي فتيحة، التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عندها، مرجع سابق، ص 4
3. نفس المرجع ، ص 5

السويد في سنة 1973 أصدرت قانون المعطيات المعلوماتية[1]، أما في فرنسا في سنة 1978 أصدرت قانون يتعلق بالمعلوماتية والحريات وفي سنة 1988 أصدرت قانون يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات .

وفي مطلع الثمانينات تبنى مجلس أوروبا اتفاقية حماية المعطيات الشخصية والمعالجة الآلية لها واستمر التطور التشريعي لمعالجة هذا النوع من الجرائم في العديد من الدول عبر العالم وبرزت الحاجة إلى ضرورة التعاون الدولي في هذا المجال أين صدرت عدة اتفاقيات إقليمية ودولية من بينها اتفاقية بودابست والمتعلقة بمكافحة الجرائم الالكترونية التي أعدها مجلس أوروبا سنة 2001 ودخلت حيز التنفيذ في 2004[2] وتلاها بروتوكولين إضافيين في سنة 2006 وصادقت على هذه الاتفاقية عدة دول وتعتبر الإطار الدولي الوحيد إلى غاية اليوم في مجال مكافحة الجرائم المعلوماتية، تهدف أساسا إلى توحيد الجهود الدولية وتوطيد التعاون الدولي للتصدي لهذا النوع من الإجرام.

المطلب الثالث: الإطار القانوني للجريمة المعلوماتية في التشريع الجزائري .

هو مجموعة القوانين والتشريعات التي وضعتها الدول لتنظيم استخدام تكنولوجيا المعلومات ومكافحة الجرائم التي ترتكب باستخدام الوسائل الالكترونية بما يضمن حماية حقوق الأفراد والمؤسسات ويعزز الأمن السيبيراني ومن أهداف الإطار القانوني للجريمة المعلوماتية حماية الأفراد والمؤسسات وتنظيم العقوبات وتعزيز التعاون الدولي.

الفرع الأول: الدستور.

نصت عليه المواد من (41 إلى 55) المتعلقة أساسا بحماية الحريات الفردية، حماية الحياة الخاصة، الحق في سرية المراسلات والاتصالات الخاصة بحماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي.

الفرع الثاني : الاتفاقيات الدولية والإقليمية .

ومن بين هذه الاتفاقيات الدولية الإعلان العالمي لحقوق الإنسان، الذي يتم اعتماده من قبل الجمعية العامة للأمم المتحدة في عام 1948 لم يتطرق بشكل مباشر إلى الجرائم المعلوماتية وذلك لأن التكنولوجيا المعلوماتية لم تكن متطورة بما يكفي في ذلك الوقت لتشكل مصدر قلق كبير على المستوى العالمي ومع ذلك فأن الإعلان العالمي لحقوق الإنسان يحتوي على مبادئ عامة يمكن أن تنطبق على حماية الأفراد في الفضاء السيبيراني[3]، على سبيل المثال ما جاء في المواد:

---

[1] أهم ما جاء في اتفاقية السويد1973: "- اتفاقية شجعت على التعاون الدولي لحماية البيانات.
- حق الفرد في معرفة البيانات المخزنة عنه.
- حق اعتراض الفرد على استخدام بياناته والحق في حذفها.
- جمع البيانات يشكل قانوني.
- استخدام البيانات في حدود الأغراض المحددة.
- حماية البيانات.

[2] أهم ما جاء في اتفاقية بودابست: " - وضع إطار قانوني لمكافحة الجرائم الالكترونية
- تعزيز التعاون الدولي في التحقيقات المتعلقة بالجرائم السيبيرانية
- توحيد التشريعات الوطنية الخاصة بمكافحة الجريمة الالكترونية بين الدول الأعضاء.

[3] سويسي فتيحة، التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها، مرجع سابق، ص12.

المادة 12: تنص على أنه: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مراسلاته ولا لحمالات على شرفه وسمعته أو لكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات" يمكن أن يفسر هذا النص على أنه يحمي الأفراد من انتهاكات الخصوصية والتدخلات غير القانونية في اتصالاتهم بما في ذلك تلك التي تحدث عبر الانترنت.

المادة 17: "نصت على أن لكل فرد الحق في التملك بمفرده أو بالاشتراك مع غيره، ولا يجوز تجريد أحد من ملكه تعسفا "ويعني بذلك سرقة البرمجيات والأعمال الفنية أو البيانات وتعتبر انتهاكا لهذا الحق وأيضا الاحتيال الالكتروني كسرقة الأموال أو المعلومات المالية عبر الانترنت ويعتبر انتهاكا للحق في الملكية .

المادة 19: فلقد نصت على أن: "لكل شخص الحق في حرية الرأي والتعبير ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل واستقاء الأنباء والأفكار وتلقيها وإذاعتها بأية وسيلة كانت دون تقيد بالحدود الجغرافية" هذا يمكن أن يشمل الحماية من الرقابة غير المبررة على الانترنت.

المادة 29:"نصت على أن لكل فرد واجبات تجاه المجتمع الذي يتاح فيه وحده لشخصيته أن تنمو نموا حرا كاملا" ويعني بذلك مسؤولية الأفراد والشركات احترام حقوق الآخرين في الفضاء الرقمي وعدم المشاركة في أنشطة إجرامية مثل القرصنة أو الاحتيال وحماية المجتمع واجب على الحكومات والمؤسسات من الجرائم المعلوماتية التي تهدد الأمن العام[1] .

وأما فيما يخص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تم اعتمادها في القاهرة بتاريخ 21 ديسمبر 2010 المصادق عليها بموجب مرسوم رئاسي رقم 14-252 مؤرخ في 08 سبتمبر 2014 وهي أول اتفاقية عربية تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم الالكترونية وتعتبر هذه الاتفاقية إطارا قانونيا مهما لمواجهة التحديات المتزايدة التي تفرضها الجرائم الالكترونية في المنطقة العربية[2].

ومن أهم أنواع الجرائم التي تغطيها الاتفاقية هي :

1- الوصول غير المشروع إلى الأنظمة أو البيانات مثل الاختراق الالكتروني.
2- اعتراض البيانات مثل التنصت على الاتصالات الالكترونية.
3- التلاعب بالبيانات مثل تعديل أو حذف البيانات بشكل غير قانوني .
4- استخدام البرمجيات الضارة كالفيروسات وبرامج الفدية .
5- انتهاك حقوق الملكية الفكرية كقرصنة البرمجيات أو المحتوى الرقمي .

ولقد أكدت الاتفاقية على ضرورة التعاون بين الدول العربية في مجال مكافحة الجرائم الالكترونية وذلك من خلال تبادل المعلومات والخبرات وتقديم المساعدة القانونية المتبادلة في التحقيقات والمحاكمات وتدريب الكوادر المتخصصة في مجال مكافحة الجرائم الالكترونية.

---

[1] ما نصت عليه المواد من الإعلان العالمي لحقوق الإنسان.

[2] أبرز ما نصت عليه الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: " -تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات.
- وضع إطار قانوني موحد لتجريم الأنشطة الالكترونية الغير مشروعة.
- تبادل الخبرات بين الدول الأعضاء لمواجهة جرائم الكترونية

ولقد نصت أيضا الاتفاقية على إنشاء آلية لمتابعة تنفيذ أحكامها وتتألف من ممثلين عن دول الأعضاء، لتقييم التقدم المحرز في مكافحة الجرائم الالكترونية وتقديم التوصيات اللازمة.

وبالرغم من أهمية الاتفاقية إلا أن هناك بعض التحديات التي تواجه تنفيذها مثل: الاختلافات في التشريعات الوطنية بين الدول العربية ونقص الخبرات الفنية في مجال مكافحة الجرائم الالكترونية في بعض الدول والحاجة إلى مزيد من التنسيق بين دول الأعضاء.

وأما ما تضمنه المرسوم الرئاسي رقم 16-111 تصديق على اتفاقية إنشاء المنظمة العربية لتكنولوجيات الاتصال والمعلومات فهذا المرسوم يهدف إلى تعزيز التعاون بين الدول العربية في مجالات تكنولوجيا الاتصال و المعلومات ولقد حرر هذا المرسوم بالقاهرة في 13-02-2002 [1].

ثم ظهر بعد ذلك القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وهو إطار قانوني يهدف إلى توحيد الجهود العربية في مواجهة الجرائم الالكترونية، وتعزيز التعاون بين الدول العربية في هذا المجال وأبرز ما تضمنه هذا القانون تعزيز التعاون العربي في مجال مكافحة جرائم تقنية المعلومات بما في ذلك تبادل المعلومات والخبرات، وحماية الأمن القومي من خلال مكافحة الجرائم الالكترونية التي تهدد أمنها واستقرارها[2]، ولقد تم تطبيق عقوبات جنائية على مرتكبي الجرائم الالكترونية بما في ذلك السجن والغرامات المالية والعقوبات التكميلية مثل مصادرة الأجهزة أو البرامج المستخدمة في ارتكاب الجرائم ولقد تم وضع إجراءات محددة لجمع الأدلة الرقمية في مثل هذه الحالات وتحليل الأدلة واستخدام تقنيات متقدمة لتحليلها واثبات الجرائم وللحد من هذه الجرائم تم وضع تدابير وقائية حيث شدد هذا القانون على أهمية اتخاذ تدابير لمنع الجرائم الالكترونية ومن بينها:

1- تعزيز وتشجيع الدول على أمن شبكاتها وأنظمتها المعلوماتية.

2- نشر الوعي بين الأفراد حول مخاطر الجرائم الالكترونية وكيفية الوقاية منها.

3- منع الوصول إلى البيانات الشخصية.

الفرع الثالث:القوانين .

القانون رقم 09-01 المؤرخ في 26 جوان 2001 هو قانون جزائري يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهذا القانون يهدف إلى وضع إطار قانوني لمكافحة الجرائم المعلوماتية وتعزيز الأمن السيبيراني في الجزائر ومن أبرز ما جاء في هذا القانون هو الوقاية من الجرائم المعلوماتية ووضع تدابير لمنع الجرائم المتصلة بتكنولوجيات الإعلام

---

[1] أبرز ما تضمنه المرسوم 16-111 :" يؤكد التصديق على الاتفاقية التي تم اقرارها من قبل الدول العربية لإنشاء المنظمة العربية لتكنولوجيات الاتصال والمعلومات هذه الاتفاقية تهدف إلى تعزيز التعاون العربي في مجالات التكنولوجيات والاتصالات ومن بين أهداف هذه المنظمة: - تعزيز التعاون بين الدول العربية في مجالات تكنولوجيات الاتصال والمعلومات.
- تطوير البنية التحتية لتكنولوجيات المعلومات والاتصالات للدول العربية.
- تعزيز الأمن السيبيراني وحماية البيانات في الفضاء الرقمي.

[2] أهم الجرائم التي يغطيها القانون العربي الاسترشادي "- جرائم الدخول الغير مشروع مثل الاختراق الإلكتروني للأنظمة والشبكات
- جرائم الاعتداء على البيانات مثل تدمير أو تعديلها بشكل غير قانوني.
- جرائم الاحتيال الالكتروني مثل التلاعب بالبيانات المالية لتحقيق مكاسب غير مشروعة.
- جرائم الإرهاب الالكتروني مثل إستخدام التكنولوجيا لتنفيذ عمليات إرهابية

والاتصال وتوفير أدوات قانونية لمحاسبة مرتكبي الجرائم الالكترونية، وحماية الأنظمة المعلوماتية وتعزيز أمن الأنظمة والبيانات الشخصية للأفراد والمؤسسات، ويعتبر هذا القانون هو أول نص تشريعي في الجزائر يهدف إلى حماية المعطيات الشخصية من الهجمات الالكترونية ويوفر إطارا قانونيا لمكافحة الاحتيال الالكتروني والتزوير الرقمي ويواكب التطور التكنولوجي ويضع أسسا للجرائم المستحدثة في المجال الرقمي[1].

أما القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 والمتعلق بالمساس بأنظمة معالجة البيانات الآلية هذه المواد تهدف إلى تعزيز الأمن السيبيراني وحماية الأنظمة المعلوماتية من الجرائم الالكترونية وتوفير إطار قانوني موحد للدول العربية لمكافحة الجرائم من خلال حماية الأمن القومي ومع ذلك فان نجاح هذا القانون يعتمد على مدى التزام دول الأعضاء بتنفيذ أحكامه وتطوير قدراته الفنية والقانونية في هذا المجال وهذا القانون يتضمن مواد جديدة تعاقب على المساس بأنظمة معالجة البيانات الآلية وهي جزء من الجهود التشريعية الرامية إلى حماية البيانات في الجزائر ومن أبرز المواد الجديدة المتعلقة بأنظمة معالجة البيانات الآلية فهي 13 مادة[2] .

أما القانون 16-02 المؤرخ في 10 جوان 2016 بالجرائم المعلوماتية يتمثل في تمويل الإرهاب عبر شبكة الانترنت فالقانون يعاقب على استخدام الوسائل الرقمية لتحويل الأموال أو دعم الجماعات الإرهابية ويشمل ذلك العملات الرقمية، التحويلات الالكترونية المشبوهة والمعاملات عبر الانترنت، أما فيما يتعلق باستخدام التكنولوجيا في تبييض الأموال فإن قانون العقوبات يشدد على غسل الأموال عبر الأنظمة المالية الرقمية ويمكن أن يشمل التداول الاحتيالي استخدام الحسابات الالكترونية الوهمية والاحتيال عبر الانترنت ومن أبرز المواد المضافة أو المعدلة في قانون 16-02 [3].

---

[1] أهم المواد التي جاء بها القانون 09-01:- المادة 394 مكرر:"يعاقب بالحبس من 3 أشهر إلى سنة غرامة 50000 دج إلى 100000دج، كل من يدخل أو يبقى عن قصد، وبطريقة غير مشروعة في نظام معالجة آلية للمعطيات".بمعنى تعاقب على أي دخول غير مصرح به إلى الأنظمة المعلوماتية حتى ولو لم يكن هناك ضرر مباشر وتشدد العقوبة إذا أدى الفعل إلى إتلاف أو تعديل البيانات.

المادة 394 مكرر1:"يعاقب بالحبس من 6 أشهر إلى سنتين وغرامة من 100000 دج إلى 200000 دج كل من يقوم عمدا بمحو أو تغيير أو تسبب في اضطراب تشغيل نظام معلوماتي." تتعلق هذه المادة بتدمير وإتلاف البيانات المخزنة الكترونيا وذلك بنشر فيروسات التي تؤدي إلى تعطيل النظام .

[2] أهم المواد التي جاء بها القانون 15-04:- المادة 01 "تعرف الجرائم المعلوماتية بأنها أي فعل غير مشروع يتم ارتكابه بإستخدام تقنية المعلومات أو الشبكات الالكترونية" ويشمل ذلك الوصول غير المصرح به والتلاعب بالبيانات والاحتيال الالكتروني والانتهاك الخصوصي.

المادة 02:"يعاقب القانون أي شخص يقوم بالوصول غير المصرح به إلى أنظمة معالجة البيانات الآلية "أي الوصول غير المشروع ويشمل الدخول إلى الأنظمة أو الشبكات دون إذن و العقوبة جنائية مثل السجن و الغرامات المالية.

لمادة 03: " يعاقب القانون أي شخص يقوم بتعديل أو تدمير البيانات بشكل غير قانوني" ويشمل تغيير أو حذف البيانات دون إذن وعقوبتها السجن وغرامات مالية. -

المادة04: " يعاقب القانون أي شخص يقوم بتعطيل أنظمة معالجة البيانات الآلية أو إعاقة عملها" ومعناها التعطيل المتعمد و يشمل إيقاف أو إعاقة عمل الأنظمة المعلوماتية.

[3] أهم المواد التي جاء بها قانون 16-02: المادة87 مكرر12" يعاقب بالسجن لمدة تتراوح بين 5 إلى 10 سنوات وغرامة 100000 دج إلى 500.000 كل من يستخدم تقنيات المعلومات والاتصال لتجنيد أشخاص لصالح منظمة إرهابية تستهدف هذه المادة الأفراد الذين يستغلون الوسائل الرقمية مثل الانترنت ووسائل التواصل الاجتماعي لتجنيد أو تحريض آخرين على الانضمام إلى جماعات إرهابية .

المادة87 مكرر 13 "يعاقب بالسجن لمدة تتراوح بين 5 إلى 10 سنوات وغرامة مالية من 100.000 دج إلى 500.000 دج كل جزائري أو أجنبي مقيم في الجزائر يسافر أو يحاول السفر إلى دولة أخرى بقصد إرتكاب أو التحريض لأعمال إرهابية"

قانون رقم 20-06 المؤرخ في 28 أفريل 2020 المعدل والمتمم الأمر رقم 66-156 المؤرخ في 08 جوان 1966 والذي يتضمن قانون العقوبات الجزائري، يهدف إلى تحديث وتعديل بعض الأحكام الواردة في قانون العقوبات لمواكبة التطورات الاجتماعية والقانونية الحديثة فلقد تم إدخال إجراءات جديدة لحماية الضحايا بما في ذلك إمكانية إغلاق المواقع الالكترونية أو الحسابات المستخدمة في ارتكاب الجرائم بعلم مالكيها وتم تحديث بعض الإجراءات القانونية لتسهيل عملية التقاضي وضمان سرعة الفصل في القضايا مع التركيز على الجرائم الالكترونية وجرائم عنف وجاءت تعديلات أخرى في بعض المواد القديمة في قانون العقوبات لتكون كثر ملائمة للواقع الحالي مع مراعاة ظروف الجناة وطبيعة الجرائم المرتكبة .

ومن أهم الجرائم الالكترونية المرتكبة كالاختراق غير المصرح به للأنظمة المعلوماتية وسرقة البيانات ونشر البرمجيات الضارة فتتراوح عقوبتها إلى السجن 15 سنة في حالات الجرائم الخطيرة وعقوبات مالية وأيضا مصادرة الأجهزة والبرامج المستخدمة في ارتكاب الجرائم الالكترونية[1] .

أما ما جاء به قانون 18-07 هو حماية البيانات الشخصية للأفراد من الاستخدام غير مصرح به أو التسريب فمن بين الجرائم الالكترونية التي تمس بالشخص الاختراق أي الوصول إلى الأنظمة المعلوماتية والتصيد الاحتيالي كسرقة المعلومات الشخصية عبر وسائل الالكترونية ونشر الفيروسات والتشهير الالكتروني كنشر معلومات كاذبة أو مسيئة عبر الانترنت.

أما القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ويهدف هذا القانون إلى وضع إطار قانوني لمكافحة الجرائم الالكترونية وضمان أمن المعلومات في الجزائر ويلزم هذا القانون مزودي خدمات الانترنت باتخاذ التدابير اللازمة لمنع الجرائم الالكترونية بما في ذلك سحب المحتوى الغير قانوني فور العلم به ووضع ترتيبات تقنية للحد من الوصول إلى المعلومات المخالفة للنظام العام أو الآداب العامة[2] .

وفيما يخص القانون 18-04 المؤرخ في 10 ماي 2018 والمتعلق بالبريد والاتصالات الالكترونية له علاقة غير مباشرة بالجرائم المعلوماتية حيث يضع الإطار القانوني لتنظيم قطاع الاتصالات الالكترونية والبريد في الجزائر وهو القطاع يستخدم في تنفيذ العديد من الجرائم المعلوماتية فهذا القانون يحدد استغلال خدمات الاتصالات الالكترونية مما يساعد في مراقبة ومنع الاستخدام غير مشروع للشبكات لأغراض إجرامية ويلزم متعاملي الاتصالات بحماية البيانات الشخصية لمستخدميهم واتخاذ التدابير اللازمة لمنع الاختراقات والتجسس الالكتروني ويفرض عليهم التعاون مع السلطات في مكافحة الجرائم المعلوماتية مثل الاحتيال الالكتروني والتجسس السيبيراني.

---

[1] أهم التعديلات المتعلقة بالجرائم والعقوبات تم إضافة فصل جديد تحت عنوان المساس بنزاهة الامتحانات والمسابقات يتضمن مواد جديدة من 253 مكرر 06 إلى 253 مكرر 12 "تعاقب على جرائم تسريب ونشر مواضيع وأجوبة الامتحانات والمسابقات واستبدال المترشحين في الامتحانات فالعقوبات تتراوح بين الحبس من سنة إلى 15 سنة وغرامة 1.5 مليون دج" تم تعزيز العقوبات على الجرائم المرتكبة باستخدام الوسائل التكنولوجية أو من قبل مجموعة من الأشخاص مع إمكانية مصادرة الأجهزة والبرامج المستخدمة في إرتكاب الجرائم.

[2] ينص قانون 09-04 :" إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنسيق الجهود في هذا المجال وتقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في تحقيقات المتعلقة بالجرائم الالكترونية.

المطلب الثالث: أنواع الجرائم المعلوماتية .

لقد أفرز تزايد استعمال شبكات الاتصال الحديثة والأنظمة المعلوماتية إشكالات قانونية هامة لاسيما ما يتعلق منها بمسألة حماية الحقوق المختلفة المتداولة عبر المواقع أو التي تنشأ من خلالها، فظهرت أنماط جديدة من الجرائم لم تكن معهودة في السابق يتم تنفيذها عبر معدات أو أجهزة الكترونية أو تبث عبر شبكة الانترنت أو محتوياتها، تلحق أضرارا مادية وجسدية أو حتى نفسية بالضحية بشكل مباشر أو غير مباشر فالجرائم الواقعة على الأنظمة المعلوماتية جرائم تنصب على معطيات الحاسوب ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب وذلك لقدرته الفائقة في معالجة البيانات والمعطيات مما جعله مجالا خصبا لارتكاب الجرائم [1].

الفرع الأول : الجرائم التي تقع على الأشخاص .

هي الجرائم التي تنال بالاعتداء وتهدد بالخطر الحقوق ذات الطابع الشخصي البحت، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم وفي الحرية والحق في صيانة الشرف.

أولا: جريمة انتحال الشخصية: هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه رغم انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوأ إستغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهه من أجل الحصول على بطاقات ائتمانية وغيره ومن خلال هذه المعلومات يستطيع المجرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت إسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت[2].

ثانيا: جريمة المضايقة والملاحقة: وهو نوع حديث من الجرائم المتزايدة باستمرار وهو عبارة عن مساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض، وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة، وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني، ولا تتطلب الجريمة المرتكبة عبر الانترنت أي اتصال مادي بين المجرم والضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية[3].

ثالثا: جرائم التغرير والاستدراج: هي من أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أوساط صغار السن ومن مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت، والجريمة المعلوماتية التي قد تتطور إلى لقاء مادي بين

---

[1] مراد بنار، الجرائم المرتكبة عبر الوسائط الالكترونية، مذكرة ماستر قانون خاص تخصص العلوم الجنائية و الأمنية، كلية العلوم القانونية و الاقتصادية و الاجتماعية، جامعة القاضي عياض، مراكش، 2016-2017، ص23.

[2] منير محمد الجمبيهي،ممدوح محمد الجمبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص42-43.

[3] محمد أمين الشوابكة، جرائم الحاسوب الأولى والانترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2004، ص45.

الطرفين وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وهي دون حدود سياسية واجتماعية إذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة، وكذلك يقع ضحيتها أي مستخدم حسن النية[1].

رابعا: الجرائم المخلة بالأخلاق والآداب العامة: إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر على مستخدم دون الآخر، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين، قد تشكل جريمة يعاقب عليها القانون في حين أنها لا تكون كذلك في أي بلد آخر، وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم عبر الرسائل الالكترونية أو محاولة إغوائهم لارتكاب هذه الأنشطة، أو نشر معلومات عنها عبر الحاسب الآلي ودعوتها إلى القيام بأعمال فاحشة وتصوير قاصرين ضمن أنشطة للجنس[2].

الفرع الثاني: الجرائم التي تقع على الأموال.

هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية ويدخل في نطاق هاته الحقوق الحق ذو قيمة اقتصادية وإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فإنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على ما يتعلق بالحاسب الآلي من برمجيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها.

أولا: جرائم صناعة ونشر الفيروسات: الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل وأما عن مبدأ عملها فيتحدد طبقا لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها، وقد تبدأ بمجرد تشغيل البرامج الموجودة عليه، وتعتبر هذه الصناعة من أهم جرائم الانترنت وأكثرها اتساعا وانتشارا.

ثانيا: جرائم الاختراقات: الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير والشبكات الالكترونية، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات أو الشبكات، وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم لمجرد الفضول والبعض الآخر لسرقتها وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها.

ثالثا: جريمة النصب والاحتيال: أصبح التعاقد عبر الانترنت حاجة وضرورة نظرا لسرعة وسهولة التعامل عبرها، لكن هذه الميزة ما لبثت أن شابتها سلبيات عديدة، هي عبارة عن أفعال إجرامية تعرف النصب والاحتيال ومن بينها خرق التعاملات عبر طرق احتيال جديدة تم ابتكارها، وكذلك زادت من وقوع جرائم النصب التي لا يزال يقع فيها عدد كبير من مستخدمي الانترنت، أما المظهر

---

[1] عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، 2015-2016، ص19.

[2] محمد أمين الشوابكة، جرائم الحاسوب الأولى والانترنت، ص114.

الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات المبالغ الموجودة داخل حسابات الضحايا ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم لذلك من الصعب جدا والقبض عليهم.

رابعا: جريمة تعطيل الأجهزة والشبكات: قد يؤدي تعطيل برامج الحاسب الآلي إلى أعطال فنية تقع على القطع الالكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة وتتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها وهو الأمر الذي يعيقها عن تأدية عملها[1].

المبحث الثاني: مفهوم الأدلة الجنائية الرقمية.

أول نقطة ينبغي التطرق إليها في دراسة الدليل الجنائي الرقمي هو مفهوم هذا النوع من الأدلة، فمن خلال المفهوم يتحدد الإطار الوصفي للموضوع محل الدراسة.

عندما يشير الباحث عمر بن يوسف إلى: "إن الدليل الرقمي يختلف عن الدليل المادي حيث أن هذا الأخير هو تعبير عن وضعية مادية ملموسة كما هو الشأن في بصمة الأصابع مثلا في حين أن الدليل الرقمي ليس سوى تعداد غير محدود لأرقام ثنائية موجودة في الرقمين (0-1) يبدو في حقيقة الأمر من خلال هذه العبارة أن الدليل الرقمي فعلا دليل غامض ومتميز مقارنة مع غيره من أدلة الإثبات، الأمر الذي يقتضي دراسة أعمق لهذا النوع من الأدلة انطلاقا من توضيح مفهومه وهذا بالاعتماد على مسألة التعريف بالدليل الرقمي كونها تعتبر أهم مسألة بدونها لا يمكن الوصول إلى فهم الموضوع كما ينبغي في هذا الإطار التطرق إلى كل ما يتعلق بالدليل الرقمي وذكر خصائصه.

المطلب الأول: مفهوم الدليل الجنائي الرقمي وخصائصه.

يشكل الدليل أهمية قصوى في مجال الإثبات الجزائي من حيث كونه الأداة أو الوسيلة التي يبني عليها القاضي حكمه في إدانة أو براءة المتهم الذي نسبت إليه الجريمة ولمعرفة ماهية الشيء يستلزم البحث في مفهومه من تعريفه وخصائصه التي يتميز بها عن غيره .

فالدليل الرقمي 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 معلومات في أشكال متنوعة فهذا الدليل يمكن إستخدامه في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات الجريمة، وفي سبيل التعرف الشامل على هذا النوع من الأدلة خصوصا لحداثته في علم القانون الجنائي وتعلقه بوسائل تقنية غير مادية.

---

[1] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر، كلية العلوم الاقتصادية والتجارية، جامعة قاصدي مرباح، ورقلة، 2019، ص07-08-09.

يجب علينا تبيان ماهية الدليل الجنائي الرقمي، وأن نوضح مفهومه من خلال التعريف به لغة واصطلاحا وبيان خصائصه وأنواعه، ثم نتعرض من جهة أخرى لكيفية استخلاص الدليل الجنائي الرقمي، وذلك استكمالا لماهيته [1].

الفرع الأول: تعريف الدليل الجنائي الرقمي.

لغة: يقصد بالدليل في اللغة ما يستدل به، ويقال أدل، وفلان يدل فلان، والدليل يعني المرشد، وجمعه أدلة، وكذلك يقصد بالدليل البرهان، بحيث يقال أقام الدليل أي بين وبرهن، وقد جاء في القرآن الكريم معنى الدليل بقول الله تعالى :"ألم تر إلى ربك كيف مد الظل ولو شاء لجعله ساكنا ثم جعلنا الشمس عليه دليل ." سورة الفرقان، الآية 45.[2]

وأما كلمة "الرقمي" فهو إسم منسوب للدليل، وأصلها "رقم" جمعها أرقام، وهي علامات الأعداد المعروفة، وينصرف إلى معناها أيضا كلمة عدد، وجمعها أعداد.[3]

اصطلاحا: اجتهد العديد من فقهاء القانون الجنائي في إيجاد تعريف مناسب للدليل الجنائي الرقمي في ظل عدم توافر تعريف قانوني له، فالمشرع الجزائري إلى تعريف الدليل الرقمي ونفس الشيء بالنسبة للمشرع الفرنسي، ولهذا سأقوم بعرض بعض التعريفات التي أتى بها فقهاء القانون الجنائي فقد عرفه البعض بأنه:" الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل موجات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم وذلك من أجل اعتماده أمام أجهزة تنفيذ وتطبيق القانون ويتم اعتماده كدليل أمام القضاء[4].

الدليل الجنائي الرقمي:" هو عبارة عن ذبذبات أو نبضات الكترونية مسجلة على وسائط أو دعائم مادية " [5].

الدليل الجنائي الرقمي:" الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الالكترونية من معطيات الحاسوب وشبكة الانترنت، والأجهزة الالكترونية الملحقة والمتصلة به وشبكات الاتصال، من خلال إجراءات قانونية لتقديمها للقضاء كدليل الكتروني جنائي يصلح لإثبات الجريمة"[6].

الدليل الجنائي الرقمي:" معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها

---

[1] عايدة بلعابد،الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية،مجلة آفاق العلمية،المجلد 11،عدد1، 2019، ص137.

[2] الآية 45 من سورة الفرقان.

[3] طاهر عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة مسيلة،2015، ص 02

[4] ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر، 2006، ص88.

[5] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الفكر الجامعي، مصر، 2009، ص176.

[6] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص230.

وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه".[1]

الدليل الجنائي الرقمي:" يشمل جميع المعلومات والبيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة، أو أنه عبارة عن مجموعة من معلومات أو بيانات ذات قيمة في التحقيق، والتي جرى تخزينها أو إرسالها عبر جهاز الكتروني[2].

ومن جهة أخرى تم تعريف الدليل الجنائي الرقمي من طرف مجموعة العمل العلمية للأدلة الرقمية بأنه:" مجموعة المعلومات القيمة التي تخزن أو ترسل في شكل رقمي"[3] .

وعرفته أيضا المنظمة الدولية لدليل الحاسوب:" بأن الدليل الجنائي الرقمي هو المعلومات التي جرى تخزينها أو إرسالها في شكل ثنائي، والذي يمكن أن تعتمد عليه المحكمة ".

والملاحظ من خلال التعريفات السابقة للدليل الرقمي أنها تحصر مفهومه في ذلك الدليل الذي يستخرج من الحاسب الآلي ولا شك في أن ذلك فيه تضييق لدائرة الأدلة الرقمية فهي كما يمكن أن تستمد من الحاسب الآلي من الممكن أن يتحصل عليها من أية آلة رقمية أخرى، فالهاتف وآلات التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدرا للدليل الرقمي .

الفرع الثاني: خصائص الدليل الرقمي .

على غرار خصائص ومميزات الجريمة المعلوماتية والمجرم المعلوماتي، أيضا يتميز الدليل الرقمي بخصائص تميزه عن باقي الأدلة الجنائية فهو أداة مبتكرة تستخدم لتقديم المعلومات والإرشادات عبر وسائل التكنولوجيا الحديثة مثل: الانترنت والتطبيقات الذكية، وهو الوسيلة الفعالة لعرض المحتوى بشكل منظم وتفاعلي حيث يوفر للمستخدمين تجربة سهلة للوصول إلى المعلومات ومن بين خصائص الدليل الرقمي :

أولا: الدليل الرقمي دليل علمي.

يتكون الدليل الرقمي في أساسه من مجموعة من البيانات والمعلومات ذات صبغة الكترونية غير ملموسة يتم إدراكها بواسطة أجهزة ومعدات وأدوات الحاسبات الآلية والاستعانة بنظم برامجية حسابية، هذا يجعل من الدليل الرقمي أدلة علمية حديثة، نظرا لبيئته التقنية في المجال الافتراضي، كما أنه وباعتبار الدليل الرقمي عبارة عن نبضات رقمية ذات طبيعة ديناميكية تتميز بالسرعة الفائقة المتعدية لحدود الزمان والمكان كل هذا يجعل الدليل الرقمي دليل يعتمد على التقنيات بالدرجة الأولى.[4]

---

[1] خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب، مرجع سابق، ص 230

[2] The technical working group for electronic crime science investigation [electronic crime investigation] the national institute of justice the united state of America 2001 page 6

[3] طيب بلواضح، أدلة الإثبات الجنائي، ط1،مكتبة الوفاء القانونية، الجزائر، كلية الحقوق، المسيلة، 2022، ص78.

[4] عمر محمد بن يونس،الدليل الرقمي،دون دار النشر،مصر،2006 ص 07

ثانيا : الدليل الرقمي ذو طبيعة تقنية .

ومفاد هذه الخاصية أن يتم التعامل مع الدليل الرقمي من قبل مختصين في العالم الافتراضي وفي الدليل الالكتروني، لأن هذا الأخير ليس كدليل، فهو عبارة عن ذبذبات الكترونية تكمن قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب في أي شكل يكون عليه، وعلى اثر ذلك قام المشرع البلجيكي بتعديل قانون التحقيق الجنائي بمقتضى القانون 28 نوفمبر 2000 كذلك بالنسبة للمشرع الأمريكي الذي قام بتدعيم تقنيات التحقيق الكاملة، وهو ما يستفاد من خلال الفصل بين الخبرة وسلطات الاستدلال والتحقيق فيها يتعلق بالدليل الرقمي مع توافر هذه السلوكيات على عناصر ذات خبرات عالية الكفاءة فيما يخص هذا الدليل[1] .

ثالثا : الدليل الرقمي يصعب التخلص منه.

من أهم ما يميز الدليل الرقمي 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 الرقمي على تطبيقات وبرامج لمعرفة ما إذا كان قد تعرض للعبث أو التحريف[2].

رابعا : الدليل الرقمي ذات طبيعة مزدوجة .

تعتبر الطبيعة المزدوجة التي يختص بها الدليل الرقمي 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 شكلا ثنائيا أو رقميا، ومراد ذلك أن الحاسب الآلي أو أي جهاز آخر له نفس خصائصه يقوم باستقبال هذه البيانات والمعلومات وتحويلها إلى أرقام ثم معالجتها .

فمضمون الطبيعة المزدوجة للدليل الرقمي، هو اختزال البيانات أو المعلومات كالنصوص أو الصور أو أي معلومة أخرى، إلى رموز ثنائية وهذه الرموز الثنائية تتكون من سلسلة من رقم الصفر ورقم واحد، ومثال ذلك أن الحرف (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.

---

[1] شهرزاد حداد، الدليل الالكتروني في مجال الإثبات الجنائي، مذكرة ماستر تخصص حقوق، كلية الحقوق والعلوم السياسية جامعة أم البواقي، 2017، ص14.

[2] أوشن حنان، وادي عماد الدين، الإثبات الجنائي والوسائل العلمية والحديثة، دار الخلدونية للنشر والتوزيع، الجزائر،2015، ص98-99.

خامسا: الدليل العلمي دليل متطور.

مصطلح الدليل الرقمي يشمل جميع البيانات والمعلومات الرقمية التي يمكن تداولها رقميا بمختلف أشكالها وأنواعها، سواء كانت هذه الأدلة متعلقة بالحاسب الآلي أو غيرها من الأجهزة، أو شبكة الانترنت، أو شبكة الاتصال السلكية واللاسلكية، ومنه فالآثار الرقمية المستخلصة من الحاسب الآلي أو شبكة الانترنت، تكون ثرية جدا ومتنوعة بما تحتويه من معلومات عن وقائع قد تشكل جريمة ما، وترتقي إلى أن تصبح دليل براءة أو إدانة، ومن بين هذه المعلومات صفحات المواقع الالكترونية المختلفة، البريد الالكتروني، النصوص والصور والفيديوهات الرقمية، الملفات المخزنة في الكمبيوتر الشخصي، والمعلومات المتعلقة بمستخدم شبكة الانترنت وغيرها ومنه فهذا التنوع إن دل على شيء فإنما يدل على اتساع قاعدة الدليل الرقمي، بحيث يمكنه أن يشمل أنواعا متعددة من المعلومات والبيانات الرقمية التي تصلح لأن تكون دليلا جنائيا ببراءة المتهم أو إدانته.[1]

سادسا: الدليل الرقمي له سعة تخزين عالية .

يتميز الدليل الرقمي بالسعة التخزينية العالية حيث يمكن لآلة الفيديو الرقمية تخزين مئات الصور ويمكن لقرص صغير أن يقوم بتخزين مكتبة صغيرة، كما أن الدليل الرقمي يمكنه رصد معلومات عن الجاني وتحليلها في ذات الوقت حيث يمكنه تسجيل تحركات الفرد وتسجيل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لهذا فان البحث الجنائي يجد غايته بسهولة أفضل من الدليل المادي التقليدي[2].

الفرع الثالث:تقسيمات الدليل الجنائي الرقمي.

يقصد بتقسيمات الدليل الجنائي الرقمي مجموعة الأنواع التي يتواجد في إطارها الدليل الرقمي ويلاحظ في هذا الإطار إلى أن هذه التقسيمات هي عبارة عن اجتهادات قضائية وفقهية وبالتالي يمكن أن تظهر هناك تقسيمات تأخذ بها بعض التشريعات بخلاف التشريعات الأخرى أو يأخذ بها بعض الفقه دون البعض الآخر ومن أهم التقسيمات :

أولا: التقسيمات الفقهية للدليل الرقمي .

القسم الأول: الأدلة الرقمية الخاصة بأجهزة الكمبيوتر: وتشمل على جهاز الحاسب الآلي وملحقاته كالطابعات وكذا المودم والأقراص المدمجة وذاكرة الفلاش والأشرطة الممغنطة [3].

القسم الثاني: الأدلة الرقمية الخاصة بالشبكة الدولية للمعلومات: كالبريد الالكتروني وغرف المحادثات .

القسم الثالث: الأدلة الخاصة بالبروتوكولات نقل وتبادل المعلومات بين الأجهزة المتصلة بشبكة الانترنت[4].

---

[1] أسامة حسين محي الدين عبد لعالي، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والاقتصادية، العدد76، جوان 2021، ص645.

[2] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في قانون جزائري، جامعة إسكندرية،2010، ص 42

[3] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص82.

[4] بروتوكول (transmission protocol control / internet protocol)(TPC/IP)

القسم الرابع: الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات.

ثانيا:التقسيمات التشريعية والقضائية للدليل الرقمي:

أشارت وزارة العدل الأمريكية سنة 2002 إن الدليل الرقمي أشكال مختلفة وقد قسمت إلى ثلاث أقسام :

القسم الأول: السجلات المحفوظة في الحاسوب: وتشمل الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني ورسائل غرف الدردشة وملفات برامج معالجة الكلمات.

القسم الثاني: السجلات التي تم إنشائها بواسطة الحاسوب: وتعد مخرجات أصلية للحاسوب حيث لم يشارك الأشخاص في إعدادها مثل سجلات الهاتف وفواتير أجهزة السحب الآلي للنقود.

القسم الثالث: السجلات المختلطة: التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه عن طريق حاسب آلي ومنها أوراق العمل المالية التي تم حفظها بالإدخال ثم معالجتها عن طريق برنامج Excel لإجراء العمليات الحسابية عليها.

ثالثا: تقسيم الأدلة الجنائية بحسب مصدرها.

1- الدليل القانوني: وهو مجموع الأدلة التي حددها المشرع وعين قوتها والثبوتية في المواد المدنية أما في المسائل الجنائية غير المحصورة والقاضي حر في تكوين عقيدته ولكن في بعض الأحيان تكون استثناءات على حريته في الإثبات والاقتناع .

2- الدليل الفني: هو الدليل الذي ينبعث من رأي الخبير الفني بناء على معايير علمية فهو يتمثل عادة في الخبرة .

3- الدليل القولي: هو الدليل الذي ينبعث من أشخاص أدركوا معلومات مفيدة للإثبات بإحدى حواسهم كالإعتراف .

4- الدليل المادي: هو الدليل الناتج عن عناصر مادية ناطقة بنفسها ولها تأثير على اقتناع القاضي بطريقة مباشرة .

المطلب الثاني: أنواع الأدلة الجنائية الرقمية .

مع التطور الهائل في التكنولوجيا الرقمية واعتماد المجتمعات بشكل كبير على الوسائل الالكترونية في مختلف الأنشطة اليومية، أصبحت الجرائم المعلوماتية تهديدا حقيقيا للأفراد والمؤسسات والحكومات، نتيجة لذلك ظهرت الحاجة إلى توظيف الأدلة الرقمية الجنائية في التحقيقات كونها وسيلة فعال لكشف الحقائق وإثبات الجرائم، فالأدلة الرقمية ليست مجرد بيانات عادية بل هي معلومات الكترونية تستخرج من أجهزة وأنظمة تقنية متنوعة مثل: الحواسيب، الهواتف الذكية، شبكات تستخدم هذه الأدلة لتوضيح ملابسات الجريمة ولتنظيم عملية جمع وتحليل الأدلة

هو مجموعة من البروتوكولات القياسية التي تستخدم لربط الأجهزة والشبكات المختلفة عبر الانترنت أو الشبكات المحلية، ويعتبر العمود الفقري للشبكة الانترنت الحديثة، ويحدد كيفية تبادل البيانات بين الأجهزة بطريقة موثوقة ومنظمة.

(كوكيز cookies) هي ملفات نصية صغيرة تخزن على الجهاز المستخدم كمبيوتر،هاتف بواسطة مواقع الويب التي تزورها تستخدم لتتبع نشاط المستخدم و تخزين المعلومات تسهل تجربة تصفح (المصدر بن فردية محمد الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية).

الرقمية ظهرت تصنيفات متنوعة تساعد الخبراء والمحققين في فهم مصادر الأدلة وأهميتها[1] حيث يمكن تصنيفها إلى أنواع مختلفة وهي :

الفرع الأول: أنواع الأدلة الرقمية من حيث نشأتها.

1- أدلة معدة لتكون وسيلة للإثبات: وهذه الأدلة تكون عبارة عن مخرجات للحاسب الآلي أو ملحقاته، أو لشبكات المعلومات أو ما في حكمها، وهي تنشا نتيجة تعامل الإنسان معها، وعادة ما يكون له دور في إنشائها، وتكون بهدف إثبات واقعة معينة، أو إثبات إرتباطها بشخص ما .

2- أدلة غير معدة لتكون وسيلة للإثبات: وهذه الأدلة تكون عبارة عن بيانات ينشئها النظام بشكل تلقائي عند كل تعامل يجري معه، حيث تسجل فيه أطراف الرسالة وتاريخها، وجهة إصدارها، وحجمها، وكذلك نوع الخدمة التي تدور حولها، فهي بيانات تنشأ بطريقة آلية نتيجة تعامل الإنسان معها، ويكون مصدر إنشائها الحاسب الآلي أو الجهاز الرقمي دون تدخل من الإنسان، وهي ما يطلق عليها الآثار الرقمية أو البصمة الرقمية[2].

الفرع الثاني: أنواع الأدلة الجنائية الرقمية من حيث مصدرها[3].

1- الأدلة الرقمية الخاصة بأجهزة الحاسب الآلي وشبكاتها: وهذه الأدلة تكون مخزنة على الأجزاء الصلبة للحاسب الآلي عادة أو على وسائط التخزين المتعلقة بالشبكات المعلوماتية.

2- الأدلة الرقمية الخاصة بالشبكة الدولية للمعلومات: وهي شبكة عالمية تتكون من مجموع أجهزة الحاسب الآلي وملحقاتها، وكذلك مجموعة الشبكات المحلية، سواء أكانت محدودة أو موسعة، وذلك من أجل التشارك وتبادل المعلومات بين مستخدميها.

3- الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين الشبكة الدولية للمعلومات: أو ما يطلق عليها بروتوكول التحكم في نقل البيانات، و بروتوكول الانترنت.

الفرع الثالث: أنواع الأدلة الرقمية بالنظر لأشكالها.

1- الصور الرقمية: وهي ملفات تأتي بأحجام وتنسيقات مختلفة، ويمكن فتحها على شاشات الأجهزة الرقمية، ويمكن أن تكون هذه الصور بلون واحد أو أكثر، وتمثل الصورة الرقمية لتظهر ثنائية البعد على أجهزة العرض، وذلك عن طريق برامج خاصة تكون قادرة على عرض الصور على الشاشات، هذه البرامج تعرف بإسم "مستعرضات الصور"[4].

2- الفيديوهات الرقمية: هي تمثيل لحركة الصور المرئية في شكل بيانات رقمية مشفرة، وهي عكس الفيديو العادي الذي يمثل حركة الصور المرئية بإشارات تناظرية، وهي فيديوهات يتم تسجيلها بواسطة الأجهزة الرقمية.

---

[1] أسامة حسن محي الدين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، مرجع سابق، ص 655-656

[2] علي محمود إبراهيم، الأدلة الرقمية وحجتها في إثبات الجرائم الالكترونية، المجلة العلمية، كلية الشريعة والقانون، جامعة الأزهر، العدد32، إصدار 02 جويلية 2020، ص1088.

[3] يسرى بهاء الدين الجاسم، حجية الأدلة الرقمية في النظام القضائي الإسلامي، مجلة البحوث الفقهية الإسلامية، تركيا، العدد 37، نوفمبر 2021، ص176-177

[4] يسرى بهاء الدين الجاسم، حجية الأدلة الرقمية في النظام القضائي الإسلامي، مرجع سابق، ص178.

3- التسجيلات الصوتية: هي التي يتم تسجيلها بواسطة الأجهزة الرقمية، والفائدة الأساسية للصوت الرقمي هي تخزين واسترجاع وبث الإشارات من دون أي تدني في مستوى جودة الصوت، كذلك فإن توزيع المواد الصوتية كملفات بيانات رقمية وليس كأشياء مادية "شرائط، أقراص" قد ساهمت بشكل ملحوظ في تخفيض تكاليف التوزيع[1].

4- النصوص المكتوبة: هي النصوص التي تتم بواسطة الأجهزة الرقمية، أو بمعنى آخر هي كل نص ينشر الكترونيا، سواء كان على شبكة الانترنت أو على أقراص مدمجة أو في شكل كتاب الكتروني، ويقصد بعملية ترقيم النص تحويل النص المكتوب المطبوع أو المخطوط من صيغته الورقية إلى صيغته الرقمية، ليصبح قابلا للمعاينة على شاشة الحاسب الآلي[2].

الفرع الرابع: أنواع الأدلة الرقمية من حيث تركيبتها[3].

1- التسجيل الرقمي البسيط: هو التسجيل الذي يظهر أمرا قد حدث في الواقع المادي أي أن له شكل مادي ملموس، كالصور الرقمية أو التسجيلات الصوتية، بحيث يتم تحويل هذا التسجيل الرقمي إلى شكله المادي مرة أخرى بواسطة مخرجات الحاسب الآلي، كالطباعة الورقية للنصوص الرقمية، أو استخدام معالجات النصوص لمشاهدتها على شاشة الحاسب، أو إظهار الصورة الرقمية على شاشة الحاسب الآلي أو الاستماع إلى التسجيلات الرقمية .

2- التسجيل الرقمي المركب: أو ما يطلق عليه سلسلة التسجيلات الرقمية، وهنا يكون الدليل سلسلة من التسجيلات الرقمية المرتبطة ببعضها البعض، كالتوقيع الرقمي الذي يتم التثبت من مصداقيته من خلال علاقات معينة، ويكون مرتبطا بالمصدر لهذا التوقيع، وعلى العكس من التسجيل الرقمي البسيط، الذي يكون قابلا للتلاعب به ومحوه، فإن التسجيل الرقمي المركب يتمتع بدرجة مصداقية أكبر، حيث يمكن التأكد من صحته بشكل أيسر من التسجيل الرقمي البسيط.

المطلب الثالث: مراحل الدليل الرقمي في الإثبات الجنائي .

يشهد العالم اليوم تطورا متسارعا في مجال التكنولوجيا الرقمية، ما أدى إلى تغيرات جذرية في أنماط الجريمة ووسائل ارتكابها، ولم تعد الجرائم محصورة في الفضاء الواقعي، بل امتدت لتشمل الفضاء الالكتروني، مما استوجب على أجهزة العدالة الجنائية تطوير أدواتها وأساليبها بما يتناسب مع هذه المستجدات، في هذا السياق برز الدليل الرقمي كأداة إثبات حديثة تلعب دورا محوريا في التحقيق والمحاكمة، لما يتميز به من قدرة على كشف الجرائم الالكترونية وغير الالكترونية المرتكبة باستخدام أجهزة أو شبكات رقمية، ونظرا للطبيعة الخاصة لهذا النوع من الأدلة التي تتسم بالتعقيد التقني والحساسية العالية، فقد أصبح من الضروري اعتماد منهجية دقيقة في جمعه وتحليله وتقديمه أمام الجهات القضائية لضمان مشروعيته وحجيته في الإثبات، من هنا يكتسي موضوع مراحل الدليل الرقمي في الإثبات الجنائي أهمية خاصة، باعتباره مسارا يحدد الضوابط الفنية والقانونية التي ينبغي

---

[1] فاطمة جخدم، النصوص الرقمية المفهوم والخصائص، مجلة المزهر، أبحاث في اللغة والأدب، معهد الآداب واللغات، المركز الجامعي، سي الحواس، بريكة، باتنة، العدد6، جوان 2022، ص93.

[2] فاطمة جخدم، النصوص الرقمية المفهوم والخصائص، نفس المرجع ، ص 95.

[3] يسرى بهاء الدين الجاسم، حجية الأدلة الرقمية في النظام القضائي الإسلامي، المرجع السابق، ص 178

الالتزام بها خلال دورة حياة هذا الدليل من لحظة اكتشافه إلى غاية عرضه أمام المحكمة، ومنه ستتم دراسة هذه المراحل في الفروع الآتية:

الفرع الأول :مرحلة التحريز.

هو الاحتفاظ بالأدلة الموجودة عن طريق إرسالها إلى المختبر الجنائي بطريقة لا تمكنها من التلف أو الكسر أو الإفساد، كما يتم أيضا التقاط الصور الفوتوغرافية أو بواسطة الفيديو لجميع آثار الجريمة كالحواسيب وملحقاتها والبصمات وكل الأشياء التي تفيد في إظهار الحقيقة، والتي تم العثور عليها في مسرح الجريمة المعلوماتية، وأثناء هذه المرحلة يكون المحقق أو الخبير في وضع لا يعرف أي نوع من البيانات يمكن من خلالها الحصول على الدليل الجنائي الرقمي، وعليه الحفاظ على النظام الرقمي وكامل القيم الرقمية ليتم تحديد الضرورية منها لاستخلاص الدليل لاحقا، وكذلك يستلزم نسخ جميع البيانات المخزنة داخل الحاسب الآلي موضوع الجريمة إلى الحاسب الخاص بالمختبر الجنائي الرقمي للاعتماد عليه بالإضافة إلى نسخ البيانات المخزنة داخل جهاز الحاسب الآلي المشكوك فيه[1] .

الفرع الثاني: مرحلة التحليل

يتم في هذه المرحلة القيام بالفحص، والتحليل لجميع الآثار المرتبطة والمستمدة من مسرح الجريمة ويشمل ذلك القيم الرقمية لتحديد نوع الدليل حيث يتم الفحص في محتويات الوثائق والملفات والمسارات واستعادة المحتويات التي تم حذفها ويجب أن يتم الفحص بالصيغة العلمية عن طريق استخدام البرامج والتطبيقات الخاصة بتحليل نظام الملفات والمسارات، بالإضافة إلى ذلك يمكن من خلال تحضير قائمة البيانات المحذوفة وعرض البيانات المخزنة على شك forma للاستفادة منها والأمر المهم جدا في هذه المرحلة وجوب قيام الفحص والتحليل على نسخ مطابقة الأصل لعدم تغيير خصائص الملفات حيث يتم الإحتفاظ بالنسخة الأصلية المضبوطة من اجل التحقيق والتدقيق على أن البيانات الموجودة مطابقة للأصل ولم يطرأ عليها أي تغيير أو حذف ويهدف من وراء قيام عملية الفحص والتحليل إلى استنباط ثلاثة أنواع من الأدلة :

أ- دليل الإدانة: ويعد الدليل المؤكد والمستند إلى وجود فكرة معينة على ارتكاب وإسناد الجريمة محل التحقيق .

ب- دليل البراءة: يعتبر الدليل الذي يخالف فكرة ارتكاب الجريمة موضوع التحقيق .

ج- دليل محايد: هو الدليل المرتبط لا بالإدانة لا بالبراءة بل يستعان به في إثبات انه لم يطرأ أي تعديل أو تغيير في النظام الرقمي للحاسب الآلي لاستبعاد استخدام محتوياته أو الاستعانة به كدليل[2].

الفرع الثالث: مرحلة التقديم و العرض.

هي التي يتم من خلالها تقديم وعرض النتائج التي تم التوصل إليها عن طريق التحقيقات والفحص والتحليل الفني إلى جهة المحكمة المختصة، ويطبق على عملية هذه المرحلة النظام الجنائي

---

[1] معمش زهية، غانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرا، بجاية، 2012-2013، ص61.

[2] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص125.

المطبق في تلك الدولة ويستلزم الأمر موثوقية الأدلة الجنائية الرقمية لضمان مصداقيتها حيث أنه يمكن توثيق الأدلة الجنائية الرقمية بالعديد من الوسائل المختلفة منها التصوير الفوتوغرافي، التصوير بالفيديو والقيام بنسخ الملفات المخزنة في الأقراص أو في الحاسب الآلي كما يستوجب تدوين التاريخ والوقت وتوقيع الشخص الذي قام بإجراء الحفظ عند حفظ الأدلة الرقمية، بالإضافة إلى إسم ونوع نظام التشغيل والمعلومات المسجلة في الملف المحفوظ وقسم البرامج أو الأوامر التي استعملت في إعداد النسخ.

فالتوثيق يفيد تأكيد مصداقية الدليل وعدم القيام بتعديله أي تغييره مثل شهادة الأفراد المسؤولين عن جمع الأدلة ومطابقتها مع تلك التي قاموا بتحصيلها والحفاظ عليها مع تلك الأدلة المقدمة والمعروضة لجهة الحكم، كذلك يمكن الإستفادة من التوثيق في حالة إعادة تكوين مسرح الجريمة بإعتبار أن أجهزة الحاسب الآلي وملحقاتها تتشابه، مما يصعب إعادة تنظيمها في حالة إنعدام وجود حالة توثيق فوتوغرافي أو توثيق فيديو سليم ومفصل يقوم بتحديد أجزاء ومكونات بأوضاعها وحالتها الأصلية بدقة، وبالتالي يعتبر التوثيق من ضمن إجراءات حفظ الأدلة إلى غاية الإنتهاء من إجراءات التحقيق والمحاكمة لاحتوائه على تحديد دقيق على الجهات التي تحتفظ بالأدلة، بالإضافة إلى إعداد رسالة التصنيف الحسابي التي تستعمل لمضاهاة الأدلة الجنائية الرقمية الرسمية مع النسخ من أجل التأكد من صحتها وأنها لم تتعرض للتحريف أو التعديل، فهي تعتبر مجموعة من الأحرف والأرقام المركبة والمنظمة بصيغة حسابية خاصة تمثل كل نوع من البيانات الرقمية ففي حالة إدخال ملف الدليل الرقمي على رسالة التصنيف تكون قراءة الملف مطابقة لقراءة النسخة الأصلية لنفس الملف بالأحرف والأرقام، أما في حالة تحريف أو تعديل في النسخة فنتيجة المضاهاة تكون قراءة مختلفة ومغايرة للنسخة الأصلية[1].

الفرع الرابع: مرحلة القبول.

إن أمر قبول الأدلة الجنائية الرقمية المستخرجة من الوسائل الإلكترونية في المحاكم يعتمد على المبادئ القانونية التي تنظم عملية الإثبات أمام تلك المحاكاة أو بعبارة أخرى أن سلطة القاضي الجنائي في تقدير أدلة الإثبات تختلف من دولة إلى أخرى حسب ما تخضع له قواعد الإثبات في كل دولة حيث يتضح وجود نظامين للأدلة الإثباتية، نظام الإثبات المحدد أو المقيد وأطلق عليه أيضا نظام الأدلة القانونية أين تكون الأدلة فيه محصورة ومقيدة مسبقا من طرف المشرع، أما النظام الثاني هو نظام الأدلة الإقناعية والمسمى بحرية الإقتناع، إذا فإن كرحلة قبول الأدلة الجنائية الرقمية في الإثبات موقوفة إلى مدى توافر هذا الدليل في النصوص القانونية بالنسبة لنظام الإثبات المحدد، وإلى مدى إقتناع القاضي الجنائي للدليل الرقمي بالنسبة لنظام الأدلة الإقناعية[2].

---

[1] سيدي محمد البشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص87.

[2] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، مرجع سابق، ص127-128.

الفصل الثاني: طرق إثبات الجرائم المعلوماتية باستخدام الأدلة الرقمية

الفصل الثاني : طرق إثبات الجرائم المعلوماتية باستخدام الأدلة الرقمية.

نظرا لخطورة الجريمة المعلوماتية في حد ذاتها فهي مجموعة معطيات وذبذبات الكترونية يصعب على الجاني القيام بعمل إجرامي دون ترك آثار ودون أن يستغرق هذا العمل وقتا طويلا وهو ما يجعلها صعبة الاكتشاف والإثبات، الأمر الذي أدى إلى ظهور مشكلات إجرائية أثناء التحقيق وأمام القاضي الجزائي عند الفصل في الدعوى المعروضة أمامه كونها حديثة النشأة، ولا يمكن تطبيق النصوص التقليدية عليها لذلك عمد المشرع إلى وضع قواعد إجرائية لإستخلاص جميع الأدلة التي يمكن بها إدانة المتهم أو تبرأته من الجرم المنسوب إليه، فصعوبة إثبات مثل هذه الجرائم يرجع إلى الطبيعة الخاصة للدليل الرقمي فهو ليس بدليل مرئي يمكن فهمه بمجرد القراءة، إلى جانب صعوبة الوصول إليه وإستخلاصه، وهذا نتيجة قيام كبرى المواقع العالمية الالكترونية بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية لمنع التسلل والوصول إليها لتدميرها، أو تبديلها، أو الاطلاع عليها، أو نسخها كما يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه من خلال استخدامه لكلمات المرور بعد تخريب الموقع مثلا أو استخدامه لتقنيات التشفير، لذلك لم تكثف التشريعات الحديثة بحماية معطيات الحاسب الآلي بصفة عامة من خلال تجريم صور الاعتداء عليها أي الحماية الموضوعية إنما وضعت مجموعة من الإجراءات الخاصة باستخلاص الأدلة الرقمية منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الخاصة بالمعطيات ومنها ما لا يطبق إلا على الجريمة المعلوماتية[1] .

المبحث الأول :إجراءات استخلاص الدليل الرقمي .

انتهجت السياسة الجنائية الحديثة عدة طرق وأساليب إجرائية للوقاية من الجريمة المعلوماتية وقمعها، والجريمة الرقمية من بين هذه الجرائم التي يتطلب التحقيق فيها من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه واستخلاص الدليل يتم عن طريق محاضر الضبطية القضائية بل يستلزم الأمر في بعض الجرائم الإنتقال لإجراء معاينات مادية وعمليات تفتيش وضبط وهي نفس الإجراءات المتبعة في الجرائم التقليدية، كما أن عملية الحصول على الدليل الرقمي أمر صعب الوصول إليه لما تتطلبه من خبرة ومهارة كبيرة في مجال التكنولوجيا الرقمية بالإضافة إلى تعدد صور وأشكال الجريمة المعلوماتية وسرعة تنفيذها وللحصول على هذا النوع من الأدلة الجنائية يجب اتباع طرق ووسائل فنية وإجراءات حديثة[2] .

المطلب الأول: الإجراءات المادية الخاصة بالتحقيق في الجرائم الرقمية .

في ظل التطور السريع للتكنولوجيا وانتشار استخدام الانترنت في مختلف مناحي الحياة، ظهرت أنواع جديدة من الجرائم تعرف بالجرائم الرقمية التي تستهدف البيانات والأنظمة المعلوماتية ونظرا لطبيعتها الخاصة، فإن التحقيق في هذه الجرائم يتطلب إجراءات مادية وتقنية دقيقة تختلف عن

---

[1] جليلة بلعلمي، صالح مزري، الدليل الرقمي والإثبات الجنائي، مذكرة الماستر، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2021-2022، ص06.

[2] نفس المرجع، ص06-07.

الأساليب التقليدية المتبعة في الجرائم العادية، وتنفذ من طرف متخصصين في التحليل الجنائي الرقمي لضمان استخلاص الأدلة بشكل صحيح وقانوني يمكن الإستناد إليه أمام القضاء وتكمن أهمية هذه الإجراءات في كونها الأساس الذي يبنى عليه مسار التحقيق والمحاكمة، إذ أن أي خطأ في جمع أو حفظ الأدلة قد يؤدي إلى ضياع الحق أو بطلان الدعوة[1]، وتشمل الإجراءات المادية مجموعة من الخطوات الأساسية هي:

الفرع الأول: المعاينة.

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة لإجراء المعاينات للأزمة لأن هذا هو حجر الأساس في التحقيق الجنائي، ولذلك تعتبر المعاينة من أهم إجراءات التحقيق لأهميتها القصوى في إثبات الواقعة الإجرامية فالهدف منها هو جمع الآثار الناتجة عن الجريمة وإتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة، فإجراء المعاينة في الجرائم المعلوماتية، هي معاينة الآثار التي يخلفها مستخدم الشبكة المعلوماتية، كالرسائل المرسلة منه أو التي استقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية فإجراءات المعاينة في مسرح الجريمة الرقمية تتم عن طريق اتباع بعض القواعد والإرشادات الفنية عند معاينة مسرح الجريمة المعلوماتية وتتمثل في :

1- عند العثور على حاسبات آلية أو أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها فيجب تدوين الحالة التي هي عليها إذا كانت منطفئة أما في حالة التشغيل ينبغي ترقيم لواحقها بشكل متسلسل.

2- يجب تحرير الأوراق المطبوعة على الحاسب الآلي والتي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالتها ويمكن إعادة الطباعة إذا كان الجهاز في حالة تشغيل وتحرير الأوراق التي تمت طباعتها بالإضافة إلى تفقد الجهاز وتسجيل ما إذا كانت هناك برامج تم إستخدامها لحظة دخول مسرح الجريمة[2].

3- عند العثور على دعائم التخزين (أسطوانات، أقراص، حوامل مغناطيسية) يجب ترقيمها وتسجيل الحالة التي هي عليها والمكان الذي وجدت فيه داخل الحاسب الآلي أو خارجه .

4- عند الانتهاء من الترقيم يجب تصوير الأجهزة وملحقاتها في الحالة التي هي عليها .

5- يجب تحرير جميع العينات التي عثر عليها من أجهزة ودعائم داخل أكياس خاصة (بلاستيكية أو ورقية) كما ينبغي حمايتها من الكسر وتأثير العوامل الجوية وأبعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات وإرسالها إلى المخبر لإجراء الخبرة.

ويعتمد المحقق الجنائي لإجراء المعاينة الإلكترونية بحثا عن الأدلة الرقمية على فحص مجموعة من المصادر.

---

[1] Marie Christine droit pénal général Ed ellicses parie France 2002 p15

[2] نبيلة هبة هروال، الجوانب الإجرائية لجوانب الانترنت في مرحلة جمع الإستدلالات، دار الفكر الجامعي، الإسكندرية، 2013، ص212.

أولا: معاينة مكونات الحاسب.

تعتبر الحواسيب مصدرا غنيا بالأدلة الالكترونية خاصة الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوك الأفراد ونشاطاتهم ورغباتهم، لذلك فإن عملية فحص هذه الحواسيب تمثل نقطة البداية في الكشف عن خفايا الجريمة بإعتبار هذه الأجهزة وسيلة تنفيذها أو محل وقوعها، والمعروف أن الحاسب الآلي هو العنصر الذي يتوزع بين القطع الصلبة والبرمجيات[1]، فمعاينة هذا الحاسب يستلزم الفحص المادي والمعنوي لكل هذه العناصر وتعتمد هذه العملية على طريقتين أساسيتين، الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكوناته وتقديم تقرير كامل إلى طالب الفحص، أما الطريقة الثانية فهي الفحص بواسطة حاسب إلى آخر أو أجهزة تقنية عالية للبحث في جزئيات عبر الحاسب[2].

ثانيا: معاينة القرص الصلب.

يتم معاينة القرص الصلب للحاسب الآلي بالفحص الجزئي أو الكلي للبيانات الرقمية ذات الطابع الثنائي المتواجدة بداخله، والتي تتميز بعدم التشابه الذي يتكون منه تفصيل هذه البيانات[3]، ولتحقيق ذلك يقوم المحقق بنزع القرص من الحاسب المراد فحصه بكل عناية وحذر من كل إرتجاج أو إصطدام بأي شيء تفاديا لإتلافه أو تعطيله أو فقد أي بيانات، ثم يقوم بفحص وتحليل النسخ الذي يصدر من القرص نفسه أو بواسطة خبير مختص[4].

ثالثا: معاينة البرمجيات.

يتبع المحقق في هذه العملية طريقتين هما الفحص الداخلي الذي يتم من خلال البحث عن البناء المنطقي للبرمجية بما يكشف عن وجود مجهود تجديديا في إعداده للعمل عند إنزاله في جهاز الحاسب الآلي ولعل أكثر ما يسعى إليه المحقق هو مصدر الملفات الموجودة داخل البرمجيات التي تفيد في ترتيب حدوث الجريمة المعلوماتية والتعرف على الكيفية التي تم الإعداد لها[5] ، أما الفحص الخارجي فيتم بواسطة البحث عن البناء المنطقي للبرمجية للتأكد من نسخه ومن ثم مقارنته بالنسخة الأصلية للدلالة على ثبوت إرتكاب الجريمة بدرجة مقنعة[6].

رابعا: معاينة النظام المعلوماتي.

فهو يتكون من بيانات ثنائية رقمية يتم إيداعها الحاسب الآلي في شكل تخزين ثم يقوم الحاسب بمعالجتها آليا وإبرازها على هيئة معلومة، فالمهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر الموجهة من طرف مستخدم الحاسب والاستجابة لها[7].

---

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الانترنت، جامعة المنصورة،كلية الحقوق، 2004، ص1009.

[2] نفس المرجع، ص1101.

[3] حسين بن سعيد بن يوسف الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة الجزائر، 2014، ص426.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص215.

[5] حسين بن سعيد بن يوسف الغافري، مرجع سابق، ص427.

[6] عمر محمد أبو بكر بن يونس، مرجع سابق، ص131.

[7] حسين بن سعيد بن يوسف الغافري، مرجع سابق، ص430.

فمعاينة النظام المعلوماتي للحاسب هو قيام المحقق بفحص وضبط كافة المعلومات المخزنة في ذاكرة تخزين الحاسب على شكل ملفات التي يمكن إستهدافها عبره بأية حركة إسترادادية ممكنة مادام موضوعها يشكل جريمة[1].

الفرع الثاني: التفتيش في الجرائم الرقمية .

يثير موضوع التفتيش الذي يقع على نظم الوسائل الالكترونية مسائل عديدة للبحث، منها الضوابط القانونية التي تحكم التفتيش كالضوابط الشكلية والموضوعية، وكذلك الكيانات المادية والمعنوية للحاسوب كمحل يرد عليه التفتيش، وأيضا تفتيش الوسائل الالكترونية الأخرى التي تشمل تفتيش البريد الالكتروني، وتفتيش أجهزة الهواتف النقالة والبحث في مدى إلتزام المتهم والشاهد المعلوماتي بتقديم الدليل الالكتروني، وكذلك الأثر المترتب على التفتيش[2].

أولا: الضوابط الشكلية .

وتتمثل هذه الضوابط في :

أ- **صدور إذن بالتفتيش:** الأصل في إذن التفتيش أنه إجراء لا يصح إصداره إلا لضبط جريمة وقعت بالفعل وليس لضبط جريمة مستقبلية أو محتملة، وهناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحريته الشخصية هذا إذا كان التفتيش في الجرائم التقليدية[3] .

أما بالنسبة للتفتيش في الجرائم الالكترونية فلابد من صدور إذن بالتفتيش من الجهة المختصة بإصداره وأن يكون هذا الإذن مبنيا على سبب يبرر إصداره، كونه أكثر خطورة على حريات الأفراد وحياتهم الخاصة ويعد الإذن بالتفتيش من الشروط المهمة التي يجب توافرها لصحة هذا الإجراء وبدون هذا الإذن يبطل إجراء التفتيش، لأنه من الإجراءات المهمة التي تمس حرمة الحياة الخاصة للأفراد .

ب- وقت إجراء التفتيش: يعد الميقات الزمني من الأمور المهمة جدا والتي تساعد في الحصول على الدليل الالكتروني في الجرائم المعلوماتية، وذلك لأنه من السهل جدا إتلافه ومحوه من قبل المتهم قبل وصول السلطات التحقيقية إليه، لذلك كلما كان إجراء التفتيش في وقت قريب بعد ارتكاب الجريمة كانت فرصة الحصول على الأدلة أكبر لأن الحصول على الدليل في الجرائم الالكترونية يتطلب السرعة في إجراء التفتيش في أي وقت ليلا كان أو نهارا ولقد اختلفت التشريعات الإجرائية في تنظيمها لوقت إجراء التفتيش من قبل القائم به[4] .

إن إجراء التفتيش بحثا عن الدليل الالكتروني يختلف باختلاف الأسلوب الذي يتبعه القائم بالتفتيش، فإذا قام بتفتيش الحاسوب أو الهاتف النقال أو أي وسيلة الكترونية أخرى في محل وجوده فان حضور الشهود ضروري كضمانة لعدم تعسف القائم بالتفتيش أو إتهامه بدس الأدلة ويجب أن

---

[1] خالد ممدوح إبراهيم، مرجع سابق، ص222.

[2] رفه خضير جياد العارضي، الدليل الالكتروني وأثره في مجال نظرية الإثبات الجنائي، ط1، مكتبة زين الحقوقية والأدبية، لبنان، 2019، ص114.

[3] إيهاب علي المطلب، الموسوعة الجنائية الحديثة في شرح قانون الإجراءات الجنائية، ج1، المركز القومي، الإصدارات القانونية عابدين، 2009، ص663-664.

[4] فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، ط1، مطبعة الشرطة، دار الثقافة، عمان، 2005، ص63.

يكون الشهود من الأشخاص الملمين بتقنية الحاسوب وإلا فان وجودهم لا فائدة منه، لأن أي تلاعب من قبل القائم بالتفتيش لن يكتشف إلا من أشخاص متخصصين أو على الأقل لديهم معلومات كافية عن تقنيات الحاسوب أو الوسائل الالكترونية المختلفة وهو ما يطلق عليه بالشاهد المعلوماتي .

أما إذا ضبط القائم بالتفتيش الجهاز تمهيدا لنقله إلى مختبرات تحليل الدليل الالكتروني لتفتيشه، فان حضور الشهود أيضا ضروري أثناء عملية التفتيش على أن يتم تدوين جميع ما تم ضبطه في محضر التفتيش ويوقع عليه الحاضرون[1] .

ثانيا: الضوابط الموضوعية.

وتتمثل هذه الضوابط في :

أ- توافر الخبرة الفنية لدى القائم بالتفتيش : لتفتيش الوسط الافتراضي، فإنه يقتضي أن يكون القائم به مؤهلا من الناحية الفنية ليتمكن من مباشرته، فالتفتيش في الجرائم التقليدية يختلف عن التفتيش في الجرائم الالكترونية من الناحية الفنية والأسلوب المتبع في التفتيش، مما يؤدي إلى بروز الإستعانة بالخبير المعلوماتي[2] من قبل المحقق لإجراء التفتيش، فالحصول على الدليل في الجرائم الالكترونية هو أمر فني معقد، لذلك يتطلب تفتيش الحاسوب أو أي وسيلة الكترونية أخرى للحصول على هذه الأدلة أشخاص ذوي خبرة فنية عالية ودراية كاملة بهذه التقنيات لأن أي خطأ قد يؤدي إلى ضياع الدليل أو تلف المعلومات الجاري البحث عنها لأن المعلومات التي يتم تفتيش الحاسوب لغرض الحصول عليها قد تكون مخزنة في مكان آخر يبعد عن مكان تواجد الحاسوب بآلاف الكيلومترات إذ يمكن إرسال البيانات المخزنة عبر الشبكة إلى نهاية أخرى وقد يكون جهاز الحاسوب أو الملفات مشفرة فمن الممكن أن يكون مرتكب الجريمة الالكترونية أكثر دهاءا مما تتصوره سلطات البحث والتحقيق، فيقوم المجني بمسح البيانات أو إتلاف الأقراص الالكترونية لطمس الدليل المتولد من جريمته .

ب – سبب التفتيش : الإذن بالتفتيش لا يصح إصداره إلا لضبط ماديات الجريمة الواقعة بالفعل وإتهام شخص أو عدة أشخاص بإرتكابها لذلك يجب توافر مجموعة من الشروط التي تتمثل في:

1- أن يكون التفتيش في الجريمة المعلوماتية الواقعة بالفعل سواء كانت جنحة أو جناية فمن غير الممكن القيام بالتفتيش دون وقوع الجريمة، غير أن المشرع خرج عن هذا المبدأ وجعل من التفتيش مهمة وقائية، الهدف منها هو الحيلولة دون وقوع الجريمة المعلوماتية من خلال القيام بعمليات المراقبة المسبقة للإتصالات طبقا للمادة 03 من قانون 09-04[3] .

2- لابد من إتهام شخص أو أشخاص معينين بإرتكاب هذه الجريمة الإلكترونية أو المشاركة في إرتكابها .

---

[1] سامي جلال الفقي حسين، التفتيش في الجرائم المعلوماتية "دراسة تحليلية"، دار الكتب القانونية ،القاهرة،2011 ص 49

[2] الخبير المعلوماتي:"هو الشخص الذي يتولى تفتيش الحاسوب والوسائل الالكترونية الأخرى بحثا عن أدلة الالكترونية لجريمة وقعت.بناءا على إذن بالتفتيش صادر من الجهة القضائية المختصة ويجب أن يكون قد تعمق في دراسة عمل من الأعمال الالكترونية أو تخصص في أدائه فترة زمنية طويلة مما اكسبه خبرة علمية بحيث أصبح ملما بتفصيلاته و هو على أصناف كالمبرمج و المحلل و مهندس صيانة و اتصالات

[3] ربيحة زيدان،الجريمة المعلوماتية في التشريع الجزائري و الدولي،دار الهدى،الجزائر،بدون طبعة، 2011 ص 93

3- لابد من توافر دلالات وإمارات قوية على وجود أجهزة، أدلة معلوماتية تفيد في كشف الحقيقة لدى المتهم[1].

ج- محل التفتيش: يقصد بمحل التفتيش مستودع سر الإنسان وهذا المستودع ينصب على محل له حرمة خاصة كالمسكن، أو على الشخص ذاته أو رسائله بالنسبة للجرائم التقليدية، وأما محل التفتيش في الجرائم الالكترونية، فهو الحاسوب بمكوناته المادية والمعنوية وشبكاته، إضافة إلى الوسائل الالكترونية الأخرى، وذلك يستلزم مراعاة أن يتم الإشارة إلى محل التفتيش في الإذن المقرر له، فلقد أشارت التشريعات المقارنة على إختلافها، إلى أن يحدد المكان والأشخاص المراد تفتيشهم بدقة، إذ لا محل للتفتيش بالنسبة للجرائم التي تقع على الوسائل الالكترونية أو التي تقع بواسطتها إلا إذا كانت هناك جريمة الكترونية (أي جريمة يكون محلها هو المعلومات) قد وقعت بالفعل وأن تكون هذه الجريمة من نوع الجناية أو الجنحة، فلا يحق لسلطة التفتيش أن تفتش الهاتف النقال العائد للشخص أو الكمبيوتر الخاص به طالما أن الدلائل لو تدل على وجود معلومات تتعلق بالجريمة في هذه الوسائل وألا يترتب على هذا التفتيش البطلان[2].

الفرع الثالث: الضبط في الجرائم الرقمية.

إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه فالضبط إذن هو غاية التفتيش القريبة، والأثر المباشر الذي يسفر عليه الإجراء والأساس القانوني للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق والتي تفيد في كشف الحقيقة ضد المشتبه فيه أو ما كان في مصلحته.

أولا: حجز المعطيات المعلوماتية.

إن الأشياء المضبوطة في الجرائم المعلوماتية تكون ذات طبيعة معنوية فقد يرد ضبط الأشياء على عناصر معلوماتية منفصلة مثل الأسطوانات الممغنطة، وهنا لا يثور أي إشكال عند القيام بالضبط لكن الصعوبة تكون عندما يلزم ضبط النظام كله أو الشبكة كلها لأنها تحتوي على عناصر لا يمكن فصلها، أما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية: وحدات الإدخال (لوحة المفاتيح، الفأرة، نظام القلم الضوئي) وضبط وحدة الإخراج (الشاشة، الطابعة، الرسم، المصغرات الفيلمية) وكل ما يتم ضبطه من بيانات الكترونية يتعين تحريرها وتأمينها فنيا[3].

فلقد حرص المشرع الجزائري على جعل المعلومات محل البحث في مأمن بإستخدام التقنيات اللازمة لمنع الوصول إليها وذلك في حالة إستحالة حجزها لأسباب تقنية كما لو كانت المعطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها وهنا نستخلص أن هناك نوعين من إجراءات الضبط:

---

[1] يومايلة ابتسام، مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية، مذكرة ماستر، قسم الحقوق، كلية الحقوق و العلوم السياسية جامعة قاصدي مرباح ، ورقلة، 2020-2021، ص 53.

[2] رفاه خضير جياد العارضي،الدليل الالكتروني و أثره في مجال نظرية الإثبات الجنائي، مرجع سابق، ص114

[3] بوعناد فاطمة الزهراء، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، سيدي بلعباس،2013 العدد 01، ص 30.

أ- إجراءات مبدئية تحفظية: الهدف منها هو الحفاظ على البيانات المخزنة التي تكون لها أهميتها في التحقيق ببقائها في أمكنتها في النظام المعلوماتي للكمبيوتر أو في دعامة التخزين ومنع الوصول إليها أو إلغائها أو التصرف فيها وذلك للكشف عن مرتكب الجريمة وسهولة إثباتها.

ب- إجراءات لاحقة للضبط: وهي إجراءات لاحقة للتفتيش والدخول وهي جميع البيانات سواء بأحد دعامة تخزين المعلومات أو أخذ نسخة من البيانات المخزنة بها أو بالنظام المعلوماتي للكمبيوتر في ورق وأقراص .

ثانيا: ضوابط الحجز في جرائم الرقمنة .

وتتمثل في المشروعية واليقين، توثيق الإجراءات، حماية حقوق الأفراد :

1- المشروعية واليقين: يجب أن يتم الحصول على الأدلة الرقمية بطريقة مشروعة وأن تكون هذه الأدلة يقينية وغير قابلة للشك، وعدم احترام هذه الشروط يؤدي إلى بطلان الأدلة وعدم جواز الاعتماد عليها في الإثبات الجنائي .

2-توثيق الإجراءات: يجب توثيق جميع الخطوات المتخذة خلال عملية حجز الأدلة الرقمية بدقة بما في ذلك تسجيل تفاصيل التفتيش والأجهزة والبيانات التي تم حجزها والأشخاص المسؤولين عن العملية.

3-حماية حقوق الأفراد: يجب أن تراعي عمليات حجز الأدلة الرقمية حقوق الأفراد في الخصوصية وأن تتم وفقا للضوابط القانونية التي تحمي هذه الحقوق، مع ضمان عدم التحدي على المعلومات الشخصية دون مبرر قانوني.

تظهر هذه الضوابط التزام المشرع الجزائري بتوفير إطار قانوني يوازن بين ضرورة مكافحة الجرائم الرقمية وحماية الحقوق الأساسية للأفراد، مع ضمان سلامة ومصداقية الأدلة الرقمية المستخدمة في الإجراءات[1] .

المطلب الثاني: الإجراءات الشخصية الخاصة بالتحقيق الجنائي في الجرائم المعلوماتية.

تبرز أهمية الإجراءات الشخصية في التحقيق الجنائي وهي عبارة عن خطوات يتخذها المحقق الجنائي لجمع الأدلة وكلاحقة الجناة ضمن إطار قانوني يضمن العدالة ويحمي الحقوق الفردية، ومن هنا تأتي ضرورة دراسة الإجراءات الشخصية في التحقيق الجنائي المتعلق بالجرائم المعلوماتية، لفهم طبيعتها، والتحديات المرتبطة بها، ومدى توافقها مع القواعد القانونية المحلية والدولية، فإذا كانت الإجراءات المادية تتعلق بالشيء محل التحقيق، فإن الإجراءات الشخصية هي إجراءات تتعلق بالشخص في حد ذاته وتتمثل في الخبرة والشاهد المعلوماتي .

الفرع الأول: الخبرة التقنية في الجرائم الرقمية .

أدى التطور التقني الهائل في عالم تكنولوجيا الإعلام والاتصال إلى إحداث تغير كبير في المفاهيم المتعلقة بالدليل الجنائي مما أدى بدوره إلى تعاظم دور الإثبات العلمي للدليل وإعلان انضمام الخبرة التقنية إلى عالم الخبرة القضائية، وأصبحت الاستعانة بخبراء مختصين لفحص الأدلة التقنية

[1] بوعناد فاطمة الزهراء ،مكافحة الجريمة الالكترونية في التشريع الجزائري،المرجع السابق،ص 32

وتقويم عملية الإثبات الرقمي وتحليل الجريمة المعلوماتية أمرا ملحا لا يمكن الاستغناء عنه إذ لا يعقل أن يفصل القاضي في قضايا تقنية المعلومات دون أن يستند إلى الخبرة التقنية في هذا المجال تحقيقا لمبدأ معروف هو مبدأ التخصص وإلا كان حكمه معيبا و مطعونا فيه.

أولا: دور الخبرة التقنية.

تعتبر الخبرة الفنية بأنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء من اجل الكشف عن الدليل أو قرينه تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم[1]، فهي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها بمعرفة فنية ودراية علمية لا تتوفر لديه.

وللخبرة الفنية دور كبير في إثبات الجريمة المعلوماتية، لأنها تثير الدرب لسلطات التحقيق والقضاء وسائر الجهات المختصة بالدعوى الجزائية للوصول إلى الحقيقة وتحقيق العدالة الجنائية[2]، ولذلك ومنذ تفشي الجرائم الالكترونية، تستعين سلطات التحقيق والاستدلال والمحاكمة بأصحاب الخبرة الفنية المتميزة في مجال التقنية الالكترونية من أجل كشف غموض الجريمة المعلوماتية وتجميع أدلتها والتحفظ عنها أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الالكترونية الدقيقة ذات صلة بالجريمة محل التحقيق وقد تزايدت الحاجة إلى الخبرة الفنية للتحقيق في الجرائم المعلوماتية في الآونة الأخيرة نظرا للتحولات التكنولوجية التي مست وسائل الإعلام والاتصال، إذ تعددت أنواع ونماذج الحواسيب وشبكات الاتصال بينها، وأصبحت العلوم والتقنيات المتعلقة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتشبعة، والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب على المتخصص تتبعها واستيعابها بل يمكن القول انه لا يوجد حتى الآن خبير يملك معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكاتها أو قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها، لذلك ترك المشرع الجزائري للمحقق حرية الكاملة وفي أية مرحلة من مراحل التحقيق واختيار أي خبير يرى فيه الكفاءة الفنية اللازمة للاستعانة بخبرته، كما أنه لا يوجد في القانون ما يلزمه للاستجابة للمتهم والخصوم إذا طلبوا خبير، ومع هذا فإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمرا واجبا على جهة التحقيق أو الحكم فيه أوجب في مجال استخلاص الدليل الرقمي لإثبات الجرائم المعلوماتية، لتعلقها بمسائل فنية آية في التعقيد لا يكشف غموضها إلا بمتخصص بارع في مجال تخصصه ذلك لأن الذكاء والفن لا يكشفه ولا يفهمه إلا ذكاء وفن مماثلين[3] .

وتبرز أهمية الاستعانة بخبير لإثبات الجرائم المعلوماتية بشكل أكبر عند غيابه، فقد تعجز سلطات التحقيق والاستدلال عن إسقاط اللثام عن الجريمة وجمع الدليل بخصوصها لنقص الكفاءة

---

[1] عادل عزام سقف الحيط، جرائم الدم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، ط1، 2011، ص 120.

[2] بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، ص 424

[3] فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ، رسالة لنيل دكتوراه في القانون، كلية الحقوق،مسيلة،2013 ص640

والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل أو محوه بسبب الجهل أو الإهمال عند التعامل معه.

ثانيا: أساليب عمل الخبير ودوره في حفظ الدليل في الجريمة المعلوماتية.

الخبير هو كل شخص له دراية بمسالة من المسائل التحقيق وقد يستدعي هذا التحقيق إلى فحص مسألة تستلزم كفاءة خاصة فنية أو علمية لا يشهر المحقق بتوافرها في نفسه فيمكنه أن يستشير فيها خبيرا، ومن المعلوم أن هناك حاجة دائمة إلى الخبراء وفنيين عند وقوع الجريمة الالكترونية ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه، وإن نجاح أعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء، وكذا يجب على المحقق الجنائي أن يحدد الخبير المعلوماتي دوره في المسالة وهناك أسلوبان لعمل الخبير:

1- القيام بتجميع وتحصيل مجموعة المواقع: التي تشكل جريمة في حد ذاتها كجريمة التهديد أو النصب وجرائم النسخ ثم يقوم الخبير بعملية تحليل رقمي لها، وذلك لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها وكيف تم التوصل إلى معرفتها.

2- التحفظ على الأجهزة والبيانات: يتم التحفظ على الأجهزة الالكترونية المشتبه بها وضمان عدم العبث بها لحين استخراج البيانات منها بطريقة قانونية.

3- استخدام أدوات متخصصة: يقوم باستخدام برامج وتقنيات متقدمة لنسخ البيانات بطريقة تحفظ سلامتها مثل إنشاء نسخة طبق الأصل دون التأثير على البيانات الأصلية .

4-تحليل الأدلة الرقمية: تحليل رسائل البريد الالكتروني، السجلات، المواقع التي تم زيارتها، النشاط على وسائل التواصل، أو محاولات الاختراق.

ثالثا: دور الخبير في حفظ الدليل الرقمي.

1- ضمان سلامة الدليل: لأن الدليل الرقمي يمكن تغييره أو محوه بسهولة، يقوم الخبير بإجراءات لحمايته مثل استخدام أدوات تحقق لضمان عدم تغييره .

2- منع فقدان البيانات: يقوم الخبير بنسخ البيانات فورا واستخراجها بطرق متقدمة، مما يمنع ضياعها أو تدميرها .

3- إثبات العلاقة بين الجريمة و الفاعل: عبر تحليل البيانات الرقمية وربطها بالمستخدم من خلال عناوين IP ، توقيت الاستخدام وتاريخ الملفات.

4- تقديم شرح فني للمحققين والقضاة: يوضح لهم محتوى الدليل وطريقة فهمه ضمن الإطار القانوني.

الفرع الثاني: الشهادة .

الشهادة بصفة عامة هي إثبات حقيقة واقعة معينة علم بها الشاهد من خلال ما شاهده أو سمعه أو أدركه بحواسه الأخرى عن تلك الواقعة بطريقة مباشرة، فالشهادة على هذا الأساس تعد وسيلة إثبات أساسية في المسائل الجزائية[1]، ويطلق عليه إسم الشاهد المعلوماتي لأنه هو الشخص الفني

[1] إبراهيم الغمار، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه ،كلية الحقوق، جامعة القاهرة، مصر،1989، ص30.

صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي والذي يكون لديه معلومات جوهرية لازمة للدخول لنظام المعالجة الآلية للبيانات فلذلك نجد أن الشاهد ينحصر في عدة طوائف تتمثل في تشغيل الحاسب الآلي خبراء البرامج والمحللون ومهندسو الصيانة والاتصالات ومديرو النظام .

وللشاهد التزامات لابد التقيد بها مثل طبع الملفات والبيانات المخزنة في ذاكرة الحاسوب الآلي على أن يقوم بطبعها وتسليمها إلى سلطات التحقيق للإفصاح عن كلمات المرور السرية وكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة[1].

المطلب الثالث: الإجراءات المستحدثة في التحقيق الجنائي في الجرائم المعلوماتية.

تبين من الإجراءات التقليدية أنها صعبة الإتباع للحصول على الدليل الرقمي، فكان من الضروري على التشريعات المختلفة خلق أدلة أو إجراءات حديثة تتماشى مع طبيعة الخاصة للدليل وهذا عن طريق الاعتماد على تكنولوجيا المعلومات، والمشرع الجزائري كغيره قام بإرسال جملة من المقومات التشريعية لمكافحة الجريمة المعلوماتية من خلال ما جاء به في القانون، والأمر 66-155 المتعلق بإجراء التسرب واعتراض المراسلات السلكية واللاسلكية وكذلك بموجب إصدار قانون إجراء خاص به، المتضمن للقواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، واستخدام إجراء المراقبة التكنولوجية وسنتطرق إلى دراسة هذه الإجراءات المستحدثة في مجال المعلوماتية في فروع الآتية :

الفرع الأول: التسرب.

هو الإجراء المستحدث الذي نصت عليه المواد من 65 مكرر إلى 65 مكرر 20 من قانون الإجراءات الجزائية التي أضيفت بموجب القانون 15-02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الجديد المعدل هذه المواد تنظم التحريات الخاصة في الجرائم المعلوماتية، ومن ضمنها ما يخص "تسرب البيانات" إذ اعتبر ذلك فعلا إجراميا متعلقا بإختراق أو إستخدام غير مشروع للمعطيات، وتكون عملية التسرب في الجريمة المعلوماتية بدخول ضابط أو عون شرطة إلى العالم الإفتراضي وذلك عن طريق إشتراكه في محادثات لمعرفة الدردشة، أو إختراق مواقع معينة مستخدما في ذلك أسماء أو صفات وهيئات مستعارة وهمية، سعيا منه لاستفادة المشتبه فيهم عن طريق منهم في كيفية إقتحام الهاكر الموقع، أو القيام بحلقات إتصال بالبريد الالكتروني، ووكيل الجمهورية هو من يقوم بمراقبة أو قاضي التحقيق وفقا للمادة 65 مكرر 06 من قانون الإجراءات الجزائية الجزائري[2] ويمكن لهما الأمر أن يوقف التسرب في أي مرحلة وذلك من أجل تأمين متسلسل من الشبكة الإجرامية.

---

[1] بن زرت أسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، 2019، ص 26

[2] نصت المادة 65 مكرر05:"تجيز لوكيل الجمهورية أو قاضي التحقيق إجراء تحريات خاصة باستخدام الوسائل التقنية في الجرائم المتعلقة بأنظمة المعلومات و تشمل جمع البيانات و تحليلها"

- المادة 65 مكرر7:"تسمح بمراقبة الاتصالات الالكترونية، بما في ذلك البريد الالكتروني في إطار جرائم المعلوماتية"

- المادة65مكرر11:"تحدد كيف يمكن للضبطية القضائية نسخ أو حجز البيانات الرقمية بما في ذلك البيانات المسربة أو المقرصنة"

الفرع الثاني: المراقبة.

تناول المشرع الجزائري هذا الإجراء من المادة 04 من قانون رقم 09-04 المتعلق بالقواعد الخاصة بالرقابة من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها بعنوان مراقبة الإتصالات الالكترونية.

والمشرع لم يعرف بإجراء المراقبة بل ترك أمر تعريفها للفقه عرفها بأنها: "عمل أساسي له نظام معلومات إلكتروني، ويقوم فيه المراقِب بمراقبة المُرَاقَب بواسطة الأجهزة الإلكترونية أو عبر شبكة الإنترنت لتحقيق وتحديد التقارير بالنتيجة[1].

نجد أن المشرع لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الرقمي فقط بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة المعلوماتية[2].

الفرع الثالث: إعتراض المراسلات السلكية واللاسلكية.

قد عرف المشرع الجزائري الاعتراض بالتفصيل في المادة 65 مكرر05 من قانون الإجراءات الجزائية إذ اعتبر عملية مراقبة المراسلات بأنها "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض "نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور) أو الدعامة التي تنصب عليها (الورقية، الرقمية) أو الوسيلة المستعملة لإرسالها سلكية كانت (كالفاكس، تيلغرام) أو اللاسلكية (البريد الالكتروني، الهاتف النقال) باستثناء الكتب والمجلات والرسائل التي تعد مراسلات خاصة، وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين وذلك لغرض التنصت والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل لمواجهة المتهم[3].

و لعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة والتي تمثل مصدرا غنيا لأدلة إثبات الجرائم المعلوماتية، كون هذه التقنية من أكثر الوسائل الحديثة إستخداما للاتصال عبر الانترنت ومجالا خصبا للربط بين الأشخاص بسرعة فائقة.

وتجدر الإشارة إلى أن المشرع الجزائري لم يتبنى في القانون رقم 09-04 مراقبة الاتصالات الالكترونية كإجراء تقتضيه التحريات والتحقيقات القضائية فقط مثلما هو في قواعد الإجراءات الجزائية، إنما أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني في إطار الوقاية من بعض الجرائم التي يحتمل أن تشكل خطرا على أمن الدولة، فالمشرع الجزائري سمح بإجراء التحقيق

---

[1] مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت، دار الكتب القانونية، مصر،2005 ، ص 192.

[2] اوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور جامعة الجلفة ، 2019 – 2020، ص 21-22

[3] ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 157

في عمليات المراقبة للاتصالات الالكترونية لأشخاص أو مجموعات بمجرد وجود احتمال تورطهم مستقبلا في ارتكاب إحدى هذه الجرائم .

المبحث الثاني: طرق الحصول على الدليل الرقمي والصعوبات التي يواجهها.

لمواجهة التحديات التي تواجه الدليل الرقمي كدليل إثبات فلابد من دراسة الجانب القانوني للجريمة والدليل الرقمي يعتبر من أولويات التشريع ولا ينبغي أن ينفصل القانون عن هذا التطور التكنولوجي والفني، فالدليل الرقمي حتى ينتج أثره في الدعوى الجنائية لابد من معرفة مصدره وضرورة سلامته من أي عيب وكذلك المحكمة حتى تطمئن على سلامة الإجراءات التي اتخذت في كيفية الحصول على الدليل الرقمي هنالك طرق وتقنيات تتبع في فحص الأدوات والآلات الالكترونية تحتاج إلى كفاءة ودقة عالية جدا لا يستطيع الشخص العادي معرفتها، كما أن الشخص التقني الذي يقوم باستخراج الدليل أو تجميعه يقع عليه عبء تحليل الرموز والبيانات المتحصل عليها من تلك المصادر ومنه سنتناول في هذا المبحث طرق والوسيلة التي يتم الحصول على الدليل الرقمي في المطلب الأول والصعوبات التي تواجه الدليل الرقمي عند استخراجه في المطلب الثاني.

المطلب الأول: الوسائل المستخدمة في الحصول على الدليل الرقمي.

عند القيام بالتحقيق في جريمة ما، فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية وسهولة الوصول إلى الجاني، ولأن الجرائم المعلوماتية طابعها الخاص المميز لها، فإن التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة، وبالتالي حل لغزها والوصول إلى الجاني .

فعملية الحصول على الأدلة الجنائية الرقمية أمر صعب الوصول إليه وذلك لما تتطلبه من خبرة ومهارة كبيرة في مجال التكنولوجيا الرقمية، إضافة إلى ذلك تعدد صور وأشكال الجريمة المعلوماتية، وعليه للحصول على هذا النوع يعتمد المحقق على مجموعة من الوسائل المختلفة[1].

الفرع الأول: الوسائل المادية الحديثة في جمع الأدلة الجنائية الرقمية.

الوسائل المادية أدوات فنية تستخدم في بنية نظم المعلومات والتي يمكن استخدامها لتنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها[2]، ومنه فالوسائل المادية هي أدوات أو برامج ذات طبيعة تقنية يتم استخدامها في التحقيق بغرض إثبات وقوع الجريمة وتحديد مرتكبها أو بالأحرى وسائل فنية الهدف منها جمع مختلف الأدلة الجنائية الرقمية التي يمكن من خلالها الكشف عن ملابسات الجريمة المعلوماتية ومنه عندما يستعمل المستخدم شبكة الانترنت فإنه يترك آثار وراءه عن كل موقع يزوره، إذ يفتح هذا الأخير سجلا خاصا يحتوي على معلومات كثيرة من بينها نوع الحاسب الآلي والمتصفح وغيرها وكل هذه البيانات تعتبر من قبيل المعلومات الجد الهامة في التحقيق وانطلاقا لما تقدم سنلقي نظرة سريعة على أجهزة

---

[1] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، عدد4 ، جانفي 2018، جامعة تبسة ، ص 54

[2] ممدوح عبد الحميد، جرائم الكمبيوتر عبر الانترنت، كلية الحقوق، جامعة الشارقة، إمارات، 2000، ص 29 .

الكمبيوتر للمشتبه فيه ثم المجني عليه والبرامج المستخدمة والبروتوكولات التي تتبع وغيرها من الوسائل[1].

أولا: البرامج المستخدمة والأنظمة.

1- البروكسي: حيث يعمل كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة.

2- برامج التتبع: حيث تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على إسم الحدث وتاريخ حدوثه وعنوان (IP) الذي تمت من خلاله عملية الاختراق وإسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق، وأرقام مداخلها أو مخارجها على شبكة الانترنت ومعلومات أخرى ومن الأمثلة على هذه البرامج برنامج (hack tracer vl 2)[2] .

3- نظام كشف الاختراق: ويرمز له اختصارا بالأحرف (IDS) وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الالكترونية أو الشبكة مع تحليلها بحثا عن أي إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسبة الالكترونية أو الشبكة ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الالكترونية أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة[3] .

4- برنامج الدمج وفك الدمج: يستعين الخبير الالكتروني بهذا البرنامج عادة لفك البرامج التي قام المجرم المعلوماتي بدمجها قصد التعرف على طبيعة البيانات التي يحتويها وتحليلها، ودمج البرامج هي تقنية عالية يستعملها المجرم لإخفاء المعلومات حيث لا يمكن الاطلاع عليها إلا بعد فك الدمج.

5-الذكاء الإصطناعي: هي تقنيات وبرامج الحاسب الآلي التي يستعين بها الخبير الالكتروني لحصر الأسباب والفرضيات المتعلقة بالجريمة وجمع الأدلة الجنائية وتحليلها واستخلاص الحقائق منها، عن طريق عمليات حسابية يتم حلها بواسطة برامج الحاسب الآلي صممت خصيصا لهذا الغرض كبرنامج (xtree progold) الذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة أو الأقراص الصلبة أو الأقراص المرنة المضغوطة، وقراءة محتوياتها في صورتها الأصلية[4].

---

[1] سليمان العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2003 ، ص98

[2] المرجع نفسه، ص 99

[3] عز الدين عثماني، إجراءات التحقيق والتفتيش، المرجع السابق ص 54

[4] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب و الانترنت، مرجع سابق ،ص 51

ثانيا :أجهزة الكمبيوتر ومقدم خدمة الانترنت.

1- جهاز كمبيوتر المشتبه فيه: يتم ذلك بمناظرة جهاز الكمبيوتر الخاص بالمشتبه فيه وفحصه بطريقة فنية والاطلاع على وحدة الذاكرة (هارد ديسك) وبيان البرامج الوسيطة التي يستعملها ويستخدمها وإمكانية استخدام هذه البرامج في الجريمة المرتكبة .

2- جهاز كمبيوتر المجني عليه: مما لاشك فيه أن المجني عليه هو المصدر الكاشف والنتيجة التي يترتب عليها ما قام به المشتبه فيه من جرائم، والمجني عليه قد يكون شخص طبيعي أو مؤسسة خاصة أو عامة أو مؤسسة مالية أو هيئة حكومية وغيرها وبالتالي فإن فحص مثل تلك الأجهزة تمكن المحقق من معرفة الدخول وتتبع مصدر المشتبه فيه[1].

3- مقدم خدمة الانترنت: تم التطرق إلى مقدمي خدمات الانترنت ضمن مجموعة من القوانين والتنظيمات التي تعنى بتنظيم قطاع الاتصالات وتكنولوجيا المعلومات، ونظرا للدور المهم الذي يقوم به مزود خدمات الانترنت كان من الضروري إيجاد تنظيم تشريعي متكامل يحدد مركزه القانوني ويبين في نفس الوقت مسؤوليته عما يرتكب من مخالفات عبر الشبكة العالمية للانترنت

الفرع الثاني: الوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية.

هي الوسائل التي يتم استخدامها في التحقيق لإثبات الجريمة المعلوماتية والتي تحدد شخصية مرتكبها وذلك باستخدام تقنيات وبرامج الكترونية مختلفة، تماشيا مع إرادة المشرع في مكافحة الجرائم المعلوماتية، فالمشرع الجزائري تطرق إلى هذه الوسائل الحديثة في جمع الأدلة الجنائية الرقمية في النقاط التالية :

أ- إقتفاء الأثر يمكن تقصيه بطرق عدة سواء عن طريق بريد الكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

ب- الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

ج- الاستعانة بالذكاء الاصطناعي من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الالكترونية وفق برامج صممت خصيصا لهذا الغرض.

د- مراقبة الاتصالات الالكترونية لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الاتصالات، على عكس بعض التشريعات التي عرفتها[2].

ومن أهم المواد التي نظمها المشرع الجزائري في القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتعلق بالوسائل الإجرائية الحديثة [3].

---

[1] سليمان العنزي، وسائل التحقيق في جرائم نظم المعلومات، المرجع السابق ، ص 98

[2] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال ومعلوماتية، مرجع سابق، ص55

[3] نصت المادة 65 مكرر5 على التفتيش الالكتروني الرقمي:"تجيز لوكيل الجمهورية أو قاضي التحقيق تفتيش أنظمة المعلومات أو الوسائط الالكترونية عند وجود مؤشرات على استخدامها في ارتكاب الجريمة ، يسمح للمحققين بالدخول إلى أجهزة الرقمية و البحث عن أدلة رقمية مع احترام ضمانات قانونية".

المطلب الثاني :صعوبات استخلاص الدليل الرقمي.

بالرغم من الجهود المبذولة في مكافحة الجريمة المعلوماتية، إضافة إلى الدور البارز الذي يلعبه الدليل الرقمي في الإثبات، إلا أن الواقع العملي والقانوني كشف عن الكثير من الصعوبات التي تثيرها عملية الإثبات بتلك الأدلة الرقمية، فمن الصعوبات التي قد تواجه عملية استخلاص الدليل في الجريمة الماسة بأنظمة الاتصال والمعلوماتية هو مسالة نقص الخبرة لدى رجل الضبط القضائي أو أجهزة الأمن بصفة عامة وكذلك لدى أجهزة العدالة الجنائية متمثلة في سلطات الاتهام والتحقيق الجنائي وذلك فيما يتعلق بثقافة الحاسب الآلي وأنظمة الاتصال والإلمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها وذلك على الأقل في بلدان العربية بشكل عام، نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وإنتشارها في هذه البلدان جاءت متأخرة كما أن أجهزة العدالة المقاومة للجرائم المرابطة بهذه التقنية تبدأ في التشكل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتا إبطاء من وقت انتشار الجريمة، لأن الجريمة الماسة بأنظمة الاتصال المعلوماتية تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها[1] .

الفرع الأول: صعوبات تتعلق بالدليل الرقمي.

في ظل التطور المتسارع وإعتماد المجتمعات بشكل متزايد على الوسائط الرقمية أصبح الدليل الرقمي أحد الأدلة الأساسية في التحقيقات القضائية والجنائية، ورغم أهميته المتناهية إلا أن التعامل مع هذا النوع من الأدلة يواجه العديد من الصعوبات والتحديات، فالدليل الرقمي يتسم بطبيعة خاصة تجعله مختلفا عن الأدلة التقليدية، حيث يعتمد على البيانات الالكترونية التي قد تكون عرضة للتلف أو التلاعب بسهولة، فضلا عن تعقيد طرق جمعها وتحليلها وتقديمها أمام الجهات القضائية، كما تبرز إشكاليات قانونية وتقنية تتعلق بكيفية ضمان موثوقية وسلامة هذا الدليل، ومدى قابليته للإعتماد عليه في الإثبات ضمن الأطر القانونية المعتمدة، ومن هنا تبرز الحاجة إلى فهم شامل للصعوبات التي تحيط بالدليل الرقمي.

أولا: صعوبة رؤية الدليل الرقمي.

تتميز الجريمة المعلوماتية بأنها تتم في العالم الافتراضي والذي بدوره تكون فيه الأدلة عبارة عن نبضات أو مجالات مغناطيسية أو كهربائية في شكل بيانات أو معلومات رقمية، وهذا ما يثير إشكال جمع وتحليل الدليل الرقمي لعدم إمكانية رؤيته، مما يجب أن تتوفر لدى المحققين المهارة الكبيرة والدراية الكافية في التعامل مع هذا النوع من الأدلة [2].

ثانيا: سهولة محو و تدمير الدليل الرقمي.

نظرا للسهولة التي تتميز بها هذه العملية وعدم استغراقها للوقت الطويل فإنها تعد من بين أكبر التحديات والصعوبات التي تواجه عملية استخلاص الدليل الرقمي، لأن مرتكبي الجرائم المعلوماتية

---

[1] خيرة علي محرز، التحقيق في جرائم الحاسب الآلي ، دار الكتاب الحديث ،2012 ،ص 81

[2] عبد الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، ط1، دار الفكر الجامعي،مصر،2006،ص78

يتميزون بالذكاء الخارق والإتقان الفني للعمل الذي يقومون به وعليه فإنهم يسعون لمحو وتدمير وتعديل أي دليل يمكن إدانتهم، من خلال التلاعب الغير المرئي في أنظمة الحاسب الآلي ومحتوياته[1].

ثالثا: إعاقة الوصول إلى الدليل الرقمي.

تجدر الإشارة إلى أنه من الصعب ملاحقة مرتكبي الجرائم المعلوماتية لأنهم يلجؤون إلى إخفاء هوياتهم الخاصة عند استخدام شبكة الانترنت من خلال استعمال العديد من البرامج والتطبيقات التي تعمل على طمس الهوية في شبكة الانترنت، ومن بين الوسائل المبتكرة التي يلجؤون إليها باستخدام تقنية التشفير لعرقلة جمع أدلة الإدانة أو اتخاذ تدابير أمنية وذلك باستخدام كلمة السر[2] .

رابعا :ضخامة البيانات المتعين فحصها.

من بين أكبر التحديات والصعوبات التي تواجه سلطات التحقيق ورجال الضبط استخلاص الدليل الرقمي، هو ذلك الكم الكبير والوفير للمعلومات والبيانات المراد فحصها وتحليلها لذلك يتعين على المحقق أن تتوافر لديه في مجال الحاسب الآلي وملحقاته، القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة في جهاز الحاسب الآلي أو في دعائم التخزين الرقمية ولتجاوز هذه الصعوبات وجب الاستعانة بخبراء فنيين في مجال الحاسب الآلي [3].

الفرع الثاني: صعوبات تتعلق بجهاز التحقيق.

وجب في استخلاص الأدلة الرقمية وفحصها توفر مهارات وخبرات خاصة في مجال الحاسب الآلي، زيادة إلى أساسيات وأصول التحقيق الجنائي الفني المطبقة في الجرائم التقليدية، ومنه فنقص خبرة المحققين وعدم متابعتهم للمستجدات في مجال الإعلام الآلي، وعدم معرفتهم للتقنيات والأساليب المستعملة في ارتكاب الجريمة المعلوماتية يعد عائقا كبيرا في جمع الأدلة الرقمية وتحليلها.

ولتفادي هذه الصعوبات قام المشرع الجزائري بإنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام تحت وصاية القيادة العامة للدرك الوطني بموجب مرسوم الرئاسي رقم 183-40 المؤرخ في 26-06-2004 [4]حيث نصت المادة 04 منه على العديد من المهام الموكلة إلى هذا المعهد أهمها إجراء الخبرات والفحوص العلمية بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، زيادة إلى ذلك المساعدة التقنية والفنية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية التي تقوم بتجميع وتحليل الأشياء والآثار وكل ما أخذ من مسرح الجريمة، ويحتوي هذا المعهد على قسم الإعلام الآلي الذي يقوم بالتحقيق عن طريق جمع الأدلة الرقمية وتحليلها [5].

كما استحدث المشرع الجزائري المعهد الوطني للبحث في علم التحقيق الجنائي تحت وصاية المديرية العامة للأمن الوطني حيث أوكلت لها مهام إعداد تقارير الخبرة، القيام بالتكوين وتجديد

---

[1] بن مالك احمد، الخال إبراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، جامعة تمنراست، مجلد 05، عدد 2021، ص113-114.

[2] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي، مرجع سابق، ص 121.

[3] ثنيان الناصر أل ثنيان، إثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، سعودية 2007 ص 131

[4] الجريدة الرسمية رقم 41، الصادرة بتاريخ 27-06-2004 ص 18.

[5] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، باتنة ، كلية الحقوق والعلوم السياسية, 2013 ص 189 .

المعارف في ميدان علم التحقيق الجنائي والإجرام، كما يحتوي هذا المعهد على مصلحة الخبرات الخاصة بالدلائل التكنولوجية.

الفرع الثالث : صعوبات تتعلق بالتشريع.

على المستوى الدولي فإنه من أبرز المعوقات التي تواجه الدول في تنظيم موضوع الجرائم المعلوماتية هو القصور التشريعي، مما جعل هذه الدول تعمل على إعادة وتحديث منظومتها القانونية عن طريق تعديل قوانينها الإجرائية، وعليه نجد أن الجزائر من بين هذه الدول، حيث قامت باستحداث آليات قانونية تيسر من عملية جمع الأدلة الرقمية، وذلك عن طريق ما جاء به القانون 09-04 المؤرخ في 05-08-2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أتى بإجراءات وأساليب تقنية تمثلت في مراقبة الاتصالات الالكترونية (المادة 4) وتفتيش المنظومة المعلوماتية (المادة 5) وكذلك حجز المعطيات المعلوماتية (المادتين 06-07) بالإضافة إلى قيام المشرع الجزائري بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وإعادة تنظيمها [1].

المبحث الثالث: حجية الدليل الرقمي في الإثبات أمام القضاء الجنائي .

مما لاشك فيه أن التطورات التكنولوجية الحديثة قد أحدثت تغيرات جذرية في وسائل الإثبات الجنائي الذي يعد من المواضيع الشائكة في المواد الجنائية التي تواجه القاضي على وجه الخصوص بسبب أن الإثبات ينصب ويتعلق بوقائع مادية ونفسية يتعذر إثباتها في المسائل الجنائية على عكس المسائل المدنية محل إثبات فيها وقائع قانونية يسهل إعداد دليلها سلفا كما تعد من أصعب الأمور التي يقوم بها القاضي وهي تقدير الأدلة التي تعتبر من أهم المسائل التي تساهم في إصدار الحكم الذي يريد القاضي الوصول إليه استنادا لهذه الأدلة والنصوص القانونية الخاصة بها، فالحجية هي وصف ثابت بحكم الشرع يلحق مضمون الحكم القضائي أو الأمر القضائي فيه ويكون غير قابل للمناقشة فيه [2].

يعتبر مبدأ حرية القاضي من أهم المبادئ التي يقوم عليها الإثبات في المواد الجزائية، ويعني هذا أن يتيح للقاضي قبول جميع الأدلة المقدمة إليه من أطراف الدعوى وتقديرها بكل حرية، وله بعد ذلك أن يستبعد أي دليل لا يطمئن إليه، فليس هناك دليل يفرض عليه، وسلطته التقديرية كاملة في تقدير قيمة كل دليل على حدة، وله في النهاية تنسيق بين الأدلة المقدمة إليه واستخلاص نتيجة منطقية من هذه الأدلة المجتمعة والمتساندة تتمثل في تقرير البراءة أو الإدانة ذلك ما يؤسس لما يعرف بمبدأ الاقتناع الشخصي ليعلن بذلك عن الحقيقة القضائية التي يفترض أن تتطابق مع الحقيقة الواقعية التي يهتم الدليل بنقلها أمام القضاء، إلا أن هذا الدليل قد أثار لدى الفقه تساءل إن كانت الصفة الرقمية الملحقة بالدليل من شأنها أن تكسر مبدأ وتغير النظرة النموذجية للإثبات الجزائي من هنا نرى بأن

---

[1] المرسوم الرئاسي رقم 21-439 المؤرخ في 07-11-2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد86، المؤرخة في 11-11-2021 ص 05.

[2] فراحتية خلود، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، كلية الحقوق والعلوم السياسية، جامعة برج بوعريريج 2021-2022 ص 38 .

الاقتناع الشخصي للقاضي الجزائي بقي صامدا في مواجهة استقبال الساحة القضائية للدليل الرقمي في نطاق الإثبات الجزائي للجريمة ولم ينتهك بأي شكل من الأشكال[1] .

المطلب الأول: سلطة القاضي الجنائي في تقدير الدليل الرقمي.

قبل أن يبدأ القاضي الجنائي في تقدير الدليل الجنائي بصفة عامة والدليل الرقمي بصفة خاصة لابد من قبوله أولا للتأكد من مدى صلاحيته وملائمته كدليل إثبات جنائي، ولقبول القاضي الجنائي لهذا الدليل في الإثبات لابد أن يستند على أساس[2]، فمرحلة قبول الدليل تعد أول خطوة يتخذها القاضي وذلك قبل البدء في تقديره وهنا لتأكيد صلاحيته وملائمته لتحقيق ما قدم لأجله فهذه المرحلة هي النشاط الإجرائي الذي يمارسه القاضي على أدلة الإثبات المقدمة من سلطة الاتهام وهذا للتيقن من صحتها وتوافر كافة الشروط فيها، وهو ما يعبر عنه ضمنيا من طرف القضاء فيما يتم ممارسته على الدليل من عمليات تبدأ بالفحص وتنتهي بالتقدير واستنباط ما يحويه من قيمة إثباتية فهذه العملية ليست بالسهلة فهي تخضع لعدة شروط ومعايير يضاف إلى ذلك أن الدليل الذي سيمارس عليه القاضي سلطته ليس دليلا ماديا وإنما دليلا رقميا ينتمي إلى صنف الأدلة العلمية مما يثير صعوبات ترد على سلطة القاضي الجنائي في قبول هذا النوع من الأدلة وعليه نظرا للطبيعة الخاصة التي يتميز بها الدليل الرقمي وما يصاحب الحصول عليه من خطوات معقدة فإن قبوله يثير العديد من المشكلات فالتلاعب في الدليل وتغيير حقيقته أمر وارد[3] ومنه سنتناول من خلال الفرعين شروط قبول الدليل الرقمي كدليل إثبات في المواد الجنائية والفرع الثاني أساس قبول الدليل الرقمي.

الفرع الأول: شروط قبول الدليل الرقمي كدليل إثبات في المواد الجنائية.

يتمتع القاضي الجنائي بسلطة واسعة في تقديره لأدلة الإثبات حتى وإن كان الدليل الرقمي بإمكانه أن يتحرى عن الحقيقة عن طريق جمع الأدلة دون إلزامه بتفضيل مسبق لدليل معين حتى وإن تم تحديد مسبق لنوع الأدلة الرقمية، فإنها تعد بمثابة صمام أمان إتجاه انحراف القاضي عند ممارسته لها وتضفي عليها المصداقية واقترابها من الحقيقة، فقبول القاضي الجنائي للدليل الرقمي وحجيته يتوجب توافر شروط معينة، أولها ضرورة أن يتم الحصول على الدليل الرقمي مشروع ومقبول، وثانيا ضرورة مناقشة هذا الدليل الرقمي وثالثا ضرورة بلوغ الاقتناع القضائي لدرجة اليقين[4] .

أولا: شرط مشروعية الدليل الرقمي.

إن القاضي الجنائي يتمتع بسلطة تقدير الدليل الرقمي المقبول في الدعوى، حيث يشترط لقبوله في الدعوى أن يتم الحصول عليه بطرق مشروعة وفقا للأمانة والنزاهة، ذلك أنه يستلزم على القاضي الجنائي تطبيق الدليل تطبيقا سليما وأن يستمد اقتناعه من دليل رقمي مقبول لأن محل الحرية

---

[1] قادري سوسن،عبار عمر،الدليل الرقمي بين اقتناع القاضي الجزائي ورقابة المحكمة العليا، مجلة القانون العام الجزائري والمقارن مجلد 10، العدد1، جويلية 2024 ص 232-233

[2] عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت،رسالة دكتورا،كلية الحقوق،جامعة عين الشمس،2004،ص823

[3] بن فردية محمد،الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية مرجع سابق، ص211

[4] عائشة بن قارة مصطفى،حجية الدليل الالكتروني في الإثبات الجنائي في القانون الجزائري ، مرجع سابق،ص267- 268

التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة[1] وعليه فمشروعية الدليل الرقمي تعد ضمانا كبيرا للحرية الفردية، إذ يترتب على استخدام وسائل غير مشروعة للحصول على الأدلة الرقمية بطلان الإجراءات وعدم صلاحيتها لأن تكون أدلة إدانة في المواد الجنائية ومن أمثلة الطرق غير مشروعة، استخدام الإكراه المادي أو المعنوي أو الغش ضد الجاني في الجرائم المعلوماتية من أجل فك الشيفرة الخاصة بالدخول إلى النظام والوصول إلى الأدلة المتحصلة من الوسائل الالكترونية[2] .

ثانيا : شرط مناقشة الدليل الرقمي .

من أهم القواعد في الإجراءات الجنائية أنه يجب على القاضي أن يبني حكمه على أدلة طرحت أمامه لمناقشة الدليل في جلسة، ويترتب على ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تمنح للخصوم فرصة الاطلاع عليه ومناقشته، ولا يختلف ذلك بالنسبة للدليل الرقمي أيا كان شكله سواء كانت بيانات معروضة على شاشة الحاسب الآلي أو معلومات مخزنة على أقراص أو أشرطة ممغنطة أو مستخرجة في شكل مطبوعات، فجميعها تكون محلا للمناقشة في حالة الأخذ بها كأدلة إثبات أمام المحكمة وتقوم مناقشة الدليل الرقمي على عنصران، الأول يتمثل في إتاحة الفرصة للخصوم للاطلاع على الدليل الرقمي والرد عليه وذلك من أجل التزام حقوق الدفاع وأن يتمكن الخصوم من مواجهة هذه الأدلة والرد عليها، ويتيح مبدأ المواجهة وتجسيد ضمانات منها لزوم إحاطة المتهم علما بالتهمة المنسوبة إليه ومنحه الوقت الكافي لتحضير دفاعه والسماح له بالاستعانة بمحامي ومن ناحية أخرى أثناء عملية المواجهة يسمح لكل طرف من الخصوم تقديم ما لديه من مستندات وسؤال الشهود والخبراء، حيث يمكن إتخاذ أي إجراء يرى القاضي الجنائي أنه مناسب لإظهار الحقيقة أما العنصر الثاني يتمثل في أن يكون الدليل الرقمي أصل في أوراق الدعوى، وذلك حتى يكون إقتناع القاضي مبني على أساس، بالتالي ألزم المشرع تحرير محضر الجلسة لإثبات وقائع الدعوى الجنائية وأدلتها، وحتى يتمكن كل من قاضي الموضوع أو أحد من الخصوم الرجوع إلى هذا المحضر لتوضيح أي من الوقائع الثابتة به[3] فمبدأ المواجهة تحدثت عنه المواد من 155، 168، 177، وما بعدها، 300 أما الضمانات القانونية للمتهم تحدثت عنه المواد 51 مكرر، 100 وما بعدها، 123، 134، 135.[4]

ثالثا: شرط بلوغ الإقناع القضائي درجة اليقين.

يجب على القاضي أن يصدر الحكم عن إقتناع يقيني بالأدلة المحصلة من الوسائل الإلكترونية فاليقين هو وجود حقيقة يستنتجها القاضي الجنائي بواسطة المعرفة الحسية بعيدا عن كل غموض أو إحتمال وهذا عن طريق معاينة القاضي لهذه الوسائل وفحصها بالمعرفة الذهنية وإستقراء النتائج ليتأكد من وجود الحقيقة[5]، فشرط اليقين في أحكام الإدانة هو شرط عام، حيث أنه سواء كانت الأدلة

---

[1] نفس المرجع،ص 268

[2] علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، منظمة المؤتمر شرطة دبي، مركز البحوث والدراسات، ع1، دبي، الامارت العربية 2003 ، ص38

[3] عائشة بن قارة ، مرجع سابق، ص 271-273

[4] علي محمود علي حمودة ، مرجع سابق ، ص 37

[5] عائشة بن قارة، مرجع السابق، ص277.

التي يستنتج منها تقليدية أو مستحدثة كالدليل الرقمي، لذلك لابد أن يكون الدليل الرقمي غير قابل للشك، إذ أن هذا الأخير يفسر لصالح المتهم إستنادا إلى قاعدة أن الأصل في الإنسان البراءة، فيكفي أن يتشكك القاضي من صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة، وذلك إعمالا بمبدأ تفسير الشك لصالح المتهم، وهذا ما نصت عليه المادة 59 الفقرة الأخيرة من الدستور الجزائري[1].

وإذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالمعرفة الحسية أو العقلية عن طريق التحليل والإستنتاج، فإن الجزم بوقوع الجريمة المعلوماتية ونسبتها إلى المتهم المعلوماتي تحتاج من القاضي نوع آخر من المعرفة وهي المعرفة العلمية بالأمور المعلوماتية خصوصا أن القاضي الجنائي يلعب دورا إيجابيا في الإثبات، ويؤدي الجهل في هذه الأمور إلى التشكيك في قيمة الدليل الرقمي، وبالتالي يقضي إلى الحكم بالبراءة، ويستفيد من هذا الشك المتهم المعلوماتي مما يؤدي إلى إفلات المجرمين من تطبيق العدالة والقانون، ومن ثم يترتب على ثبوت التهمة بلوغ الإقتناع بالإدانة درجة اليقين من طرف القاضي الجنائي لأن الإقتناع ثمرة اليقين[2].

الفرع الثاني: مناقشة الأدلة الجنائية الرقمية.

فالقاضي لا يمكن أن يبني حكمه ويؤسس اقتناعه الشخصي إلا على العناصر الإثباتية والأدلة التي طرحت أمامه بجلسة المحاكمة وأثناء التحقيق النهائي للدعوى المنشورة أمامه وهذا ما أقر به المشرع الجزائري، ومن الأسس التي تقوم عليها الأدلة أن القاضي لا يمكن أن يباشر سلطته في تقدير هذه الأدلة ما لم تطرح في الجلسة وبحضور الخصوم وتتم مناقشتها، وغاية ذلك أن يتاح لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة إزاءه، ويبين موقفه منها ومن مقتضيات هذا الضابط أن تعرض أدلة الدعوى جميعا في جلسة المحاكمة وتطرح للمناقشات، فالشاهد يدلي بشهادته والمتهم يدلي بأقواله و يقرأ تقرير الخبرة.

وضابط وضعية الدليل الرقمي يقوم على عنصرين أساسيين حيث يتمثل العنصر الأول في إتاحة الفرصة للخصوم للاطلاع على الدليل والرد عليه، أما العنصر الثاني يتمثل في أن يكون الدليل أصلا في أوراق الدعوى.

بالنسبة للعنصر الأول فحواه أنه على القاضي مبدئيا أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم، حتى يكونوا على بينة مما يقدم ضدهم من أدلة ليتمكنوا من مواجهة هذه الأدلة والرد عليها، وهذا احتراما لحقوق الدفاع والذي يعد أحد المظاهر الأساسية في القانون[3].

ويتيح مبدأ المواجهة تجسيد هذا الأخير حيث يقضي مبدأ حق الدفاع حضور كل الخصوم في الدعوى وأن يطلع خصومه على ما لديهم من أدلة ويواجه بها وأن يناقش كل واحد منهما أدلة الطرف الآخر ومبدأ المواجهة، يجب أن تتوفر فيه نوعين من الضمانات:

---

[1] نصت المادة 59 من الدستور الجزائري 2020 على :"يستفيد المتهم من قرينة البراءة و يفسر الشك لفائدته"

[2] عائشة بن قارة مصطفى ، المرجع السابق، ص 278-279.

[3] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص237.

أ- تكون سابقة على عملية المواجهة الأولى ذاتها بين طرفي الدعوى وهو يتضمن ضرورة إحاطة المتهم بالتهم المنسوبة إليه وأن يمنح الوقت والوسائل اللازمة لتحضير دفاعه وأن يسمح له بالاستعانة عند الاقتضاء بمترجم.

ب- من الضمانات يتم أثناء عملية المواجهة ذاتها وهي الأكثر تأثيرا في الدعوى العمومية إذ يلزم أن يسمح لكل طرف بتقديم ما لديه من سندات وسؤال الشهود والخبراء وأن يطالب بإتخاذ أي إجراء يقدر فائدته وإثارة أي دفع أو إيداع مذكرات ثم حق كل طرف في مناقشة تقارير الخبرة والبحث فيما ورد فيه، ولهذا فإنه لا يجوز للقاضي الجنائي أن يبني إقتناع قدمه أطراف الدعوى إلا إذا عرض هذا الدليل في جلسة المحاكمة، إذ أن العدالة تقتضي أن حكم القاضي يأتي بعد مناقشة هادئة ومجادلة حرة ومتكافئة لكل صاحب حق مشروع في الدعوى[1].

أما بالنسبة للعنصر الثاني من ضبط وضعية الدليل يتمثل في أن يكون أصل في أوراق الدعوى حتى يكون اقتناع القاضي الجنائي مبني على أساس ومن أجل ذلك أوجب المشرع تحرير محضر الجلسة لإثبات وقائع الدعوى الجزائية وأدلتها لكي يتمكن قاضي الموضوع أو أي شخص من الخصوم للرجوع إلى هذا المحضر إذا ما رغبوا في إيضاح أي من الوقائع الثابتة به بهدف منع التحكم من طرف القاضي الجنائي وتحقيق العدالة بالإضافة إلى ذلك فإن الغرض أيضا تمكين المحكمة المطعون أمامها من مراجعة الحكم المطعون فيه وتقديره من حيث الخطأ والصواب[2].

ويجوز له أن يستند إلى معلومات عامة التي يفترض الكل أن يعلم بها والتي يكتسبها القاضي من خبرته وثقافته العامة، مما لا تلتزم المحكمة قانونا ببيان الدليل عليه فهي لا تعد من قبيل المعلومات الشخصية المحظورة على القاضي أن يبني حكمه عليها، إلا أن ما ينبغي الإشارة إليه أن هذه القاعدة يجب أن لا تتعارض مع الدور الايجابي للقاضي في البحث عن الحقيقة أو عن حريته بالاستعانة بكافة وسائل الإثبات طالما أنه يطرح الأدلة المتحصلة عليها للمناقشة بين أطراف الدعوى، فالحضر يقع على المعلومات التي يستقيها بصفة شخصية وليس بصفته القضائية وهذه القاعدة ورد عليها استثناء أنه لا يجوز للقاضي أن يحكم بما رآه وسمعه بنفسه[3].

المطلب الثاني: الرقابة على مبدأ الاقتناع الشخصي للقاضي الجزائي .

إن مبدأ الاقتناع الشخصي للقاضي الجزائي لا يعني أنه حر في تصرفاته وأن يحكم بما يشاء حسب أهوائه، بل ألزمه المشرع بعدة ضوابط ينبغي عليه احترامها والعمل بها ومنها ضوابط تتعلق بإجراءات التحقيق النهائي وضوابط أخرى تتعلق بتسبيب الأحكام والقرارات الجزائية والطعن فيها.

الفرع الأول: الضوابط المتعلقة بإجراءات التحقيق النهائي.

لقد وضع المشرع جملة من المبادئ على القاضي يجب مراعاتها أثناء التحقيق النهائي في الجلسة التي من خلاله يمكن له بناء قناعته، فالقاضي يبني اقتناعه بناءا على ما يدور في الجلسة وهذا يعتبر كضمان للمتهم، وأهم ضابط للقاضي يتجسد في المبادئ ذات الطابع الإتهامي لإجراء التحقيق

---

[1] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في الإثبات الجنائي في القانون الجزائري، مرجع سابق، ص272.

[2] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، مرجع سابق، ص237.

[3] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في الإثبات الجنائي في القانون الجزائري، مرجع سابق، ص 272.

النهائي، فالضابط الموضوعي لاقتناع القاضي يتمثل في الخصائص العامة التي تميز إجراءات المحاكمة.

أولا: مبدأ شفوية المرافعات.

بمقتضى هذا المبدأ، فإن القاضي لا يكتفي في تكوين اقتناعه على ما كتب في محاضر التحقيق الابتدائي، وإنما يتوجب عليه أن يسمع الشهود وإعتراف المتهم بنفسه وما يدلي به الخبراء ويطرح جميع الأدلة الأخرى للمناقشة الشفوية والذي يعتبر صلة قوية بمبدأ القناعة القضائية، والذي يفترض فيه أن يستمد قناعته من حصيلة المناقشات التي تجري أمامه في الجلسة[1]، والأصل في إجراءات المحاكمة أن تجري شفاهة أمام القاضي وفي حضور جميع الخصوم ويقدم كل منهم طلباته وأوجه دفاعه، ويترتب على مبدأ الشفوية أن ينبغي على الشهود أن يدلوا بشهاداتهم شفويا كما يمكن لرئيس الجلسة أن يمنح لمساعديه أو للمحلفين وثائق مصورة أو تقرير خبير قبل سماع الشهود والخبراء أو تقديم وثائق أخرى من غير قراءتها شفويا أو قبل الاطلاع عليها من طرف المتهم، وينبغي على الخبراء أن يتلو تقاريرهم شفويا، إلا أن أهم شيء هو استجواب المتهم شفهيا من طرف الرئيس والاستماع إلى تفسيرات الأطراف ودفاعهم وإلى محاميهم، كما أن الأسئلة التي تطرح على الشهود ينبغي أن تطرح شفاهة .

فشفوية المرافعات قاعدة أساسية يترتب على إغفالها بطلان إجراءات المحاكمة، لأن ذلك الإغفال معناه من جهة بناء الحكم على غير عقيدة القاضي الذي أصدره، ويؤدي من جهة أخرى إلى الإخلال بحق الدفاع بحرمان الخصوم من الإلمام بالأدلة المقدمة ضدهم ومناقشتها قبل بناء الحكم عليها[2].

ثانيا: الإجراءات العلنية.

من المبادئ الأساسية المقررة في مختلف التشريعات الحديثة أن تجري المحاكمة في جلسة علنية وهي تشكل إحدى أهم الضمانات الممنوحة للمتهم وضمان لمصداقية العدالة وهو مبدأ دستوري وقد عبرت عنه المحكمة العليا في إحدى قراراتها "القاعدة العامة هي أن مبدأ العلنية يحكم جلسات المحاكمة في المواد الجزائية باعتبار أن حق الجمهور في حضور الجلسات ضمان لمصداقية العدالة وللرقابة على الإجراءات المتبعة أمامها"، لذا أوجبت المادة 300 من قانون الإجراءات الجزائية[3] على علنية جلسات المحاكمة والمادة 308 من قانون الإجراءات الجزائية[4] على حضور الجمهور ومن جهتها تنص المادة 365 من قانون الإجراءات الجزائية[5] على كيفية النطق بالحكم أو القرار في جلسة علنية، لذلك قضي بأن مبدأ العلنية إجراء جوهري يتعلق بالنظام العام[6].

---

[1] محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة للنشر، ط7، الإسكندرية، مصر، 2005، ص796.

[2] محمد زكي أبو عامر، الإجراءات الجنائية، مرجع سابق، ص797,

[3] نصت المادة 300 من ق.إ.ج: "يجب أن تكون الجلسة علنية، إلا إذا إقتضت المصلحة العامة أو النظام العام أو الآداب العامة أن تعقد الجلسة سرا بقرار معلل من المحكمة".

[4] نصت المادة 308 من ق,إ.ج: "حضور الجمهور خلال المحاكمة أمام محكمة الجنايات تعيد تأكيد مبدأ العلنية".

[5] نصت المادة 365 من ق.إ.ج: "يجب أن يكون النطق بالحكم في جلسة علنية يتلو الرئيس أو أحد القضاة الحكم".

[6] جلالي بغدادي، الاجتهاد القضائي في المواد الجزائية، الجزء3، مؤسسة لازار بلوس للطبع، الجزائر، 2016، ص250.

ولكن كإستثناء من هذه القاعدة فقد تنعقد جلسة المحاكمة في سرية وهذا لإعتبارات تتعلق بالنظام العام والمحافظة على الآداب وهذا ما نصت عليه المادة 300 من قانون الإجراءات الجزائية أما بالنسبة للمحاكمة الخاصة بالأحداث فإن المرافعات تكون سرية وينطق بالحكم في جلسة علنية.

ثالثا: مراعاة المواجهة بين الخصوم.

يسهل ضابط المواجهة بين الخصوم مهمة القاضي في كشف الحقيقة والوصول إلى تكوين اقتناعه المطلوب في الأحكام الجزائية، في الحقيقة التي ينشدها الحكم الجنائي ليست نسبية أو مفترضة وإنما حقيقة واقعية وهذه لا يمكن توافرها إلا باليقين القضائي لا بمجرد الظن والاحتمال، فالاقتناع هو مناط الحقيقة القضائية وليس هو الذي ينفرد به القاضي باعتباره اقتناعا شخصيا بل هو الاقتناع الذي يفرض نفسه على القاضي وعلى كافة من يطلعون بالعقل والمنطق على أدلة الدعوى، فيجب أن تخرج الحقيقة التي تلوح في ذهن القاضي لكي تنتشر في ضمير الكافة ويستوي في الحقيقة التي يعلنها الحكم، أن تكون في صالح الاتهام أو في صالح المتهم لذلك فإن إجراءات الكشف عن الحقيقة لا ينبغي أن تتوفى إثبات الإدانة بقدر ما يجب أن تتسم بالموضوعية وتوفير الضمانات التي تكفل المحاكمة العادلة ليس للمتهم فحسب وإنما لجميع أطراف هذه الدعوى، فالقاضي لا يتمكن من تكوين اقتناعه تكوينا سليما إلا عن طريق تمتع أطراف الخصومة بما فيهم المتهم والضحية وكذا دفاعها بالحرية التامة وتكافئ الفرص بينهم أثناء هذه المرحلة الحاسمة والمتميزة بخطورتها ودقة إجراءاتها[1].

الفرع الثاني: ضوابط تتعلق بتسبيب الأحكام والطعن فيها.

يعد تسبيب الأحكام القضائية والطعن فيها من أبرز الضمانات التي تكفل حسن سير العدالة، وتحقق مبدأ الشفافية والرقابة على العمل القضائي، فالتسبيب هو الذي يكشف عن الأساس الذي بني عليه الحكم ويبرز مدى إلتزام القاضي بالتطبيق الصحيح للقانون على الوقائع المطروحة أمامه، مما يضفي على الحكم قوة الإقناع ويعزز من شرعيته، ومن جهة أخرى فإن تمكين الخصوم من الطعن في الأحكام يعد من أهم الحقوق الإجرائية التي تتيح لهم الدفاع عن مصالحهم وتصحيح ما قد يشوب الحكم من أخطاء ومن هنا جاءت الأنظمة القضائية لتضع ضوابط دقيقة تنظم تسبيب الأحكام وتحدد شروط وإجراءات الطعن فيها، تحقيقا للعدالة وحماية للحقوق.

أولا: التسبيب.

يعد التسبيب ضمانة للحكم الجنائي كما أنه ضمان لحياد القاضي وعدم ميله حيث أن العدالة تستوجب أن يحاكم الناس جميعا على منهج واحد ومن الظلم تطبيق قرارات مختلفة على المتقاضين وقد أقرت محكمة النقض المصرية في إحدى أحكامها بأن تسبيب الأحكام من أعظم الضمانات التي فرضها القانون على القضاة، إذ هو مظهر لقيامها بما عليهم من واجب التحقيق والبحث وإمعان النظر للوصول إلى الحقيقة التي يعلنوها فيما يرونه ويقدمونه بين أيدي الخصوم والجمهور، وبه يرفعون ما يتبادر للأذهان من الشك[2].

---

[1] فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، مرجع سابق، ص267-268.

[2] إيمان محمد علي الجابري، يقين القاضي الجنائي، دراسة مقارنة في القوانين المصرية والإماراتية والدول العربية والأجنبية، منشأة

فتسبيب الأحكام هو شرط موضوعية القاضي فهي التي يستند عليها حتى يقوم عليها الحكم الجزائي أي الحجج التي يقوم عليها الحكم الجزائي، والتي استخلص منها منطق الحكم وهي الأسانيد والمقدمات المنطقية التي تقود إلى النتيجة التي خلص إليها الحكم من حيث إدانة المتهم وبراءته فهي تمثل التسجيل الدقيق والكامل للنشاط القضائي المبذول من قبل القاضي لإصدار الحكم والمراد ببيان الأسباب القانونية لبيان الجريمة وظروفها والنص المطبق عليها أما الأسباب الموضوعية والواقعية يقصد بها بيان الأدلة التي بنى عليها القاضي قناعته، فإذا كان القاضي حر في تكوين اقتناعه بما يمليه عليه ضميره فإن ذلك لا يعفيه من تسبيب أحكامه، والتسبيب يدعو القاضي إلى تمحيص رأيه، إذ يلتزم بصياغة مقدمات تؤدي عقلا ومنطقا إلى النتيجة التي انتهى إليها، ولا يصدر حكمه تحت تأثير عاطفة عارضة أو شعور وقتي[1].

ثانيا: الطعن في الأحكام والقرارات الجزائية.

يحرص المشرع على أن تنقضي الدعوى الجزائية بحكم أقرب ما يكون إلى الحقيقة الواقعية والقانونية غير أن إحتمال الخطأ وارد بالنسبة للعمل القضائي عامة والأحكام على وجه الخصوص، ومصدر هذا الاحتمال هو أن القاضي بشر يصيب ويخطئ في عدم الإحاطة الشاملة والمطلقة بجميع عناصر الدعوى، وهو الأمر الذي جعل المشرع يمنح فرصة لأطراف الدعوى ليتمكنوا من استظهار عيوب الحكم والمطالبة لدى الجهة القضائية المختصة بإلغاء هذا الحكم أو تعديله، وتعرف طرق الطعن في الأحكام بأنها مجموعة من الإجراءات تستهدف إعادة طرح موضوع الدعوى على القضاء بغية تقدير قيمة الحكم في ذاته، ومن ثم إلغاء الحكم أو تعديله[2].

والحكمة من رخصة الطعن في الأحكام هي منح ضمانة لمن حكم عليه ضد أي خطأ من جانب القاضي وذلك بإجازة عرض الأمر على القضاء من جديد وقبل أن يصبح الحكم حجة على الكافة ويصبح عنوانا للحقيقة[3].

وبالرجوع إلى المشرع الجزائري فإنه توجد طرق طعن العادية المتمثلة في المعارضة والاستئناف وطرق الطعن غير عادية وتتمثل في الطعن بالنقض وإلتماس إعادة النظر وعلى سبيل المثال تكون المعارضة في الأحكام والقرارات الغيابية أمام نفس الجهة التي أصدرت الحكم ومن أثارها توقف تنفيذ الحكم أو القرار الغيابي وتلغي ما قضى به وإعادة الخصومة أمام نفس الجهة مصدرة الحكم أو القرار[4].

المعارف للنشر، الإسكندرية، مصر، 2005، ص384.

[1] فاضل زيدان محمد، مرجع سابق، ص336.

[2] محمد مجيب حسني، شرح قانون الإجراءات الجنائية، ط3، دار النهضة العربية، القاهرة للنشر والتوزيع، عمان، 2005، ص999.

[3] محمد سعيد نمور، أصول الإجراءات الجزائية، شرح لقانون المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص544

[4] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هوما للنشر والتوزيع، 2010، ص133.

الخاتمة

مع تطور الاتصال والمعلوماتية في العصر الحديث وارتباطها بأجهزة الكمبيوتر والانترنت، وبمقدار الإفراط في استعمال هذه الوسائل ظهر نوع جديد من الجرائم المقترنة بهذه الثورة التكنولوجية لم يكن معروفا في السابق، جعل من الفقه يبحث عن إعطاء مفهوم محدد لهذه الجرائم والتي اصطلح على تسميتها بالجريمة المعلوماتية، فالجزائر على غرار دول عديدة سعت بكل جهودها من أجل مكافحة هذه الجرائم المستحدثة مع أنها فرضت نوعا من الخصوصية، بحيث أصبحت لصيقة بهذه الجرائم نظرا لشمولها مجالات عديدة ونظرا كذلك لخطورة أثارها.

وإن كان لم يتفق الفقه حول إعطاء مفهوم محدد للجرائم المعلوماتية فإن غالبية الدول والتي من بينها الجزائر سعت إلى إرساء أرضية حقيقية من أجل مكافحة هذه الجرائم بالرغم من كل الصعوبات المقترنة بها.

تمتاز الجريمة المعلوماتية بعدة خصائص تميزها عن باقي الجرائم التي تصنف في خانة الجرائم الكلاسيكية بينما هي خصائص عامة ومنها ما ارتبط بها بصفة خاصة الأمر الذي جعلها تحتل موقعا هاما في المنظومات الجنائية الدولية والوطنية، وهو الذي نتج عنه القيام بإنشاء معاهدات واتفاقيات دولية وإقليمية لمحاربة هذه الظاهرة الجديدة على العالم بالاعتماد على تضافر الجهود الدولية والتعاون الدولي.

كما انعكس نفس الأمر على السياسة التشريعية في الجزائر من خلال تعديل قانون العقوبات ومن خلال حماية حقوق الملكية الفكرية وكذا حماية المعطيات الشخصية والجريمة المعلوماتية المتعلقة بتكنولوجيات الإعلام والاتصال.

وعليه ومن أجل حماية فعلية لمجابهة الجرائم المعلوماتية في الجزائر لابد من العمل على تجسيد حقيقي للحماية الجنائية للمعطيات عبر تطوير أنظمة الحماية التقنية في إطار المعالجة الآلية للمعطيات، كما يجب العناية بالعنصر البشري المتخصص في مكافحة هذه الجرائم سواء من ناحية التكوين أو من ناحية المتابعة ومواكبة مختلف الأنظمة الجنائية المقارنة، وكذلك تطوير عملية تبادل الخبرات والكفاءات بين مختلف الدول لاسيما المجاورة.

كما حان الوقت للعمل على توحيد النصوص القانونية وضم القواعد الواردة في قانون العقوبات مع كل القوانين الأخرى المتعلقة بمكافحة الجرائم المعلوماتية في نص واحد تحت المسمى قانون مكافحة الجرائم المعلوماتية والقانون 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ولإثبات هذه الجريمة كان لابد من توافر أدلة رقمية التي لديها دور كبير في إثبات هذه الجريمة حيث يعد الدليل الرقمي من أهم نتائج التطورات الحديثة الحاصلة في مجال الإعلام الآلي والانترنت كما كان له الدور البارز والفعال في إثبات مختلف الجرائم المعلوماتية نظرا للدقة الموضوعية التي يتسم بها والتي جعلت منه دليلا حاسما ويقينيا، لهذا فقد عمدت أغلب التشريعات إلى اعتماده كدليل إثبات ضمن منظومتها القانونية.

وحتى يعتبر الدليل الرقمي دليلا لابد من وجود ضوابط منها ما يتعلق بالمعلومات محل الدليل الرقمي فهي كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو نقله أو مشاركته أو نسخه بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وهذه المعلومات قد تنشأ أو تتكون دون تدخل من الإنسان، ومنها ما يتعلق بالقوة الثبوتية لهذه المعلومة، فيشترط لإعتبار معلومة الكترونية ما دليلا رقميا أن تكون قادرة على إثبات إرتكاب الجريمة ونسبته إلى فاعلها، أما ما يتعلق منها بالوسيط الذي يحيا فيه الدليل الرقمي، حيث يمتد إلى جميع الأجهزة الرقمية وشبكات المعلومات، متى كانت لديها القدرة على تخزين أو نقل أو استخراج المعلومات، وبالنسبة لما يتعلق منها بالوسائل التي يمكن كشف الدليل الرقمي بها فيكون ذلك عن طريق أجهزة أو برامج أو تطبيقات تكنولوجية خاصة، فكل تفاعل من المستخدم مع وسائل تقنية المعلومات أو أجهزة الحاسب الآلي أو الأجهزة الرقمية ينتج عنه مجموعة من الآثار الرقمية والتي تتحول إلى دليل رقمي متى أمكن استخدام الأجهزة أو التطبيقات التي تربط بينها وبين الجريمة المرتكبة.

فالدليل الرقمي مهما تقدمت طرقه وعلت قيمته الفنية أو العلمية في الإثبات فدوره لا يكتمل إلا بوجود قاضي جزائي يملك سلطة تقديرية واسعة لازمة لتصفية الدليل من أي خطأ، كما نجد أن أهمية السلطة التقديرية للقاضي تظهر في جعل الحقيقة العلمية حقيقة قضائية.

فالحقيقة مهما كانت في حاجة إلى دليل لإثباتها، فلابد للدليل الذي تقوم به أن يكون متطورا ليستمر في ممارسة دوره كأداة لإثبات الحقيقة وبالتالي تطور وسائل استخلاصه.

ونتيجة لهذا نجد أن الدليل الرقمي فرض نفسه كدليل إثبات في المجال الجنائي يتمتع بقوة ثبوتية وحجية كافية على الرغم من طبيعته المعقدة والخاصة وصعوبة العمل به.

وبعد التطرق لموضوع يكتسي أهمية بالغة كونه يتعلق بأحد المواضيع المستحدثة في إطار القانون الجزائي، والذي يعالج إثبات أحد أخطر الجرائم الحالية التي تقوم على التقنية الرقمية ومن خلال الدراسة النظرية والتحليل القانوني توصلنا إلى مجموعة من النتائج المهمة حول دور الأدلة الرقمية في إثبات الجرائم المعلوماتية.

النتائج:

- إعتراف الأنظمة القانونية الحديثة بالأدلة الرقمية حيث تبين أن العديد من الدول خصوصا تلك التي طورت قوانين خاصة بالجريمة المعلوماتية، قد إعترفت بالأدلة الرقمية كوسائل إثبات جنائي، شرط مراعاة الضوابط القانونية والإجرائية لجمعها وتحليلها.
- تأثير الكفاءة الفنية على فاعلية الإثبات فقد أظهرت الدراسة أن الكفاءة التقنية للجهات الأمنية والقضائية تلعب دورا محوريا في فاعلية الإثبات، حيث أن ضعف المهارات أو غياب التدريب قد يؤدي إلى رفض الأدلة أو التشكيك في مصداقيتها.
- مواجهة الأدلة الرقمية لتحديات قانونية وتقنية معقدة حيث أوضحت النتائج أن الأدلة الرقمية تواجه صعوبات متعددة مثل سهولة التلاعب بها وصعوبة إثبات نسبتها إلى شخص بعينه وحاجتها لخبرات متخصصة لفهمها وتفسيرها.

- قصور بعض التشريعات الوطنية حيث كشفت الدراسة عن وجود فجوات تشريعية في بعض الدول، ما يؤدي إلى ضعف الحماية القانونية للأدلة الرقمية، ويؤثر سلبا على إمكانية قبولها أمام القضاء، خاصة في غياب نصوص قانونية صريحة تنظمها.
- أهمية الخبرة الفنية في تفسير الأدلة الرقمية وذلك بالاعتماد على خبراء في الأدلة الجنائية الرقمية أمر ضروري، نظرا للطابع الفني المعقد لهذه الأدلة وهو ما يعزز من مصداقيتها ويضمن فهم المحكمة لها بشكل دقيق.
- تزايد الحاجة إلى تطوير البنية القانونية والمؤسسية فقد أكدت النتائج أن التطور السريع في تقنيات المعلومات يفرض على المشرعين تحديث القوانين بشكل مستمر وإنشاء وحدات متخصصة داخل الأجهزة الأمنية والقضائية للتعامل مع الجرائم السيبيرانية بكفاءة.
- يعتبر هذا النوع من الأدلة دليل ذاتي قائم بنفسه متميز عن غيره من باقي الأدلة، فهو بالإضافة إلى كونه من طبيعة تقنية غير مرئية يتميز بسهولة حركته بين الأنظمة التقنية الحديثة مما يكسبه خاصية الاتساع العالمي، يضاف إلى هذا قابليته للنسخ مما يكسبه ميزة صعوبة التخلص منه.
- إن الدليل الجنائي الرقمي يقوم على أسس علمية وموضوعية وهو بذلك ينتمي إلى طائفة الأدلة العلمية، وفي تعريفه عبارة عن مكون رقمي لتقديم معلومات في أشكال متنوعة تتجسد في نصوص مكتوبة أو صور أو أصوات أو رسومات بغية اعتماده أمام أجهزة إنفاذ وتطبيق القانون.
- محل الدليل الجنائي الرقمي هو الجريمة المعلوماتية وتعرف بأنها كل استخدام مخالف للقانون يقع على النظام المعلوماتي أو أحد ملحقاته أو على شبكات الاتصالات أو بواسطتها رتب القانون له عقوبة.
- تتميز الجرائم المعلوماتية بوقوعها في بيئة المعالجة الآلية للبيانات، مما أكسبها صعوبة في الاكتشاف وبالتالي صعوبة في الإثبات، وهي لا ينجم من وراء ارتكابها أثار مادية ظاهرة فلا وجود لجثة أو بقع دم، كما تتميز بأنها جرائم خفية حيث في أحيان كثيرة لا يدري حتى المجني عليه بوقوعها، وهي نوع لا يعرف الحدود وهذا راجع إلى سلاسة في حركة المعلومات عبر شبكات الاتصالات الحديثة حيث أن القائم على النظام المعلوماتي يستطيع ارتكاب أي جريمة معلوماتية في أي دولة من دول العالم.
- فيما يخص طرق إثبات الدليل الرقمي فقد نصت التشريعات المختلفة على إجراءات متعددة تستهدف استخلاص الأدلة وتجميعها، ولقد انقسمت التشريعات في مدى إمكانية تطبيق وسائل الإثبات التقليدية لاسيما التفتيش والضبط في الوسط الرقمي.
- وازن المشرع الجزائري في عملية مكافحة الجرائم المعلوماتية واستخلاص الأدلة الجنائية الرقمية المثبتة لها ما بين حق المجتمع في عقاب المتهم من خلال تشريع إجراءات استثنائية وبين الحق في عدم انتهاك حرمة الحياة الخاصة.
- تعد قطعية الدليل الجنائي الرقمي من الضمانات المتعلقة بالدليل الجنائي الرقمي التي تفيد القاضي الجنائي في حرية اقتناعه، ويتم التأكد من مصداقية الدليل الرقمي بإتباع اختبارات الثقة للوصول إلى سلامته وصحته.

- الدليل الرقمي مثله مثل باقي الأدلة يجب أن يخضع لقاعدة وجوب طرح الدليل في الجلسة، ويترتب عن هذا أن لا يحكم القاضي بناء على معلوماته الشخصية في إطار الجرائم المعلوماتية، كما يجب على القاضي ألا يحكم بناء على معلومات الغير إلا إذا كان الغير هو الشاهد المعلوماتي أو كان خبيرا انتدبته المحكمة لممارسة خبرة في العالم الرقمي.

التوصيات:

- تطوير التشريعات الوطنية وذلك بضرورة سن أو تحديث القوانين المتعلقة بالأدلة الرقمية والجرائم المعلوماتية، بحيث تنظم بشكل واضح آليات جمعها، وحفظها، وتحليلها، وتحدد شروط قبولها أمام القضاء.
- إنشاء وحدات متخصصة وذلك بدعم وتوسيع إنشاء وحدات متخصصة في الجرائم المعلوماتية داخل أجهزة الشرطة والنيابة العامة، تضم كوادر مدربة ومؤهلة في مجال التحليل الرقمي والأمن السيبيراني.
- تعزيز التدريب الفني والقانوني وذلك بتوفير برامج تدريب مستمرة للقضاة، ووكلاء النيابة وأفراد الضبط القضائي على طبيعة الأدلة الرقمية، وطرق التعامل معها وكيفية تقييمها قانونيا.
- التعاون الدولي في مكافحة الجريمة المعلوماتية وتتم بتشجيع تبادل الخبرات والمعلومات بين الدول وتفعيل الاتفاقيات الدولية المتعلقة بالأمن السيبيراني، نظرا للطبيعة العابرة للحدود لهذه الجرائم.
- ضرورة وجود سجل وطني للخبراء المعتمدين في الأدلة الجنائية الرقمية، مع التأكيد على استقلالهم وحيادهم عند تقديم التقارير الفنية للمحاكم.
- إنشاء مخابر الأدلة الجنائية الرقمية التي سوف تأخذ على عاتقها فحص الدليل الرقمي وتقييمه نفيا أو إتهاما في الجرائم المعلوماتية، مع سن قوانين ومراسيم متعلقة بكيفية استخلاص الأدلة الالكترونية وحفظها والنص على توثيقها.
- دعوة المشرع الجزائري إلى مواصلة جهوده في مكافحة الجرائم الالكترونية من خلال استحداث قوانين الوقاية منها .
- إنشاء معاهد أو على الأقل إضافة تخصصات في الجامعة تعنى بالأمن المعلوماتي في جميع أشكاله وكذا وضع مقاييس خاصة لدراسة الجرائم المعلوماتية بشقيها الموضوعي والإجرائي بغية الوقاية من أخطارها.
- تدريس متخصصين في البرمجة والاتصالات مع عقد دورات تدريبية مكثفة من أجل حماية الأنظمة المعلوماتية للمرافق العامة للقطاع العمومي والبنوك والمؤسسات الخاصة.
- يجب على المشرع الجزائري إحداث إجراءات للحصول على الدليل الرقمي بما يتماشى مع خصائصه وطبيعته وعدم الاكتفاء بالإجراءات التقليدية لجمع الدليل.
- وجوب تدريب القضاة والخبراء والمحققين على التعامل مع الجرائم الالكترونية.

قائمة المصادر والمراجع:

المصادر:

القوانين والتنظيمات:

1- الدستور الجزائري الجديد 2020 المعدل والمتمم بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى 1442هـ الموافق 30 ديسمبر 2020 ونشر في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، العدد 82 .

2- تعديل قانون العقوبات بموجب قانون رقم 04-15 الصادر في 10-11-2004 المتمم للأمر رقم 156- 66 المتضمن قانون العقوبات.

3- القانون رقم 09-01 الصادر في 25فيفري2009 يعدل و يتمم الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات.

5- القانون 15-02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الجديد المعدل هذه المواد تنظم التحريات الخاصة في الجرائم المعلوماتية.

6- قانون رقم 09-04 المتعلق بالقواعد الخاصة بالرقابة من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها بعنوان مراقبة الإتصالات الالكترونية.

7- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتعلق بالوسائل الإجرائية الحديثة

10- القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 والمتعلق بالمساس بأنظمة معالجة البيانات الآلية

11- القانون 16-02 المؤرخ في 10 جوان 2016 بالجرائم المعلوماتية يتمثل في تمويل الإرهاب عبر شبكة الانترنت

12- قانون 18-07 هو حماية البيانات الشخصية للأفراد من الاستخدام غير مصرح به أو التسريب

13- القانون 18-04 المؤرخ في 10 ماي 2018 والمتعلق بالبريد والاتصالات الالكترونية

14- قانون الإجراءات الجزائية الجزائري.

المراسيم:

1.- المرسوم الرئاسي رقم 21-439 المؤرخ في 07-11-2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد86، المؤرخة في 11-11-2021.

2.- المرسوم الرئاسي رقم 21-439 المؤرخ في 07-11-2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد86، المؤرخة في 11-11-2021.

3. - مرسوم الرئاسي رقم 183-40 المؤرخ في 26-06-2004

4. المرسوم الرئاسي رقم 16-111 تصديق على اتفاقية إنشاء المنظمة العربية لتكنولوجيات الاتصال والمعلومات

5. - المرسوم الرئاسي رقم 21-439 المؤرخ في 07-11-2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد86، المؤرخة في 11-11-2021.

الكتب العامة:

1 - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، ط1،منشورات الحلبي الحقوقية، كلية الحقوق، جامعة حلوان، جمهورية مصر العربية،2005

2. منير محمد الجمبيهي،ممدوح محمد الجمبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

3.محمد أمين الشوابكة، جرائم الحاسوب الأولى والانترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2004

4. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الفكر الجامعي، مصر، 2009

5. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2011.

الكتب المتخصصة:

1. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015
2. خالد ممدوح إبراهيم، جرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، مصر،
3. طيب بلواضح، أدلة الإثبات الجنائي، ط1، مكتبة الوفاء القانونية، الجزائر، كلية الحقوق، المسيلة، 2022
4. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، ط1، مطبعة الشرطة، دار الثقافة، عمان،2005
5. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر،2006
6. نبيلة هبة هروال، الجوانب الإجرائية لجوانب الانترنت في مرحلة جمع الإستدلالات، دار الفكر الجامعي، الإسكندرية، 2013
7. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط1، الأردن، 2010.

الكتب باللغة الفرنسية:

1-The technical working group for electronic crime science investigation [electronic crime investigation] the national institute of justice the united state of America 2001

2- Marie Christine droit pénal général Ed ellicses parie France 2002

أطروحات الدكتوراه:

1- بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة الدكتوراه، كلية الحقوق، جامعة الجزائر1، 2015

2- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ،رسالة لنيل دكتوراه في القانون، كلية الحقوق، مسيلة،2013

3- عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، 2004

4-إبراهيم الغمار، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه ،كلية الحقوق، جامعة القاهرة، مصر ،1989

رسالة ماجستير:

1- سليمان العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2003.

2- ثنيان الناصر أل ثنيان، إثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، سعودية، 2007.

3- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، 2013

4- سيدي محمد البشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010

مذكرة الماستر:

1. اوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر ،كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة ، 2019 – 2020،
2. بن دراح علي إبراهيم، محاضرة في الجرائم المعلوماتية، مذكرة ماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، المركز الجامعي، أفلو، الأغواط، 2020-2021
3. بن زرت أسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، 2019
4. شهرزاد حداد، الدليل الالكتروني في مجال الإثبات الجنائي، مذكرة ماستر تخصص حقوق، كلية الحقوق والعلوم السياسية جامعة أم البواقي، 2017

5. طاهر عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة مسيلة، 2015
6. عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، 2015-2016
7. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر، كلية العلوم الاقتصادية والتجارية، جامعة قاصدي مرباح، ورقلة، 2019
1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية العلوم الاقتصادية والتجارية، جامعة قاصدي مرباح ورقلة، 2019.
8. فراحتية خلود،دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، كلية الحقوق والعلوم السياسية، جامعة برج بوعريريج 2021-2022.
9. مراد بنار، الجرائم المرتكبة عبر الوسائط الالكترونية، مذكرة ماستر قانون خاص تخصص العلوم الجنائية والأمنية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش، 2016-2017.
10. معمش زهية، غانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرا، بجاية، 2012-2013
11. يومايلة ابتسام، مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية، مذكرة ماستر، قسم الحقوق، كلية الحقوق و العلوم السياسية جامعة قاصدي مرباح ،ورقلة، 2020-2021

المجلات:

1. عيادي فريدة، الجريمة المعلوماتية في التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية.
2. أسامة حسين محي الدين عبد لعالي، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والاقتصادية، العدد76، جوان 2021

3. عـز الـدين عثمـاني، إجـراءات التحقيـق والتفتـيش فـي الجـرائم الماسـة بأنظمـة الاتصـال والمعلوماتيـة، مجلـة دائـرة البحـوث والدراسـات القانونيـة والسياسـية، عـدد4 ، جـانفي 2018، جامعة تبسة.
4. بن مالك احمد، الخال إبراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، جامعة تمنراست، مجلد 05، عدد 2021 .
5. ربيعـي حسـن، المجـرم المعلومـاتي شخصـيته وأصـنافه، مجلـة العلـوم الإنسـانية، عـدد40، جوان2015.
6. غريبـي بشرى، خصوصـية المجرم المعلومـاتي، مجلـة نـوميروس الأكاديميـة، جامعـة أبـو بكـر بلقايد، المجلد2، العدد2، 2021
7. عايدة بلعابد، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق العلمية، المجلد 11، عدد1، 2019
8. علي محمود إبراهيم، الأدلة الرقمية وحجتها في إثبات الجرائم الالكترونية، المجلة العلمية، كلية الشريعة والقانون، جامعة الأزهر، العدد32، إصدار 02 جويلية 2020
9. يسرى بهاء الدين الجاسم، حجية الأدلة الرقمية في النظام القضائي الإسلامي، مجلة البحوث الفقهية الإسلامية، تركيا، العدد 37، نوفمبر 2021
10. فاطمـة جخـدم، النصـوص الرقميـة المفهـوم والخصـائص، مجلـة المزهـر، أبحـاث فـي اللغـة والأدب، معهد الآداب واللغات، المركز الجامعي، سي الحواس، بريكة، باتنة، العدد6، جوان 2022
11. بوعنـاد فاطمـة الزهـراء، مكافحـة الجريمـة الالكترونيـة فـي التشـريع الجزائـري، مجلـة النـدوة للدراسات القانونية، سيدي بلعباس، العدد 01، 2013
12. قادري سوسن، عبار عمر، الدليل الرقمي بين اقتناع القاضي الجزائي ورقابة المحكمة العليا، مجلة القانون العام الجزائري والمقارن مجلد 10، العدد1، جويلية 2024

المداخلة:

1- سويسي فتيحة، تكييف القانوني للجرائم المعلوماتية والإشكالات العملية المترتبة عنها، مداخلة مقدمة خلال الندوة البحثية، مركز البحوث القانونية والقضائية، 2022.

2- حسين بن سعيد بن يوسف الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة الجزائر، 2014.

الفهرس:

الملخص:

أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية خاصة بعد اختراع الانترنت، فأمام هذا التطور فقد ارتبطت به ما يعرف بالجرائم المعلوماتية التي جاءت نتاجا لتطور التقنيات المعلوماتية، إذ أن هذه الجريمة تختلف كليا عن الجرائم التقليدية من حيث الخصائص والبيئة التي ترتكب فيها، كما أن إثبات هذا النوع من الجرائم يكون عن طريق دليل يختلف عن الأدلة التقليدية ألا وهو الدليل الرقمي.

ونظرا للتنامي الخطير لهذه الجريمة ظهرت العديد من الإشكالات القانونية والقضائية ومن بينها كيفية الحصول على الدليل الرقمي من خلال إجراءات التحقيق وما مدى حجية الدليل واقتناع القاضي الجزائي بهذا الدليل كونه يكون في بيئة افتراضية فسرعة التخلص منه أو إتلافه يسمى جريمة الكترونية فنظرا لازدياد ارتكاب الجرائم المعلوماتية المستحدثة وانتشارها في الوقت الحالي الأمر الذي دفع المشرع الجزائري إلى التدخل عن طريق سن قوانين تجرم وتعاقب الاعتداءات التي تحصل في المنظومة المعلوماتية على غرار قانون رقم 09-04 القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتعديل قانون الإجراءات الجزائية كما أن المشرع استحدث هيئات تعمل ميدانيا لمواجهة هذا النوع من الجرائم وتدريب الأجهزة الأمنية والقضائية من أجل مواكبة هذا التطور في مجال الجرائم المعلوماتية وذلك من خلال اعتماد على أدلة إثبات رقمية جديدة مستحدثة بدلا من أدلة إثبات تقليدية التي لم تعد كافية في مجال الإثبات في الجرائم.

Summary:

The world today lives in an era of technological advancement, or what is known as the information revolution, especially after the invention of the internet. This development has been accompanied by what are known as cybercrimes, a product of the development of information technology. This crime differs entirely from traditional crimes in terms of its characteristics and the environment in which it is committed. Moreover, proving this type of crime requires evidence that differs from traditional evidence, namely digital evidence.

Due to the dangerous growth of this crime, many legal and judicial problems have emerged, including how to obtain digital evidence through investigation procedures, the extent of the evidence's validity, and the criminal judge's conviction of this evidence, as it is in a virtual environment. The speed of getting rid of it or destroying it is called an electronic crime. Due to the increase in the commission of emerging information crimes and their spread at the present time, which prompted the Algerian legislator To intervene by enacting laws that criminalize and punish attacks that occur in the information system, such as Law No. 09-04, the law on the prevention and combating of crimes related to information and communication technology, and amending the Code of Criminal Procedure. The legislator also created bodies that work in the field to confront this type of crime and train the security and judicial agencies in order to keep pace this development in the field of cybercrime is achieved by relying on new, emerging digital evidence instead of traditional evidence, which is no longer sufficient in the field of proof in crimes.

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة ابن خلدون، تيارت
كلية الحقوق والعلوم السياسية

ميدان التكوين في الحقوق و العلوم السياسية

فريق شعبة التكوين في الحقوق

إذن بالإيداع

أنا الممضي أدناه،

الأستاذ (ة): بوسماحة الشيخ الرتبة : أستاذ

المشرف على الطالب : قاسم عائشة حنان

الشعبة: حقوق التخصص: جنائي

والمكلف (ة) بانجاز مذكرة ماستر بعنوان:

الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية

اصرح انني اطلعت على المذكرة و هي مستوفية لجميع الشروط المنهجية و قابلة للايداع من أجل المناقشة

تيارت في: 08 جوان 2025

توقيع الأستاذ(ة) المشرف (ة) :

ا.د/ بوسماحة الشيخ

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة ابن خلدون. تيارت
كلية الحقوق والعلوم السياسية

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية لانجاز بحث

أنا الممضي أدناه،

السيد(ة): ...قايم عائشة حنان... الصفة: طالب (ة) ماستر .

الحامل (ة) لبطاقة التعريف الوطنية رقم: ...1198900444018410009... الصادرة بتاريخ: 2024-10-17

المسجل (ة) بكلية: الحقوق والعلوم السياسية ... القسم: حقوق

الشعبة: حقوق ... التخصص: قانون جنائي

والمكلف (ة) بانجاز مذكرة ماستر بعنوان:

...الإثبات الجنائي بالجرائم المعلوماتية بالأدلة الرقمية...

...

أصرح بشرفي أن ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في انجاز البحث المذكور أعلاه.

تيارت في: 09 ماي 2025

توقيع المعني (ة):

ملحق بالقرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها.