الجمهورية الجزائريـــــة الديمقراطيـــــة الشعبة

وزارة التعليم العالـــــي و البحـث العلمـــي

جامعة محمد بوضياف المسيلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

ميدان الحقوق والعلوم السياسية

تخصص: قانون جنائي وعلوم جنائية

مذكرة مقدمة لنيل شهادة الماستر أكاديمي، تخصص قانون جنائي وعلوم جنائية

وسائل إثبات الجريمة المعلوماتية في التشريع الجزائري

اعدادالطلبة:

قعنب أمينة

لمين صبرينة

إشراف الأستاذ:

بوضياف الخير

لجنةالمناقشة

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
دحية عبد اللطيف	أستاذ التعليم العالي	جامعة المسيلة	رئيسا
بوضياف الخير	أستاذ محاضر ب	جامعة المسيلة	مشرفا ومقررا
بزاف إبراهيم	أستاذ مساعد ب	جامعة المسيلة	ممتحنا

السنة الجامعية: 2024 / 2025

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

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): امين صبرينة ..... الصفة: طالب، أستاذ، باحث طالبة .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 200331703 والصادرة بتاريخ 24.04.2016 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: .....

وسائل اثبات الجريمة المعلوماتية في التشريع الجزائري .....

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

التاريخ: 05.06.2023

توقيع المعني (ة)

* الملحق بالقرار رقم ....1082.... المؤرخ في ..... 2020 ماي 17 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقه العلميه ومكافحتها

الجمهوريه الجزائريه الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): قحتب أمينة ..... الصفة: طالب، أستاذ، باحث طالبة .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 108058689 والصادرة بتاريخ 10/13/2022 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: وسائل إثبات الجريمة المعلوماتية في التشريع الجزائري .....

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

التاريخ: 2022/06/08...

توقيع المعني (ة)

إهداء

إلى من انبثق الحب من أكفهم قبل أن أعرف معناه والدي الحنونين صخرة الأمان و منبع الإيمان، و إلى روح أبي الثاني رحمه الله أنا كنت فقط الوسيلة و أنتم الغاية التي سعيت لها بكل قلبي، و إلى أغصان دوحتي إخوتي الأعزاء، اليوم أزف لكم شهادتي كما تهدى التيجان للملوك فأنتم سكان قلبي و سر فرحتي، هذا التخرج ليس ختاما لمسيرة دراسية بل تتويجا لحبكم و صبركم، ودعمكم الذي لا ينتهي.

شكرا لكم لأنكم كنتم و ستظلون دوما أعظم انتصاراتي.

قعنب أمينة

إهـــــداء

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

"أمي محبوبتي وملهمتي"

إلى من وهبني الله نعمة وجودهم مصدر قوتي وأرضي الصلبة وجدار قلبي المتين

"إخوتي وأخواتي (دون أن أنسى أولادهم)"

إلى من رافقني بالقلب قبل الدرب

"أصدقائي و أحبتي"

ها أنا اليوم طويت صفحة من التعب وسجلت في تاريخي فخرا لا ينسى لم أعد أتساءل عن ملامح الوصول فقد رأيتها في عيوني تلاشت غيوم التعب وابتسم الأفق بعد عتمة الانتظار ها هي الخطى التي كانت تتعثر أحيانا قد وجدت مستقرها في قمة الإنجاز وبين طيات الطريق تنفست سلاما وفرحا وامتنان وآخر دعواهم أن

"الحمد لله رب العالمين"

لمين صبرينة

شكر و تقدير

قال رسول الله - صل الله عليه وسلم-

"من لم يشكر الناس لم يشكر الله"

نحمد الله جزيل نعمه، ونشكره على توفيقه لإنجاز هذه الدراسة، فبفضل مشيئته تيسر لنا كل ما هو صعب، وأضاء دربنا شعاعا منيرا فوصلنا بعونه وحسن توفيقه إلى إنجاز هذا العمل المتواضع وإتمامه، له الحمد وله الشكر أن وفقنا في تحقيق بعض ما طمحنا أليه.

نتقدم بأصدق عبارات الامتنان و العرفان إلى أستاذنا المشرف الفـــــــاضل

" الخيـــــر بوضيـــــاف"

الذي تفضل بتوجيهنا بحكمة و صبر، و إلى أعضاء لجنة المناقشة الموقرة لما قدموه من ملاحظات قيمة أثرت هذا الجهد، و أخيرا أتقدم بالشكر ل:

جامعة محمد بوضياف

التي وفرت الإمكانيات لإنجاز هذا العمل.

قعنب أمينة

لمين صبرينة

قائمة المختصرات:

ج، ر: الجريدة الرسمية

ق، ع، ج: قانون العقوبات الجزائري

ق، إ، ج: قانون الإجراءات الجزائية

ط: طبعة

ص: صفحة

د: دار النشر

د،س.ن: دون سنة النشر

د،ر،ط: دائرة الرد والطعن وتنازل الاختصاص

Abréviations :

OECD : Organiwation for Economic Co-operation and Development

مقـــدمة

مقدمة

شهدت العقود الأخيرة تحولا جذريا في نمط الحياة البشرية، تمثل ذلك في الانتشار المتسارع للتكنولوجيا الرقمية مما جعل العالم يشهد ثورة في المعلومات مجالها الفضاء الرقمي و أداتها الإنترنت، فقد حولت هذه الأخيرة العالم إلى قرية صغيرة و مكنته من توفير قفزة نوعية حيث سهلت الاتصالات و المعاملات، بل الأكثر من ذلك أنها باتت مجالا واسعا للولوج إلى العالم شاسع من المعلومات، مما جعل من المجتمعات الحديثة تعتمد على الفضاء الإلكتروني في كافة مناحي الحياة.

رغم ما وفره هذا التحول الرقمي من فرص هائلة و سهولة غير مسبوقة في التواصل و المعاملات، إلا أنه قد حمل في طياته و جها آخر مظلما تمثل في ظهور أشكال مستحدثة من الإجرام، عرفت بـ **"الجريمة المعلوماتية"**، مما حير رجال القانون، و هذه الظاهرة الإجرامية الحديثة سرعان ما أخذت منحى في التطور و التنوع و خطورة هذه الظاهرة تكمن في كونها عابرة للحدود و لا تنحصر في إقليم محدد، كما أن مرتكبها يعرف بـ **" المجرم المعلوماتي"** و يتصف هذا الأخير بصفات خاصة و يتميز بقدر كبير من المعرفة و الذكاء، و هذا ما دفع المشرع إلى الاجتهاد في إصدار قوانين ردعية لمواجهة هذه الجريمة و مرتكبها.

من الواضح أن الجريمة المعلوماتية فرضت نفسها بقوة و ازدادت خطورتها بتزايد الاستعمالات اليومية لشبكة الإنترنت، لاسيما في مجال الاقتصاد فازدادت ظاهرة سرقة الأموال و اختراق المواقع و سرقة البيانات و الاعتداء على الحياة الشخصية، و هذا ما سرع لإصدار تشريعات متخصصة للحد من هذه الجريمة لكن الصعوبة هنا قائمة على المجرمين و كيفية ملاحقتهم، فمختلف التشريعات أوجدت النص القانوني للتعريف بالجريمة الإلكترونية و تحديد العقاب لمرتكبيها و لإثبات قيام أية جريمة لابد من توفر الدليل إلا أن الدليل في هذا النوع من الجرائم يختلف عن الدليل التقليدي حيث يعرف باسم **الدليل الرقمي** و يكمن الاختلاف هنا في أن هذا الأخير يعد دليلا غير ملموس و يقع في الفضاء الرقمي و يصعب الوصول إليه لسبب بسيط هو أن الدخول إلى الحاسوب بغية التفتيش عنه أو تعقب آثار المجرم المعلوماتي يصطدم بعوائق تميزها عمليات التشفير للبيانات أو تخزينها، إذا كان توقيع العقاب سهلا فإن جمع الأدلة و إثبات الجريمة المعلوماتية و مدى صحة الدليل الرقمي و صلاحيته، مما يطرح العديد من الصعوبات و الإشكاليات القانونية.

تبرز أهمية هذا الموضوع من خلال مدى جدية و فعالية النصوص القانونية الجنائية و الإجرائية، في مسألة الإثبات في الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و التعرف على ماهية الأدلة الرقمية في المسائل الجنائية و سلطة القاضي في تقديره، كما يمكن تسليط الضوء على الصعوبات العملية و التقنية التي تعيق إثبات الجرائم الإلكترونية، و صعوبة تتبع مرتكبيها و الكشف عن آثار الجريمة في العالم الرقمي، أما الواقع العلمي قد أثبت أن الجرائم الإلكترونية عرفت تطورا مذهلا و أصبحت تشكل تحديا كبيرا و تتطلب جهودا متظافرة من طرف مختلف الأجهزة الأمنية، و يتضح بأن الوصول إلى كشف هذا النوع من الجرائم يعد تحديا كبيرا لأن الأمر يرتكز فقط على الوسائل التقنية و العلمية و هو ما يثير الرغبة لمعرفة طبيعة هذه الأدلة و كيفية الوصول إليها و تحديد طابعها القانوني و مدي حجيتها في الإثبات الجنائي.

أهداف البحث:

تهدف الدراسة إلى التعرف و دراسة العديد من النقاط و تتمثل في:

- ✓ التعرف على الجريمة الإلكترونية.
- ✓ التعرف على الطبيعة القانونية للجريمة المعلوماتية و كذا أركانها.
- ✓ التعرف على المجرم المعلوماتي و أسباب ارتكابه لهذا الجرم.
- ✓ التعرف على ماهية الدليل الرقمي.
- ✓ التعرف على الأجهزة المختصة في البحث و الكشف عن الأدلة الرقمية.
- ✓ دراسة حجية الدليل الرقمي أمام القاضي الجزائي.

أسباب اختيار الموضوع:

من بين الأسباب التي أدت إلى اختيار هذا الموضوع:

- تطور و انتشار الجريمة المعلوماتية مما جعلها هاجسا و خطرا على البنية الرقمية للأنظمة الحساسة في الدولة، و هذا لما تلحقه من ضرر اقتصادي و أمني.
- و السبب الآخر هو معرفة كيف تصدى المشرع الجزائري لهذا النوع من الجرائم و أيضا معرفة كيفية إثبات الجريمة المعلوماتية و جمع الدليل الرقمي.

الإشكالية:

و مما سبق ذكره، تهدف دراستنا لهذا الموضوع للتعرف على الجريمة المعلوماتية و على وسائل ارتكابها و كيفية إثباتها و أيضا التعرف على آليات و إجراءات التحري في مجال الجريمة المعلوماتية، و بناءا على ذلك نطرح إشكالية الدراسة المحورية:

ما هي وسائل إثبات الجريمة المعلوماتية في التشريع الجزائري؟

و من هذه الإشكالية الرئيسية، يتفرع عدة تساؤلات فرعية و تتمثل في:

- ✓ ما هي الجريمة المعلوماتية؟
- ✓ ما هو الدليل الرقمي؟
- ✓ ما هي إجراءات البحث و التحري عن الدليل الرقمي؟

منهج الدراسة:

استخدم في هذا البحث المنهج الوصفي التحليلي، الذي يقوم على أساس تحديد خصائص المشكلة محل البحث، و وصف ماهيتها و أسبابها، و من ثم تحليل هذه المشكلة و التعرف على أنواعها و أهدافها، و ذلك للوصول إلى وسائل إثبات الجريمة المعلوماتية في التشريع الجزائري، وهو المنهج الذي سهل لنا طريقة البحث و الوصول إلى مجموعة من النتائج الدقيقة.

للإجابة على الإشكالية الرئيسية للموضوع، مع ما يتفرع منها من إشكالات فرعية ، تم تقسيم الدراسة إلى: مقدمة و فصلين و خاتمة.

تم تخصيص **الفصل الأول** لدراسة كل ما يتعلق **بالإطار المفاهيمي للإثبات الجنائي في الجرائم المعلوماتية** من خلال مبحثين، حيث بتناول **(المبحث الأول)** ماهية الإثبات الجنائي من تعريف و أنظمة و كذا التعريف بالجريمة المعلوماتية أنواعها و أركانها، أما **(المبحث الثاني)** تم التطرق فيه إلى الأدلة الرقمية من تعريف و أنواع و خصائص.

بينما **الفصل الثاني** خصص لدراسة **إجراءات البحث و الكشف عن الأدلة الرقمية في الجريمة المعلوماتية** و ذلك في مبحثين، في **(المبحث الأول)** الإجراءات الخاصة بالبحث و الكشف عن الأدلة الرقمية أما **(المبحث الثاني)** حجية الدليل الرقمي أمام القاضي الجزائي.

الفصل الأول
الإطار المفاهيمي للإثبات الجنائي في الجرائم المعلوماتية

الفصل الأول: الإطار المفاهيمي للإثبات الجنائي في الجرائم المعلوماتية

في ظل الثورة الرقمية التي يشهدها العصر الحديث، أصبحت الجرائم المعلوماتية واحدة من أبرز التحديات التي تواجه الأنظمة القانونية و العدلية حول العالم، و لم تعد الجريمة تقتصر على الفضاء المادي و التقليدي بل امتدت إلى الفضاء الافتراضي، حيث تعرف هذه الجرائم بأنها فعل ضار يرتكب باستخدام الحواسيب أو الشبكات الإلكترونية بهدف الإضرار بالبيانات أو سرقتها أو اختراق الخصوصية أو تعطيل الأنظمة، حيث ترتكب أفعال كالاختراق و انتحال الهوية و تجارة البيانات و الاحتيال الإلكتروني و حتى الهجمات الإرهابية و غيرها من الأفعال التي تستغل الثغرات التكنولوجية.

في ظل مواجهة هذه التحديات يسعى المشرع الجزائري التي تعزيز التشريعات الرقمية وتطوير آليات الأمن السبيراني، حيث يمكن القول إن إثبات هذا النوع من الجرائم يكتسي خصوصية تميزه عن إثبات غيره من الجرائم التقليدية ، وتتجسد هذه الخصوصية بصفة أساسية فيما يكتنف هذا الإثبات من صعوبات في مجال هذه الجرائم، و يسعى هذا الفصل إلى رصد الإطار المفاهيمي للإثبات في الجرائم المعلوماتية، من خلال تحليل ماهية هذه الجرائم و خصائص أدلتها، و التحديات القانونية و العلمية التي تواجه إثباتها.

المبحث الأول: ماهية الإثبات الجنائي

يعتبر الإثبات الجنائي ركيزة أساسية في منظومة العدالة الجنائية، حيث يجمع بين العلم والقانون بهدف كشف الحقيقة و تحديد المسؤولية في الجرائم، يعتمد هذا النوع من الإثبات على تحليل الأدلة المادية و العلمية باستخدام منهجيات دقيقة و تقنيات متطورة "كتحليل الحمض النووي و بصمات الأصابع، و فحص الأسلحة النارية، و التحليل الرقمي للبيانات"، تهدف هذه العمليات إلى إعادة بناء واقع الجريمة بدقة و الربط بين المشتبه بهم و الأدلة الملموسة، مما يسهم في ضمان نزاهة التحقيقات و حقوق الأفراد في المحاكمة العادلة، و سيتم التطرق إليه من خلال تعريفه و ذكر أنظمته و كذا قواعده الإجرائية.

المطلب الأول: تعريف الإثبات و قواعده الإجرائية

يعتمد الإثبات الجنائي على منظومة متكاملة من الأدلة المادية (كالبصمات، الأسلحة) و الأدلة الرقمي (مثل بيانات الهواتف)، إلى جانب الشهادات، و لتوضيح الإثبات يجب التطرق إلى تعريفه لغويا و قانونيا

الفرع الأول: تعريف الإثبات الجنائي

أولا: التعريف اللغوي

الإثبات لغة: إن كلمة إثبات تعني لغويا" الدليل أو البرهان أو البينة أو الحجة. هو إقامة الحجة و إعطاء الدليل على صحة أم ما، و يقال أثبت حجته أي أقامها و أوضحها " و قول ثابت" أي صحيح و هو مأخوذ من قولهم " ثبت الشيء إذا دام و استقر و يقال ثبت فلان على موقفه إذا لم يتراجع عنه و يسمى الدليل لأنه يؤدي إلى استقرار الأمر لصاحبه فيقال " لا أحكم بكذا إلا إذا ثبت".[1]

ثانيا: التعريف القانوني

هناك عدة تعاريف قانونية فيما يخص الإثبات الجنائي وهذا حسب وجهات النظر المختلفة لهذه المسألة نذكر منها:

هو إقامة الدليل لدى السلطات المختصة والتي تساعدها على اتخاذ الإجراءات الجزائية والتي تثبت على واقعة قانونية ذات أهمية وذلك بإتباع الطرق والإجراءات التي حددها القانون.[2]

1 د/ بوقطوشة وردة، محاضرات في الإثبات الجنائي، تخصص القانون الجنائي و العلوم الجنائية، جامعة جيجل كلية الحقوق و العلوم السياسة، سنة 2024/2023، ص 05.

2/ د/بوقطوشة وردة، نفس المرجع السابق ، ص 06.

أو هو إقامة الدليل أمام القضاء بالطرق القانونية التي حددها القانون على وجود واقعة قانونية ترتب أثارها.

إقامة الدليل على وقوع الجريمة و إسنادها لشخص معين فاعلا أصليا أو شريك أي إثبات الجريمة بوجه عام وأن المتهم هو المرتكب لها بوجه خاص.

و يعرف في المواد المدنية بأنه" إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتب آثارها".[1]

أما في المواد الجنائية فيعرفه الفقه بأنه" كل ما يؤدي إلى إظهار الحقيقة و الحكم على المتهم في المسائل الجنائية عن طريق إثبات وقوع الجريمة في حد ذاتها و أن المتهم هو المرتكب لها، و بعبارة أخرى وقوع الجريمة بوجه عام و نسبتها للمتهم بوجه خاص.

يختلف الإثبات في المواد المدنية عنه في المواد الجزائية، و ذلك بالرجوع إلى الإجراءات المدنية التي يحكمها مبدأ أساسي و هو حياد القاضي، فهو لا يتدخل في تقديم الطلبات و إقامة الدليل على الإدعاء، بل على أطراف الدعوى البحث عن ذلك و تقديمه إليه، و دوره في ذلك يكاد يكون سلبيا، و هذا على عكس القاضي الجزائي الذي له دورا إجابي في الدعوى، و هو يبحث عن الدليل و يقيمه حتى يصل إلى إدانة المتهم أو تبرئته، و هذا ما جعل البعض يقول بأن **"الدعوى المدنية هي نشاط يجري أمام القاضي بعكس الدعوى الجنائية التي هي نشاط القاضي".**[2]

ثالثا: نطاق الإثبات الجنائي

يتمثل مضمون أو نطاق الإثبات الجنائي في عدة نقاط:

* تحديد الدليل الجنائي و فحصه و مشروعيته و تقدير أثره في جميع المراحل التي تمر بها الدعوى العمومية

* إن الإثبات الجنائي لا يقتصر على إقامة الدليل أمام قضاة الحكم بل يتسع إلى سلطات الضبطية المكلفة بالتحري و الاستدلال وسلطة الاتهام وسلطة التحقيق بمعنى أن عملية الإثبات تكون عبر كل مراحل الدعوى العمومية:

- مرحلة جمع الاستدلالات من اختصاص (الضبطية القضائية).
- توجيه الاتهام (النيابة العامة).

1- أستاذ حططاش عمر، محضرات في مقياس الإثبات الجنائي، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف المسيلة،ص3.

3- أستاذ حططاش عمر،نفس المرجع السابق، ص3.

- مرحلة التحقيق القضائي.
- مرحلة المحاكمة (هي المرحلة الحازمة المبنية على اقتناع القاضي بإدانة المتهم أو براءته).

الفرع الثاني: أنظمة الإثبات الجنائي و قواعد نظامه

أولا: أنظمة الإثبات الجنائي

إن أسلوب جمع الأدلة في القانون المقارن عرف ثالث أنظمة في الإثبات الجنائي، هي نظام الإثبات القانوني أو المقيد (الأدلة القانونية) و فيه يرصد القانون أدلة معينة لا يجوز الإثبات إلا عن طريقها، و نظام الإثبات المطلق أو المعنوي (النظام الوجداني أو حرية الاقتناع الشخصي) ، و فيه لا يقيد المشرع القاضي بأدلة معينة و إنما يكون له أن يستقي اقتناعه من أي دليل يشاء، و نظام الإثبات المختلط، و فيه يجمع المشرع بين النظامين السابقين، و معظم التشريعات القانونية تأخذ بنظام الإثبات المختلط.[1]

أ. **نظام الإثبات المقيد:** يدعى هذا النظام أيضا بنظام الأدلة القانونية أو نظام الإثبات القانوني حيث يتميز هذا النظام بالصلاحيات الواسعة للمشرع في تحديد أدلة و وسائل الإثبات للقاضي مسبقا، مع إمكانية اشتراط المشرع توافر دليل معين يحكم القاضي بناء عليه و فق عقوبة مقررة، و منه وفق هذا النظام فإن القاضي مقيد في حكمه وفق ما تحدده التشريعات الجنائية دون الرجوع إلى القناعة الشخصية له، و يقتصر دوره في مراعاة تطبيق القانون من حيث توفر دليل الجريمة و شروطها.[2]

ب. الإثبات المطلق: لا يتقيد القاضي بموجب هذا النظام بطرق محددة بل يترك له حرية الإثبات لأطراف الخصومة في أن يقدموا ما يرونه مناسب لإقناع القاضي كما يترك للقاضي تكوين اعتقاده من أي دليل يطرح أمامه و يقدر قيمة اقتناعه لكل منها حتى تتكشف لوجدانه حيث لا سلطان له أو عليه إلا ضميره.[3]

ج. الإثبات المختلط: نتيجة التي تلقاها الإثبات القانوني الذي قزم من دور القاضي و جعل منه عنصرا سلبيا في عملية الإثبات، و كذلك الانتقادات التي صاحبت تطبيق النظام الحر و التخوفات من امتداد صلاحيات القاضي و احتمالية وقوعه في الانحراف و منه المساس بحقوق الأشخاص، تم السعي إلى محاولة مزج بين النامين السابقين من أجل تحقيق التوازن بينهما و ذلك من خلال إيجاد نظام مختلط.[4]

1 أستاذ حططاش عمر، نفس المرجع السابق، ص 08.

3/2 د/ بن دراح علي إبراهيم محاضرات في مقياس الإثبات الجنائي ، المركز الجامعي آفلو، معهد الحقوق و العلوم السياسية، سنة 2022/2021، ص- ص08,07.

4 د/ بن دراح علي إبراهيم، نفس المرجع السابق، ص 8.

أما فيما يخص موقف المشرع الجزائري لقد مزج بين النظام الحر و النظام المقيد، أي انه تبنى النظام المختلط.

ثانيا: القواعد العامة للإثبات الجنائي

تحكم الإثبات الجنائي مجموعة من القواعد العامة يسمح تحديدها و فهمها في التحكم في الدعوى الجزائية كما يلي:

1- مبدأ حرية الإثبات: من خلال ما نصت عليه المادة 212 من ق إ ج ج بأن المشرع قد أخذ بالنظام الإثبات الجنائي الحر، و لكن قد استثنى المشرع الجرائم الخاصة بالأحوال التي يتطلب إثباتها أركان حددها هو سلفا كما هو الشأن في جريمة الزنا م 339 قع و أورد وسائل إثباتها من نفس القانون في م 341، حيث يكون اقتناع المشرع محل اقتناع القاضي.[1]

2- مبدأ الإقناع الشخص للقاضي: حل هذا المبدأ محلا ممتازا في نظر المشرع الجزائري، و ذلك ما نلمسه في نص المادة 212 ق، أ، ج ف 2 في شطرها الأول و التي تنص على أنه "و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"، حيث أخذ المشرع هذا المبدأ من النظام المختط، و القيود التي ترد على هذا المبدأ السابق إخراج الدليل بالجلسة و مناقشته أمام القاضي و هذا ما نصت عليه ف2 في شطرها الثاني من نفس المادة، و الأدلة التي تتناقش فيها أمام القاضي نص المشرع في م 231 إلى 235 ق إ ج " اعتراف، خبرة، شهادة، انتقال للمعاينة".[2]

3- قاعدة الشك يفسر لمصلحة المتهم: تعد قاعدة الشك إحدى النتائج المترتبة عن قرينة البراءة هذه الأخيرة التي نصت عليها دساتير العالم، و منها الدستور الجزائري في نص مادته 56، و التي أضاف إليها المؤسس الدستوري بموجب التعديل الدستوري ضرورة اعتماد محاكمة عادلة.[3]

4- مشروعية الدليل: بمعنى وجوبية الحصول على أدلة الإثبات بطرق مشروعة دون مخالفة نصوص القانون و في نفس الوقت دون المساس بحقوق الدفاع، و يطبق نفس الأمر على الشهود، كما لا يجوز استعمال وسائل تم الحصول عليها قصرا إلا إذا نص القانون عليها.[4]

1 د/ بن دراح علي إبراهيم، نفس المرجع السابق، ص 10.

4/3/2، د/ بن دراح علي إبراهيم، نفس المرجع السابق، ص-ص 09، 10.

1-2 نهلا عبد القادر الممني، ماجستير في القانون الجنائي المعلوماتي ، دار الثقافة للنشر و التوزيع 2008 الطبعة 1 ص 20.

المطلب الثاني: مفهوم الجريمة المعلوماتية

في عالم تسيطر عليه الرقمنة و تتشابك فيه العلاقات عبر الفضاء الإلكتروني، تحولت الجريمة المعلوماتية إلى ظاهرة معقدة تهدد كيانات افتراضية و واقعية على حد سواء فمع تحول البيانات إلى سلعة ثمينة و الاعتماد المتزايد على البنى التحتية الرقمية، برزت أشكال إجرامية ذكية تستغل الثغرات التكنولوجية لتحقيق أهداف تتراوح بين الإثراء غير مشروع و الإضرار بالأمن القومي و على هذا المنوال لم تعد الجريمة حبيسة الأمكنة المادية أو الأدوات التقليدية ، بل تجاوزتها إلى فضاء لا يرى يعد فيه البيت"BIT" الرقمي سلاحا و البرمجة لغة للتواطؤ.

تتسع دائرة الجريمة المعلوماتية لتشمل أنماطا متعددة، مثل الاختراقات الالكترونية و تزييف الهوية و قرصنة ، وهذا ما سيتم توضيحه من خلال فروعه.

قبل التطرق إلى تعريف الجريمة المعلوماتية لا بد من تعريف بعض المصطلحات المتعلقة بهذه الجريمة.

شرح بعض المصطلحات:

1- الحاسب الآلي: هو عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها و توجيهها باستخدام أوامر خاصة لمعالجة و إدارة المعلومات بطريقة ما، و ذلك بتنفيذ ثلاث عمليات أساسية و هي: استقبال البيانات المدخلة، و معالجة البيانات إلى معلومات و إظهار المعلومات المخرجة.[1]

2- المجرم المعلوماتي: من المجرمين الذين لا يلجئون إلى العنف بتاتا في تنفيذ جرائمهم و ذلك لأنه ينتمي إلى إجرام الحيلة، و هذا النوع من الجرائم لا يستلزم القيام بها قدرا من العناء، حيث يعتبر المجرم المعلوماتي مجرم ذكي و يتمتع بالتكيف الاجتماعي و المهارة و المعرفة.

3- الدليل الرقمي: هو ذلك الدليل الذي ينشأ في العالم الرقمي و الذي يكون على شكل مستخرج مادي يتم قبوله في جلسة المحاكمة.

4 - البِتّbit: هو أصغر وحدة في النظام الرقمي (0 أو 1) ، و هو اللبنة الأساسية التي تبنى منها جميع البيانات الرقمية كالنصوص.

5- المنظومة المعلوماتية: أو النظام المعلوماتي هي كل مكونات هذا النظام المادية Hardware، و المعنوية Software، و شبكات الاتصال الخاصة به Networks، التي يتم باجتماعها العامل مع المعطيات.

الفرع الأول: تعريف الجريمة المعلوماتية و خصائصها

لقد تباينت التعريفات المتعلقة بالجريمة المعلوماتية و تعددت و ذلك نتيجة التطور المستمر لظاهرة الإجرامية المرتبطة بتقنية المعلومات، مما أسفر على تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية.

أولا: تعريف الجريمة المعلوماتية

أ. التعريف الفقهي للجريمة المعلوماتية

اختلفت وجهات النظر بين الفقهاء في تحديد مفهوم موحد للجريمة المعلوماتية، حيث عرفها جانب من الفقه بأنها ذلك النوع من الجرائم التي تتطلب الماما خاصا بتقنيات الحاسب الآلي و نظم المعلومات لارتكابها، و لقد أعطى بعض الفقهاء تعريفات تتميز تبعا لموضوع العالم المنتمي إليه و تبعا لمعيار التعريف ذاته.

فمن التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجريم، حيث عرفها الأستاذ Rosenblatt بأنه نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه.[1]

أما التعريفات التي انطلقت من وسلة ارتكاب الجريمة فإن أصحابها ينطلقون من مبدأ الجريمة المعلوماتية تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، و من هذه التعريفات نذكر تعريف الفقيه الألماني Klaus Tiedemann بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"، وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا.[2]

كما يجب الإشارة إلى تعريف منظمة التعاون الاقتصادي و التنمية OECD للجريمة المعلوماتية بأنها فعل ضار أو غير قانوني ينفذ باستخدام التقنيات الرقمية أو شبكات الاتصال، ويستهدف الأنظمة المعلوماتية أو البيانات المخزنة فيها سواء كان الهدف هو الوصول غير المشروع أو التلاعب بالمعلومات، أو تعطيل الخدمات أو تحقيق مكاسب مادية أو معنوية بشكل غير مشروع. "تم الاستناد عل هذا التعريف من تقرير OECD، المبادئ التوجيهية لأمن نظم و شبكات المعلومات 2002.

ب: التعريف القانوني للجريمة المعلوماتية

بعد التعرض لبعض التعريفات الفقيهة للجريمة المعلوماتية، سيتم التطرق فيما يلي إلى التعريف القانوني لهذه الجريمة من طرف المشرع الجزائري.

تعريف المشرع الجزائري للجريمة المعلوماتية:

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة نيل شهادة الماستر، تخصص إدارة التحقيقات الاقتصادية و المالية، جامعة قاصدي مرباح، ورقلة، سنة 2019 ص 03.

2- الأستاذ سمير شعبان، الجريمة الالكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة و المجرم ، جامعة باتنة ، ص 116.

قبل سنة2004 لم يولي المشرع الجزائري العناية اللازمة بالجرائم المعلوماتية لكنه تدارك ذلك من خلال تعديل قانون العقوبات، الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات، ثم أعقبه القانون09-04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما.[1]

حيث عرفها المشرع الجزائري في المادة الثانية من القانون 04/09 و التي أطلق عليها اسم الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بأنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، و أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

الملاحظ من خلال قراءة المادة السالفة الذكر هو أن المشرع الجزائري اعتمد في تعريف الجريمة المعلوماتية على معيارين هما: معيار موضوع الجريمة، و معيار وسيلة ارتكاب الجريمة،[2]و تتمثل في:

1- التعريف على أساس معيار الموضوع: اعتمد المشرع الجزائري في معيار موضوع الجريمة هو المساس بأنظمة المعالجة الآلية للمعطيات كأساس لتحديد الجريمة المعلوماتية، و هي الجرائم المحددة في الفصل السابع مكرر من قانون العقوبات تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات "، و التي تحكمها من المواد 394 مكرر إلى 394 مكرر 7 من هذا القانون.

2- التعريف على أساس الوسيلة: أضاف المشرع الجزائري معيارا آخر و هو وسيلة ارتكاب الجريمة و هي المنظومة المعلوماتية، أو نظام الاتصالات الإلكترونية؛ بالقول:" .... و

1- الطاهر زخمي، الجرائم المعلوماتية في التشريع الجزائري و تدابير الوقاية منها، مجلة التشريع الإعلامي المجلد 02 العدد 01، كلية علوم الإعلام و الاتصال جامعة الجزائر 3 نشر 2023/10/23، ص- ص .23,05

2- عبد القادرعميمر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم في القانون العام تخصص القانون الجنائية، جامعة الجزائر1 كلية الحقوق 2020، ص 19.

أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصال الإلكترونية.[1]

و عليه فإن المشرع الجزائري قد قسم الجريمة المعلوماتية إلى قسمين يضم القسم الأول الجرائم التي ترتكب ضد نظام المعالجة الآلية للمعطيات و تستهدف المساس الكلي أو الجزئي بهذه المنظومة، و هي الجرائم المنصوص عليها في الفصل السابع مكرر من قانون العقوبات.

أما القسم الثاني فيتضمن كل الجرائم الأخرى المنصوص عليها في قانون العقوبات أو في القوانين الخاصة التي يتم ارتكابها أو يسهل ارتكابها باستخدام منظومة معلوماتية أو نظم للاتصالات.[2]

ثانيا: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بمجموعة من الخصائص منها خصائص ذاتية في حد ذاتها، و خصائص تستمدها من وسائل ارتكابها، و خصائص أخرى تستمدها من سمات مرتكبيها.[3]

1: الخصائص الذاتية للجريمة المعلوماتية:

إن الطبيعة الخاصة للجريمة المعلوماتية و ارتباطها بالبيئة الرقمية جعلها تتميز عن الجرائم التقليدية، و تتمثل فيما يلي:

أ. الجريمة المعلوماتية جريمة عابرة للحدود: تعتبر الجريمة المعلوماتية غير مقيدة بالحدود الجغرافية بسبب طبيعة البيئة الرقمية التشبكية التي تلغي الحواجز بين الدول، و يمكن أن ترتكب الجريمة في دولة ما بينما تظهر نتائجها في دولة أخرى تبعد آلاف الكيلومترات أو حتى في وقت مختلف "كارتكابها ليلا في دولة بينما تكون نهارا في أخرى"، حيث تشترك في

2/1/ - عبد القادر عميمر، نفس المرجع السابق ، ص20.

3- عبد القادر عميمر، نفس المرجع السابق، ص28.

هذه السمة مع جرائم أخرى كالإرهاب الدولي و تهريب المخدرات لكنها تختلف عنها بعد حاجتها إلى عمليات مادية كالتفتيش أو نقل الأموال.

كما أنها لا تخضع هذه الجريمة لقيود زمنية أو مكانية تقليدية، إذ يمكن تنفيذها في لحظة واحدة عبر أنظمة رقمية دون الحاجة إلى تخطيط مكاني مادي.

ب. سهولة ارتكاب الجريمة المعلوماتية: لا تحتاج الجريمة المعلوماتية جهد عضلي في ارتكابها بل تعتمد عل القدرات الذهنية للجاني، و تحكمه الجيد في الحاسوب و وسائل الاتصال الحديثة، و لا يحتاج الجاني في ارتكابها إلى التنقل و الاستعانة بمركبة لنقل المسروقات، كما أنه لا يحتاج في غالب الأحيان لمساعدة شخص آخر لارتكاب جريمته من أجل الترصد و الحماية بل يمكن للجاني أن يرتكب جريمته وهو يرتشف فنجان قهوة خلف مكتبه و في قاعة مكيفة، كما أنه لا يوجد هناك احتمال لتعرض الجاني لخطر المواجهة و المقاومة من طرف المجني عليه أو من طرف قوات الأمن كما هو الشأن في بعض الجرائم التقليدية.[1]

ج. الجريمة المعلوماتية جريمة ناعمة: توصف الجريمة المعلوماتية بأنها جريمة ناعمة و ذلك لعدم وجود آثار مادية، أي أنها تترك آثارا رقمية غير ملموسة كبيانات معدلة أو اختراقات الكترونية بعكس الجرائم التقليدية التي تترك آثارا مادية كالكسر أو الدم، مما يصعب هذا الأمر جمع الأدلة و إثباتها أمام القضاء، خاصة مع إمكانية تزوير أو حذف البيانات الرقمية بسهولة.

د. سهولة إتلاف الأدلة من قبل الجناة: المعلومات المتداولة عبر الإنترنت على هيئة رموز مخزنة في وسائط تخزين ممغنطة و هي عبارة عن نبضات إلكترونية غير مرئية مما يجعل أمر طمس و محو الدليل سهل، و يتم محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المتخصصة لذلك، و ما أن يحس الجاني بأن أمره سينكشف حتى يبادر

1- عميمر عبد القادر، نفس المرجع السابق، ص 29.

بإلغاء هذه الأوامر أو وضع كلمة مرور أو تشفير المعلومات لمنع إيجاد أي دليل ضده مما يجعل كشف الجريمة و تحديد مرتكبها أمرا في غاية الصعوبة.[1]

هـ. جرائم تقنية المعلومات من الجرائم الجاذبة للاستثمار: حيث يلجأ الجناة لارتكابها لغرض غسل الأموال و توظيف الكثير منها في تطوير تقنيات و أساليب الدخول إلى الشبكات و السطو على البنوك و غيرها.[2]

2. خصائص الجريمة المعلوماتية المستمدة من أساليب ارتكابها:

تتميز الجرائم المعلوماتية بأساليب ارتكاب غير تقليدية، تعكس الطبيعة اللامادية للبيئة الرقمية التي تنفذ فيها، فبدلا من الاعتماد على أدوات مادية "كالأسلحة أو الأدوات الحادة"، حيث يستغل الجناة وسائل تكنولوجية متطورة تتناسب مع طبيعة المعلومات الإلكترونية غير المرئية، تتمثل في:

أ. الوسائل المساعدة في ارتكاب الجرائم المعلوماتية:

يقوم المجرم المعلوماتي باستغلال بعض الوسائل التكنولوجية من أجل ارتكاب جريمته سواء ارتكبت بطريقة فردية أو عن طريق مجموعة من الأفراد، و تستخدم هذه الوسائل بغرض الاتصال و التحضير و تنفيذ الجريمة،[3] و سيتم التطرق إلى بعضها:

البريد الإلكتروني e. mail: يستخدم البريد الإلكتروني بشكل رئيسي كوسيلة قانونية لتبادل المعلومات ، نظرا لسرعته و قدرته على اختصار المسافات، إلا أنه أصبح أداة رئيسية لارتكاب جرائم المعلوماتية مثل : (التهديد الإلكتروني و الابتزاز) أو الاحتيال المعلوماتي و ذلك عن طريق تزييف هوية المؤسسات لسرقة البيانات الحساسة.

1 - أ.د علوي علي أحمد الشارفي، الوجيز في جرائم تقنية المعلومات، إصدار المركز الديمقراطي العربي للدراسات السياسية و الإستراتجية و الاقتصادية، ط1، السنة 2024، ص 42.

2 - أ.د علوي علي أحمد الشارفي، ص 44.

3- عميمر عبد القادر، نفس المرجع السابق، ص 30.

المواقع على الانترنت: المواقع الالكترونية أو صفحات الويب و هي عبارة عن معلومات مخزنة بشكل صفحات، حيث استغلها المجرمون المعلوماتيون عن طريق إنشاء و تصميم مواقع على شبكة الإنترنت بغرض الإعداد لجرائمهم، كما تقوم بعض المواقع على شبكة الإنترنت بالمساهمة في تسهيل ارتكاب الجرائم المعلوماتية عن طريق تقديم معلومات تتعلق بكيفية اختراق و تدمير المواقع.[1]

منتديات المناقشة: منتديات المناقشة الإلكترونية هي إحدى البرمجيات الاجتماعية التي تسمح للمستخدمين بإرسال موضوعات للأعضاء لقراءتها و التعليق عليها إما بطريقة خطية متعاقبة، أو بطريقة خطية متداخلة و يتضمن المنتدى الواحد أحيانا أبوابا مختلفة يتخصص كل منها في موضوع معين، و من ثم فإن نطاق المواضيع المطروحة للنقاش واسع و الأعضاء غير مضطرين للاتصال بالإنترنت في الوقت نفسه، و تنقسم المنتديات إلى منتديات عامة تسمح للزوار بالمشاركة في التعليق، و منتديات خاصة لا يمكن المشاركة فيها إلا عن طريق تسجيل عضوية.[2]

2. أساليب ارتكاب الجريمة:

تتنوع أساليب ارتكاب الجريمة المعلوماتية بشكل كبير حيث تظهر أساليب جديدة مع تطور التقنيات الرقمية و وسائل الاتصال، مما يجعل مواكبتها صعبة في بعض الأحيان، فبعض هذه الأساليب معروفة وشائعة مثل الاختراق، بينما توجد أساليب أخرى كثر تعقيدا يصعب توقعها أو اكتشافها إلا بعد حدوثها عدة مرات كالهجمات الإلكترونية المبرمجة ، ونظرا لتعدد الأساليب نذكر بعضها:

1- عميمر عبد القادر، نفس المرجع السابق، ص 32.

2- عميمر عبد القادر، نفس المرجع السابق، ص 32.

- **التحكم في المنظومة المعلوماتية عن بعد:** تعد "شبكة الشبح" من الأساليب الإجرامية التي يستعملها المجرمون المعلوماتيون في ارتكاب جرائمهم، و هذه التقنية تعتمد على شبكة من الحواسيب المصابة بالفيروسات التي تمكن المجرمين من التحكم عن بعد في الأنظمة المعلوماتية، و يستخدم هذا الأسلوب للتجسس و سرقة البيانات الشخصية أو إرسال رسائل مزعجة "Spam" ، مما يجعل الأنظمة القانونية تواجه صعوبات كبيرة في إثبات هذه الجرائم بسبب طبيعتها غير ملموسة و تعقيداتها التقنية، و يوضح ذلك من خلال حالة Jesse Mc Grou في الولايات المتحدة من ولاية تكساس الذي اخترق أنظمة المستشفى في مدينة دالاس عام 2009 و قام بتعديل بيانات المرضى و تهديد الكوادر الطبية من خلال نشر فيديو على التطبيق الأحمر" يوتيوب" يخبرهم من خلاله أنه سوف يقوم يوم الرابع من شهر جويلية من نفس السنة بالتحكم في النظام الهوائي لغرف العمليات، و هي النقطة التي أوقعت به و تم اعتقاله في نفس السنة"2009 ".[1]

- **الاختراق:** هو أحد أساليب الجرائم المعلوماتية، و يتمثل في الدخول غير مصرح به إلى أنظمة الحواسيب أو الشبكات أو الحسابات الإلكترونية عبر استغلال الثغرات الأمنية أو استخدام تقنيات متقدمة مثل البرامج الضارة (Malware)، أو هجمات التصيد (Phishingattacks)، أو هجمات القوة الغاشمة(Brute Force)، يهدف المخترقون عادة إلى سرقة البيانات الحساسة كالمعلومات الشخصية، أو تعطيل الخدمات الإلكترونية و تدمير البنى التحتية الرقمية للشركات أو المؤسسات الحكومية، نذكر مثلا على ذلك:

- **خرق بيانات فندق ماريوت(MARRIOTT):**تعرضت مجموعة فنادق ماريوت لاختراقات أمنية في نوفمبر 2018، تم اختراق بيانات حوالي 500 مليون نزيل، مما كشف عن معلومات حساسة مثل الأسماء، عناوين البريد الإلكتروني، و أرقام جوزات السفر نتج عن الخرق غرامة قدرها123 مليون دولار من الاتحاد الأوروبي و تسوية بقيمة 25 مليون دولار مع

1- عميمر عبد القادر، نفس المرجع السابق، ص 34.

العملاء ، مما أدى إلى تضرر سمعتها بشدة كما شهدت انخفاضا كبيرا في أسعار الأسهم بعد الإعلان عن هذا الاختراق الكبير.[1]

– **نشر الفيروسات:** تعد الفيروسات من أبرز الآليات التي تستخدم في ارتكاب الجريمة المعلوماتية، حيث تمثل الفيروسات أدوات خبيثة تصمم لتعطيل عملا لأجهزة وإتلاف الملفات وكذا التجسس على المستخدمين دون علمهم، وتكمن خطورتها في قدرتها على الانتقال بين الحواسيب والتكاثر والانتشار دون تدخل بشري مباشر، فهو برنامج غير مرئي تحتاج عملية الكشف عنه إتباع أساليب علمية، وقد أطلقت عليه هذه التسمية لتشابه طريقة عمله مع الفيروسات التي تصيب الكائنات الحية، وتنتقل هذه الأخيرة عن طريق الإنترنت التي تعد الوسيلة المثلى لانتقالها من جهاز لآخر ما لم تستخدم أنظمة الحماية[2] نذكر بعض الفيروسات :

ـ **فيروسات الفدية**"**Ransomware**":هي نوع من البرامج الضارة تقوم باختطاف البيانات، حيث يقوم الفيروس بتشفير الملفات الشخصية مثل الصور، المستندات أو الفيديوهات و يجعلها قابلة للفتح دون الحاجة لمفتاح فك الشفرة، مما يحجب الوصول إليها حتى دفع فدية، مثل " فيروس Wannacryانتشر هجوم هذا الفيروس عبر أجهزة الكمبيوتر التي تعمل بنظام تشغيل Microsoft Windows، تمت السيطرة على ملفات المستخدمين و طلب فدية بعملة Bitcoin لإعادتها.[3]

ـ **فيروس حصان طروادة:** هي عبارة عن فيروسات تتنكر في شكل برامج شرعية مثل ملف PDF أو تحديث نظام لخداع الضحية لتنزيلها.

3: خصائص الجريمة المعلوماتية المستمدة من سمات مرتكبيها:

تتميز الجريمة المعلوماتية ليس فقط بوسائل ارتكابها، بل أيضا بخصائص مرتكبيها الذي يطلق عليهم المجرمون المعلوماتيون، و الذين ينتمون إلى فئة خاصة مشابهة "لذوي الياقات البيضاء"،

1- الموضوع منشور على صفحة عرب 48 / 06/03/2023https://www.arab48.com ، تم الإطلاع عليها بتاريخ 2025/05/08 على الساعة 00:46.

2- عميمر عبد القادر، نفس المرجع السابق، ص 41.

3 - الموضوع المنشور على صفحة Kasperskyhttps://me.kaspersky.com/ تم الاطلاع عليه بتاريخ 2025/05/18 بتوقيت 23:11.

و من بين الباحثين الذين اهتموا بهذا الموضوع Donn Parkerالذي توصل بعد الدراسات التي قام بها إلى أن المجرم المعلوماتي يتميز بعدة صفات هي المهارة، المعرفة، الوسائل، السلطة، الباعث، و رمز لها ب"S.K.R.A.M"[1]

أولا: سمات المجرم المعلوماتي: برزت شخصية المجرم المعلوماتي كواحدة من أكثر الظواهر تعقيدا حيث تجتمع فيه سمات فريدة تميزه عن المجرم التقليدي، فهو ليس مجرد مخترق بارع للأنظمة أو مبرمج ماهر فحسب إنما هو مزيج من الذكاء التقني و المهارة في التخفي خلف شاشات التشفير و الشبكات المظلمة، ومن سماته نذكر:

- ✓ المجرم المعلوماتي متحكم في تكنولوجيا الإعلام و الاتصال
- ✓ المجرم المعلوماتي متخصص
- ✓ المجرم المعلوماتي يتميز بالذكاء
- ✓ المجرم المعلوماتي انتكاسي
- ✓ المجرم المعلوماتي مرن و سهل التكيف
- ✓ المجرم المعلوماتي يتميز بمهارات الهندسة الاجتماعية

ثانيا: أصناف مرتكبي الجريمة المعلوماتية: بما أن المجرم المعلوماتي إنسان محترف فإنه يتمتع بذكاء كبير، وعليه يمكن تصنيف جناة الجريمة المعلوماتية إلى عدة أصناف[2] و هي:

1) القراصنة "Hackers": يشير هذا المصطلح إلى الشخص الذي يمتلك مهارات تقنية متقدمة في مجال الحاسوب و أمن المعلومات ، ويكون قادرا على اختراق الأنظمة و تحليلها و من خصائصه عدم وجود نية أو قصد لإتلاف المعلومات أو تخريب أنظمة الحساب وشبكات الاتصال، يتمثل هدفهم في الاستكشاف والبحث عن الجديد في هذا العالم

1 - عميمر عبد القادر، نفس المرجع السابق، ص 44.

2- بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق و العلوم الإنسانية، المجلد 14 العدد 04، جامعة قسنطينة 2 نشر بتاريخ 2021/11/12، ص 52.

الخيالي.[1] وهناك عدة أنواع من القراصنة تختلف هذه الأنواع بناءا على أهدافهم و أخلاقهم منهم:

❖ **أصحاب القبعات البيضWhite Hat Hackers":** يعتبرون الهاكرز الأخلاقيين، حيث يستخدمون مهاراتهم لاكتشاف الثغرات الأمنية في الأنظمة و إصلاحها.

❖ **أصحاب القبعات السود"Black Hat Hackers":** و يسمون أيضا بالكراكر"Crackers" و دورهم سلبي و يستغلون مهارتهم و نواياهم لأغراض إجرامية مثل سرقة البيانات أو تعطيل الخدمات الإلكترونية.[2]

❖ **أصحاب القبعات الرمادية"Grey Hat Hackers":**هم فئة تقع أفعالهم في المنطقة الرمادية بين الأخلاقي و غير القانوني، حيث يجمعون بين سمات القبعة البيضاء و القبعة السوداء فهم لا يلتزمون تماما بالقوانين.[3]

2) المخادعون"مهندسي،الهندسة،الاجتماعية: هم أفراد يستغلون الثقة البشرية و الخصائص النفسية للأشخاص من أجل الوصول إلى معلومات أو أنظمة محمية دون الحاجة إلى استخدام تقنيات اختراق تقليدية ، يعتمدون على التلاعب النفسي بدلا من الأدوات التقنية للاختراق من أشهرهم KEVIN D.MITNICK.[4]

3) أطفال الهاكر"Script Kidders": ينتشر هذا النوع على مواقع التواصل الاجتماعي و هم يبحثون عن الشهرة عن طريق اختراق الأجهزة و المواقع الضعيفة بشكل عشوائي و من أهم صفاتهم أنهم لا يملكون أية معرفة علمية فهم يجيدون استخدام بعض البرامج و الأدوات و استغلال الثغرات الجاهزة التي برمجها الهاكرز الحقيقيين و لكنهم ليسوا

1- بوهرين فتيحة، نفس المرجع السابق، ص52.

2- عميمر عبد القادر، نفس المرجع السابق، ص48.

3- الموضوع المنشور على صفحة Kasperskyhttps://me.kaspersky.com/ تم الاطلاع عليه بتاريخ 2025/05/21 بتوقيت 01:39.

4- الموضوع المنشور على صفحة Kasperskyhttps://me.kaspersky.com/ تم الاطلاع عليه بتاريخ 2025/05/21 بتوقيت02:46.

قادرين على برمجة أدواتهم و اكتشاف ثغراتهم الخاصة و ليسوا قادرين على تطويلا طرق و أساليب جديدة عبارة عن مستخدمين فقط.[1]

الفرع الثاني: دوافع ارتكاب الجريمة المعلوماتية و طبيعتها القانونية

أولا: دوافع ارتكاب الجريمة المعلوماتية

للجريمة المعلوماتية عدة دوافع لارتكابها فبعضها يرجع إلى دافع شخصي ومنها مايرجع إلى دافع خارجي ومنها ما يكون خاص، و كل هذه الدوافع يكون مصدرها الرغبة الإجرامية.[2]

1 الدوافع الداخلية الشخصية:

الدافع المادي: أي الرغبة في الحصول على مكاسب مادية سريعة و كبيرة مثل سرقة الأموال عبر اختراق الحسابات المصرفية أو ابتزاز الضحايا عبر برامج الفدية، ويعتبر هذا الدافع الأكثر شيوعا خاصة مع سهولة تحويل الأموال عبر الحدود باستخدام العملات المشفرة.[3]

دافع الحصول على معلومات جديدة: هناك من يرتكب جرائم الحاسوب بغية الحصول على الجديد من المعلومات، و هؤلاء الأشخاص يقومون بالبحث و اكتشاف الأنظمة و العمل من خلال الجماعة و تعليم بعضهم البعض و يفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار داخل الأنظمة.[4]

دافع الاستيلاء على المعلومات: الإقدام على هذا الجرم بواسطة تقنية المعلومات بهدف الحصول على المعلومة ذاتها و الاستيلاء عليها و التصرف فيها يتمثل ذلك في الحصول على المعلومة المحفوظة في الحاسب الآلي أو المنقولة أو تغييرها أو حذفها، و يختلف الدافع لهذا التصرف فقد يكون دافع تنافسي أو سببه الابتزاز.[5]

1- عميمر عبد القادر، نفس المرجع السابق،ص50.

2- بوهرين فتيحة، نفس المرجع السابق، ص54.

3- الموضوع المنشور على صفحة MediaCentr .gov.ae rakpolice //https/ تم الإطلاع عليه بتاريخ 2025/05/21 بتوقيت 04:18.

4- صابر بحري/ منى خرموش،أهم السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكولوجية الانحراف"مجلة دولية نصف سنوية"، المجلد 06،العدد01، السنة2021،ص49.

5- صابر بحري/ منى خرموش، نفس المرجع السابق،ص50.

أ. دافع قهر النظام المعلوماتي: قد يكون الدافع إلى ارتكاب الجرائم الإلكترونية هو الرغبة في قهر الأنظمة الإلكترونية و التغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم و إثبات الذات و تحقيق انتصار شخصي.[1]

ب. دافع الانتقام: يعد هذا الدافعمن أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك لأنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها و غالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية، فكثيرا ما يلجأ المجرم الإلكتروني إلى ارتكاب جريمته انتقاما من الضحايا.[2]

ج. دافع الصورة الذهنية: غالبا ما تكون الصورة الذهنية للمجرم المعلوماتي هي صورة البطل و الذكي الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم و مستوى ارتقائهم خلال فعلهم للجرم، و يعتبر إتيانه هذا الفعل بمثابة إنجاز ذاتي حققه و هو عمل خارق أنجزه يستدعي عليه الثناء.[3]

2 الدوافع الخارجية: تتمثل هذه الدوافع في الأسباب و العوامل التي تكون خارج ذات الفرد و لا تتعلق بشخصيته، و هي:

1.2 إلحاق الضرر بالآخرين: إن الباعث على ارتكاب الجريمة الإلكترونية قد يكون بسبب إلحاق الضرر المادي و المعنوي برب العمل انتقاما منه لأسباب شخصية تتعلق بطبيعة العلاقة التي تربط صاحب العمل بمرتكب الجريمة الإلكترونية، و لأن ارتكاب

6- صابر بحري/ منى خرموش، نفس المرجع السابق،ص52.

2- صابر بحري/ منى خرموش، نفس المرجع السابق،ص52.

4/3/2/ 5- صابر بحري/ منى خرموش، نفس المرجع السابق، ص-ص 56,54.

الجريمة يكبد المؤسسة أو صاحب العمل خسائر مادية مما يجعل مرتكب الجريمة فخورا بما فعل بدافع الانتقام.[1]

2.2 دافع التعاون و التواطؤ: غالبا ما يحدث من متخصص في الأنظمة المعلوماتية أين يقوم بالجانب الفني من المشروع الإجرامي و آخر من المحيط أو خارج مؤسسة المجني عليها يقوم بتغطية عمليات التلاعب و تحويل المكاسب المادية و عادة ما يمارسون التلصص على الأنظمة و تبادل المعلومات، و التعاون و التواطؤ يكون لإشباع دافع نفسي لدي مرتكب الجريمة الإلكترونية.[2]

3.2 الضغوط العامة: إن الأوضاع الاجتماعية و الاقتصادية المعقدة مثل الفقر و البطالة تشكل ضغوطا شديدة على الأفراد و خصوصا الشباب، مما يولد لديهم إحباطا و رغبة في البحث عن حلول سريعة لمشكلاتهم، و نتيجة لذلك يلجأ بعض من يمتلكون مهارات تقنية إلى ارتكاب الجريمة الإلكترونية كوسيلة لمواجهة التحديات و تلبية احتياجاتهم المادية و المعنوية.[3]

4.2 العولمة: أدت العولمة و انتشار الفضاء الإلكتروني إلى ظهور أشكال جديدة من الجرائم تتميز باختلاف سلوك الأفراد مقارنة بالواقع المادي، حيث يقدم البعض على ارتكاب جرائم إلكترونية بسبب إمكانية إخفاء هويتهم ، و كما ساهمت التكنولوجيا الحديثة في تقريب العالم مما سمح للجريمة الإلكترونية بتجاوز الحدود الجغرافية حيث يمكن للمجرم المعلوماتي تنفيذ أفعاله من أي مكان في العالم بدوافع متنوعة كالانتقام.[4]

ثانيا: الطبيعة القانونية للجريمة المعلوماتية

1-2 صابر بحري/ منى خرموش، نفس المرجع السابق، ص-ص54-56

3-4-5 حمزة خضري/ عشعاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية و السياسية، جامعة محمد بوضياف، المسيلة ،المجلد 07 عدد02، نشر بتاريخ 2020/06/05، ص-ص 173,172.

تتخذ جرام تقنية المعلومات من الفضاء الافتراضي مسرحا، و أدى ذلك إلى بروز أشكال جديدة من الإجراءات، مما دفع بالتشريعات الجنائية بالنص على معاقبة هذا النوع من الجرائم، لتوفير الحماية الجزائية للأنظمة المعلوماتية و أساليب المعالجة الآلية للمعطيات ، فقام المشرع الجزائري بتعديل قانون العقوبات بموجب قانون 04-15 باسم المساس بأنظمة المعالجة الآلية للمعطيات.[1]

من خلال هذا التعديل قام المشرع بحماية هذه المعطيات و ذلك بإصدار القانون رقم 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، و ما يلاحظ في هذا الشأن أن المشرع الجزائري لم يستقر على تسمية واحدة و إنما اعتمد على عدة تسميات مختلفة بين قانون العقوبات و القوانين المكملة في المجال الجنائي فسماها جريمة المساس بأنظمة المعالجة الآلية للمعطيات في قانون 04-15، في حين أعطاها تسمية الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال في قانون 04-09، و رغم هذا الاختلاف فان هاتين التسميتين و غيرها من التسميات الأخرى تصب في هدف واحد و هو مجابهة الجريمة الالكترونية.[2]

أما عن محل الجريمة المعلوماتية فيتميز عن محل الجريمة التقليدية، فمحل الجريمة الأولى هو المال المعلوماتي تمييزا لماليته المغايرة للمال التقليدي في الجريمة الثانية بكل مكوناته، فالجريمة المعلوماتية تشمل كل من أفعال السرقة أو التغيير أو حذف المعلومات مثل النشاط الإجرام الذي يستهدف اختراق البريد الكتروني و العبث بمحتوياته، و الذي يحمل في طياته انتهاك الخصوصية و الحقوق الملكية و الفكرية و أنماط جرمية أخرى.[3]

ثالثا: أركان الجريمة المعلوماتية

- **الركن الشرعي للجريمة المعلوماتية:** انطلاقا من مبدأ الشرعية وفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على:" **لا جريمة و لا عقوبة أو تدابير أمن بغير قانون"**، حيث جرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية و نص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر بعنوان" المساس بأنظمة المعالجة الآلية للمعطيات" من المواد 394 مكرر إلى 394 مكرر8 منقع.[4]

في حين جاء قانون 09-04 متضمنا بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية، من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية، و لجأ المشرع إلى النص على مثل هذه الجرائم و جعلها في نطاق مبدأ الشرعية.[5]

2/4- حمزة خضري/ عشعاش حمزة، المرجع السابق، ص173.

1-2- حمزة خضري/ عشعاش حمزة، المرجع السابق، ص174.

- **الركن المادي للجريمة المعلوماتية:** يعتبر الركن المادي للجريمة هو المظهر الخارجي لها و كيانها المادي الظاهري وهو الماديات المحسوسة في العالم الخارجي كما حددتها نصوص التجريم، إلا أن الركن المادي للجريمة المعلوماتية يختلف نوعا ما عن الجرائم التقليدية في كونه يقوم على صور في فعل الاعتداء، و المتمثلة في:

أولا: الدخول أو البقاء غير مشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك: حسب ما نصت عليه المادة 394مكرر من ق ع على أن الدخول أو البقاء غير المشروع في نظام المعالجة الآلية أو الشروع في ذلك يشكل فعلا إجراميا و لهذا الفعل صورتين:

✓ **الصورة البسيطة:** يتمثل النشاط الإجرامي في هذه الصورة في الأفعال الآتية:

أ - فعل الدخول: يتحقق هذا الفعل بمجرد الوصول إلى المعلومات المخزنة داخل النظام و دون علم و رضا صاحبه، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن بنفقات.

ب - البقاء: معنى البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له حق في السيطرة على هذا النظام، أو بتجاوز المدة المسموح له بالبقاء فيها، أو عدم الانسحاب فورا و قطع وجوده في نظام البيانات.

✓ **الصورة المشددة:** نصت المادة 394 مكرر في الفقرتين الثانية و الثالثة من ق ع على ظروف تشديد عقوبة فعل الدخول و البقاء غير المشروع عندما ينتج عن هذين الفعلين إما المحو أو تحويل المعطيات التي يحتويها النظام، و إما عدم صلاحية النظام لأداء و وظائفه من خلال تخريب نظام اشتعال لمنظومة.

ثانيا: إدخال المعطيات بطريق الغش: يقصد بفعل الإدخال حسب المادة 394 مكرر 1 من ق ع إضافة معطيات جديدة إلى نظام المعالجة الآلية أو التعديل من معلومات داخله كان يتضمنه مسبقا فغير فيها، و مثال ذلك حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة و التزوير.

- **الركن المعنوي:** يتخذ هذا الركن في أغلب الجرائم بصفة عامة صورة القصد الجنائي، و الذي يتحقق بتوافر إرادة العمل غير شرعي لدى الجاني مع علمه بأن القانون يجرمه، و نفس الأمر ينطبق على الجريمة المعلوماتية التي يقوم ركنها المعنوي على توافر الإرادة الإجرامية لدى الفاعل، و هذا يظهر من خلال من خلال استعمال المشرع الجزائي لعبارة" الغش" و" العمد" و" الإعداد للجريمة" في المواد 394 مكررو 394 مكرر1 و 2 و 5 من ق ع، و هذا إن دل فإنما يدل على أن الجريمة المعلوماتية جريمة عمدية بامتياز و لا يفترض فيها عنصر الخطأ.[1]

1. حمزة خضري/ عشعاش حمزة، المرجع السابق، ص174.

المبحث الثاني: الأدلة الجنائية الرقمية

في عالم تسيطر عليه البتات الرقمية و البيانات اللامرئية، تتحول كل نقرة على لوحة المفاتيح أو رسالة مرسلة عبر الشبكة أو حتى إشارة من جهاز ذكي، إلى أثر رقمي قد يحمل في طياته أدلة حاسمة لفك ألغاز الجرائم، حيث هذه الأخيرة لم تعد ترتكب باليد و سلاح بل صارت تنفذ عبر شفرات خبيثة و مساحات افتراضية لا ترى، مما جعل الأدلة الجنائية الرقمية عصب التحقيقات حديثة كما أنها أصبحت جسرا بين الواقع المادي و العالم الافتراضي المعقد، و هذا ما سيتم التطرق إليه في هذا المبحث من خلال مطلبيه حيث سيتناول المطلب الأول مفهوم الدليل الرقمي و أهميته في الجريمة المعلوماتية، أما المطلب الثاني سيتحدث عن الصعوبات المتعلقة بالوصول إلى الدليل الرقمي.

المطلب الأول: مفهوم الأدلة الجنائية الرقمية و أهميتها في الجريمة المعلوماتية:

تعددت التعريفات الخاصة بالدليل الرقمي وتنوعت، حتى وإن كانت تصب في نقطة واحدة تتعلق بفضاء الرقمي للدليل الحديث، حيث تتمثل هذه التعريفات في:

الفرع الأول: تعريف الدليل الجنائي الرقمي

أولا: التعريف اللغوي:

الدليل لغة: يعرف بأنه الحجة أو البرهان أو أنه المرشد و ما يستدل به، و الدليل الدال و الجمع أدلة و يعني به تأكيد الحق بالبينة و هي الدليل أو الحجة أو البرهان.[1]

ثانيا: التعريف الاصطلاحي:

الدليل الرقمي عبارة ذبذبات أو نبضات الكترونية، يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات من أجهزة الحاسب الآلي و ملحقاته أو من خلال شبكات الإنترنت أو جهاز آخر له خاصية معالجة أو تخزين المعلومات و تشكل هذه المعلومات و البيانات دليلا جنائيا يمكن الاعتماد عليه في مرحلة التحقيق و المحاكمة. [2]

1د. بوقادوم– يحياوي صليحة، الإطار المفاهيمي للأدلة الجنائية الرقمية مداخلة في ملتقى وطني بعنوان: إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال –الصعوبات والتحديات- كلية الحقوق،جامعة الجزائر 1(بن يوسف بن خدة)، المنعقد يوم 2025/04/17، ص3.

2 د. بن مالك أحمد/ د. الخال إبراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية ـ المركز الجامعي علي كافي تندوف، المجلد05، العدد01، نشر2021/04/10، ص 108.

كما يعرف أيضا بأنه ذلك الدليل الذي يتضمن بيانات إلكترونية مخزنة بالحاسب الآلي و لها وجود في الوسط الافتراضي و التي من خلالها يتم الكشف عن الجريمة و إثبات العلاقة بين الجريمة و فاعلها.[1]

ثالثا: خصائص الدليل الرقمي: يتميز الدليل الرقمي بعدة خصائص تميزه عن باقي الأدلة و تتمثل هذه الأخيرة في :

1. الدليل الرقمي غير مرئي: أي يتكون من بيانات و معلومات ذات هيئة إلكترونية غير ملموسة، بل يتم إدراكها باستخدام أجهزة و معدات الحاسب الآلي"Hardware" و نظم برمجيات الحاسوب"Software".[2]

2.الدليل الرقمي علمي و تقني: الدليل الرقمي دليل علمي و تقني حديث، يتكون من بيانات و معلومات إلكترونية غير ملموسة تعالج عبر أجهزة الحاسوب والبرامج الحاسوبية، مما يجعله يتميز بطابعه الديناميكي وسرعته الفائقة وهذا لاعتماده بشكل أساسي على التقنيات المتطورة في البيئة الافتراضية.[3]

3.الدليل الرقمي ذو طبيعة متطورة: خاصية التطور التي يتمتع بها الدليل الرقمي ناتجة عن تزايد استخدام تقنية المعلومات الرقمية، بعد أن أصبحت أجهزة الحاسب الآلي وشبكة الإنترنت تشكل مستودعا هاما للمعلومات والبيانات الرقمية.[4]

4.الدليل العلمي ذو طبيعة ثنائية: هو اختزال البيانات أو المعلومات كالنصوص أو الصور أو أي معلومة أخرى إلى رموز ثنائية، و هذه الرموز الثنائية تتكون من سلسلة من رقم صفر(0) و رقم (1)، 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.[5]

1- عيدة بلعابد،الدليل الرقمي بين حتمية الإثبات الجنائي و الحق في الخصوصية المعلوماتية، مجلة آفاق جامعة سعيدة، المجلد11، العدد01، سنة 2019، ص138.

6/2- بن فريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي"دراسة مقارنة"، كلية الحقوق و العلوم السياسية جامعة بجاية، ص 287.

3- عيدة بلعابد، نفس المرجع السابق،ص 138.

4- د. بن مالك أحمد/ د. الخال إبراهيم، نفس المرجع السابق،ص 106.

5- أوساسي فؤاد، دور الدليل لرقمي في الإثبات الجنائي، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية ، جامعة زيان عاشور، الجلفة،ص 10.

5.الدليل الرقمي قابل للنسخ: حيث أن هذه الخاصية تقلل أو تعدم مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من الفقد أو التلف، عن طريق نسخ طبق الأصل من الدليل.[1]

6.صعوبة إتلاف الدليل الرقمي: قد يتعرض الدليل الرقمي إلى عملية إتلاف سواء بصفة كلية أو جزئية وهذا من خلال عملية المحو، غير أنه وبالرغم من هذا فإن إتلافه لا يمنع من إعادة استرجاع محتوى الدليل الرقمي من ذاكرة الحاسب الآلي أو بالاستعانة بنسخ منه.[2]

7.الدليل الرقمي له سعة تخزين عالية: يتميز هذا الأخيرة بسعة تخزين عالية حيث يمكن لآلة الفيديو الرقمية تخزين مئات الصور و كذا القرص المضغوط يمكنه تخزين مكتبة صغيرة، كما أن الدليل الرقمي يمكنه رصد معلومات عن الجاني و تحليلها في ذات الوقت حيث يمكنه تسجيل تحركات الفرد و تسجيل عاداته و كذا سلوكياته، و لهذا البحث الجنائي يجد غايته بسهولة أفضل من الدليل المادي التقليدي.[3]

الفرع الثاني: أنواع و تقسيمات الدليل الرقمي

أولا: أنواع الدليل الرقمي: يتخذ الدليل الرقمي عدة أشكال مما يشكل لنا العديد من البيانات و المعلومات المختلفة التي تعد وسيلة في إثبات الجرائم المعلوماتية، حيث يأخذ الدليل الرقمي صورتين أساسيتين تتمثل في:

الأدلة الرقمية التي أعدت لتكون وسيلة إثبات: و التي بدورها تنقسم إلى نوعين:

1) البيانات و المعلومات الناشئة تلقائيا من الحاسب الآلي:

و هي مختلف المعلومات و البيانات الرقمية التي يتم إنشاؤها بواسطة الحاسب الآلي أو أي جهاز آخر و لا يكون للمستخدم دخل في إنشائها، أو السجلات التي تعد من مخرجات الحاسب الآلي.[4]

2) البيانات و المعلومات ذات الطبيعة المختلفة: وهي تلك البيانات و المعلومات التي يتم إنشاء جزء منها بواسطة الحاسب الآلي، و جزء آخر يتم حفظه بالإدخال، و أبرز مثال على ذلك المعلومات و البيانات المدخلة و المعالجة من طرف برنامج Excel.[5]

2- فراحتية خلود، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة ماستر تخصص قانون إعلام الآلي و إنترنت، كلية الحقوق و العلوم السياسية جامعة محمد البشير الإبراهيمي، برج بوعريريج، ص 13.

5/4/3- فراحتية خلود، نفس المرجع السابق، ص- ص 15,14.

2/4- عيدة بلعابد، نفس المرجع السابق،ص 138

5/4/3- أحمد فؤاد محمد سليمان، أهمية الدليل الرقمي في الإثبات الجنائي لجرائم الإيذاء الإلكتروني، مجلة جامعة أسوان للعلوم الإنسانية، كلية الحقوق، المجلد 4 العدد3 سنة 2024، ص- ص 60,59.

وعليه تكمن أهمية كلا النوعين في أنهما أعدا سلفا بغرض جعلهما وسيلة لإثبات بعض الوقائع التي تتضمنها، لهذا يتم حفظ هذه المعلومات و البيانات للاحتجاج بها كما يسهل الحصول عليها عند الحاجة.[1]

الأدلة الرقمية التي لم تعد لتكون وسيلة إثبات: و هي الأدلة غير إرادية الآثار التي يتركها المستخدم دون قصد عد استعماله للحاسب الآلي أو شبكة الإنترنت بحث تشمل الرسائل المرسلة منه أو الرسائل التي يستقبلها، و يطلق على هذا النوع من الأدلة اسم" البصمة الرقمية أو الآثار المعلوماتية الرقمية" مثل الرسائل المرسلة و المستقبلة و ملفات الولوج التي تسجل تواريخ و أنشطة التحميل .[2]

تعد هذه الأدلة ذات أهمية في الكشف عن الجرائم ومرتكبيها و ذلك لاحتوائها على بصمات رقمية و معلومات تفصيلية، كما يمكن حفظها و استعادتها حتى بعد فترات زمنية طويلة.

ثانيا: تصنيفات الدليل الرقمي: لم يتطرق أغلب فقهاء القانون الجنائي إلى دراسة شاملة و دقيقة للأدلة الجنائية الرقمية نظر لحداثة هذا النوع من الأدلة و بيئته التي تمتاز بالتطور المستمر[3]، حيث صنف الدليل الرقمي إلى أربعة تصنيفات، تتمثل في:

1.البرامج والتطبيقات: يعرف البرنامج بأنه : عبارة عن تعليمات مكتوبة بلغة معينة وموجهة إلي جهاز تقني معقد يسمي بالنظام المعلوماتي , بغرض الوصول إلى نتيجة معينة[4]، و ينقسم إلى نوعين:

- ✓ **برنامج التشغيل:** وهي مجموعة من الأوامر والتعليمات التي تتم تغذيتها للحاسوب وتساعد في تشغيله مثل برنامج التشغيلWindowsو من مهامه الرئيسية السيطرة والتحكم على مكونات الحاسوب ، وذلك بالربط بين وحدة التشغيل المركزية وبين باقي مكونات الحاسوب.[5]
- ✓ **البرامج التطبيقية:** وهي البرامج التي تصمم للقيام بمهام محددة داخل نظام الحاسوب، ومن أمثلتها برنامج Explorer Interneوهو لمستعرض الرئيس لصفحات الويب في نظام التشغيلWindows.[6]

2.الأدلة المرئية: وهي عبارة عن تجسيد للحقائق المرئية حول الجريمة، وتعرف الصور الرقمية بأنها لقطات إلكترونية مأخوذة من مشهد أو منظر تم مسحها ضوئيا من وثائق مثل

5- أحمد فؤاد محمد سليمان، المرجع السابق ص60.

2-3-4أحمد فؤاد محمد سليمان، المرجع السابق ص61.

الصورة الضوئية والمخطوطات والنصوص المطبوعة، وتتكون الصور الرقمية من عدة أشكال أو عناصر والتي يطلق عليها بيكسل" Pixel "وكل بيكسل مخصص لقيمة أو وظيفة محددة" أبيض، أسود ، الخ "والتي يتم تمثيلها في كود ثنائي " 0-1" وتخزن هذه الأرقام الثابتة التي يطلق عليها بتات" bits "لكل بيكسل في سلسلة متعاقبة بواسطة الحاسب الآلي، وتترجم وتقرأ البتات عن طريق الحاسب لإظهارها في شكل صور[1]، و قد أشار إليها المشرع الجزائري في المادة65 مكرر5 من ق06-22.

3.الأدلة الصوتية: تشمل هذه الأدلة مختلف التسجيلات الصوتية التي يتم ضبطها وتخزينها بواسطة الوسائل الإلكترونية، كالمحادثات الصوتية على غرف الدردشة عبر الإنترنت، أو عبر تطبيقات مواقع التواصل الاجتماعي Messenger , Twiter, Vibre, Skypeأو المكالمات الهاتفية، وتشكل التسجيلات الصوتية التي تكون ناتجة عن إجراء المراقبة الإلكترونية للمحادثات التي تتم عن طريق الإنترنت أو الهاتف المحمول دليلا على ارتكاب الجريمة.[2]

4.الأدلة المكتوبة : وتعد النصوص الرقمية أكثر أشكال الدليل الرقمي أهمية في مجال الإثبات، ومن تطبيقاتها ما يعرف بالمستند أو المحرر الإلكتروني، والتوقيع الإلكتروني، ورسائل البريد الإلكتروني، كما تشمل الكتابة الإلكترونية " حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة، وتعطي دلالة قابلة للإدراك " التي يقوم الأشخاص بإدخالها إلى النظام المعلوماتي والتي تتصل بالأعمال والمشاريع التي يمارسونها وأيضا تشمل الكتابة الإلكترونية البيانات المكتوبة التي ينشئها الكمبيوتر والتي تكون ناتجة عن استخدام بعض التطبيقات أو البرامج.[3]

المطلب الثاني: أهمية الدليل الرقمي و صعوبة استخلاصه

الفرع الأول: أهمية الدليل الرقمي

تعتبر و سائل الإثبات بشكل عام من أهم المسائل التي يجب عل المشرع الانتباه لها، و ذلك لما يترتب عليها من إثبات الحقوق والالتزامات[4]، كما أن الدليل الرقمي يمثل الخط الفاصل في إثبات الجريمة المعلوماتية و تكمن أهميته في:

يعد الدليل الرقمي أحد أبرز مظاهر الاعتماد على العلوم الحديثة فالأدلة الرقمية المستخرجة من الحواسيب أو الخوادم الإلكترونية لا يتم التعامل معها مباشرة، و إنما تخضع

1- سلطان سليمان الجداني، ماهية الدليل الرقمي دراسة مقارنة، مجلة International Journal Of Law and PoliticsStudies،ص 57.

2-3-4فراحتية خلود، نفس المرجع السابق، ص33.

لعمليات فنية و تحليلية دقيقة كاسترجاع البيانات، و فحص التوقعات الرقمية، و غيرها من الوسائل التقنية التي تتطلب خبرة علمية متخصصة.
تتمثل أهميته العلمية في كونه موضوعيا إلى حد كبير، أي أنه يمنح التحقيق الجنائي بعدا علميا رصينا، متى رعيت في التعامل معه شروط النزاهة التقنية.

فالبيانات التي يتم التعامل معها و جمعها من الحواسيب أو الهواتف أو الخوادم الإلكترونية تكون غالبا غير مرئية للمستخدم العادي، و لا يمكن الوصول إليها إلا باستعمال أدوات علمية متخصصة، و هنا تظهر لنا قيمته التقنية.
يتميز هذا النوع من الأدلة بصفته العلمية، حيث لا يعتمد فقط على الإدراك الحسي أو شهادة الأشخاص، بل يقوم أساسا على تقنيات متطورة يشرف عليها خبراء متخصصون.
تتجلى قيمته العلمية في كونه لا يرتكز على مجرد الحواس وشهادة الأشخاص، بل يعتمد على تقنيات متقدمة يديرها خبراء محترفون، و ينفذ ضمن إطار منهجي معين.

الفرع الثاني: صعوبات استخلاص الدليل الرقمي

تعد الصعوبات المتعلقة بالدليل الرقمي تحدا جوهريا و ذلك بسبب طبيعته المعقدة وهشاشته التقنية، و تتمثل في :

أولا: الصعوبات التي تتعلق بالدليل الرقمي

1- صعوبة رؤية الدليل: تتميز الجريمة المعلوماتية بأنها تتم في العالم الافتراضي و الذي بدوره تكون فيه الأدلة عبارة عن ذبذبات أو نبضات في شكل بيانات أو معلومات رقمية، مما يثير إشكالية جمع و تحليل الدليل الرقمي لعدم إمكانية رؤيته، مما يجب أن تتوفر لدى الفنيين المهارة الكبيرة للتعامل مع هذا النوع من الأدلة.[1]

2- سهولة محو و تدمير الدليل الرقمي: نظرا للسهولة التي تتمي بها هذه العملية و عد استغراقها للوقت الطويل فإنها تعد من بين أكبر التحديات و الصعوبات التي تواجه عملية استخلاص الدليل الرقمي، لأن مرتكبي الجرائم المعلوماتية يتميزون بالذكاء و الفطنة و الإتقان الفني للعمل الذي يقوم به من خلال التلاعب غير المرئي في أنظمة الحاسب الآلي.[2]

3- إعاقة الوصول إلى الدليل الرقمي: يلجأ مرتكبي الجريمة المعلوماتية دائما لابتكار أحدث الوسائل و الأساليب لعرقلة جمع أدلة الإدانة، و من بين هذه الوسائل استخدام تقنية التشفير أو فرض تدابير أمنية لمنع و عرقلة عملية التفتيش والإطلاع عن الأدلة أو ضبطها و ذلك باستخدام كلمة السر.

4- ضخامة البيانات المتعين فحصها: من بين أكبر التحديات و الصعوبات التي تواجه سلطات التحقيق و رجال الضبط لاستخلاص الدليل الرقمي، هو ذلك الكم الكبير و الوفير

1-عكوش حنان، خطوي مسعود، خصوصية الدليل الإلكتروني، مجلة الفكر القانوني و السياسي، المجلد 7العدد 1 سنة 2023، كلية الحقوق و العلوم السياسية، جامعة عمار ثلجي، الأغواط،ص 106.

للمعلومات و البيانات المراد فحصها و تحليلها، لذلك يتعين على المحقق أن تتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات و البيانات المخزنة في جهاز الحاسب الآلي.[1]

ثانيا: الصعوبات التي تتعلق بجهات التحقيق: يجب أن تتوفر مهارات و خبرات خاصة عند استخلاص الدليل الرقمي، زيادة إلى أساسيات و أُصول التحقيق الجنائي، و لكن قد لوحظ نقص في الخبرات التقنية للمحققين و عدم مواكبتهم للتطورات التكنولوجية، مما يعيق جمع الأدلة الرقمية و تحليلها، مما دفع المشرع الجزائري إلى إنشاء مؤسستين متخصصتين عام 2004 **المعهد الوطني للأدلة الجنائية و علوم الإجرام تحت وصاية القيادة العامة للدرك الوطني** بموجب المرسوم الرئاسي رقم183-04[2]، الذي يتولى الفحوص العلمية و الدعم التقني في التحقيقات المعقدة عبر قسم الإعلام الآلي، و**المعهد الوطني للبحث في علم التحقيق الجنائي تحت وصاية المديرية العامة للأمن الوطني** بموجب المرسوم الرئاسي 432-04 المتخصص بإعداد التقارير الفنية و التدريب و تطوير المعارف في مجال التحقيق الجنائي و التكنولوجيا.[3]

ثالثا: صعوبات تتعلق بالتشريع: من أبرز المعيقات التي تواجه الدول في تنظيم موضوع الجرائم المعلوماتية و هو القصور التشريعي، مما جعل هذه الدول تعمل على إعادة و تحديث منظومتها القانونية عن طريق تعديل قوانينها الإجرائية.[4]

مما دفع بالمشرع الجزائري إلى استحداث آليات قانونية تيسر من عملية جمع الأدلة، عبر إصدار القانون رقم 09-04 المؤرخ في 2009/08/05 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، حيث أتى لتنسيق الجهود مع السلطات القضائية في جمع الأدلة الرقمية و إجراء الخبرات، بهدف تعزيز فعالية التحقيقات.

1- فراحتية خلود، نفس المرجع السابق، ص34.

2- الجريدة الرسمية رقم84، الصادرة بتاريخ 2004/12/29،ص24.

3- قرار وزاري مشترك مؤرخ في 2007/04/14، المتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية رقم 36، الصادر بتاريخ 2007/06/03،ص14.

4- فراحتية خلود، نفس المرجع السابق، ص- ص 37,36.

الخلاصة:

يتناول هذا الفصل الإطار المفاهيمي للإثبات في الجرائم المعلوماتية، حيث يسلط الضوء على التحولات الجذرية التي فرضتها الثورة الرقمية، والتي نقلت الجرائم من الفضاء المادي إلى الافتراضي كالاختراق و انتحال الهوية، مما جعل الأنظمة القانونية تواجه تحديات عديدة في إثبات هذه الجرائم بسب تعقيداتها التقنية و سرعتها الفائقة مما يستلم تحديثا تشريعيا و بناء قدرات تقنية متخصصة، مما دفع بالمشرع الجزائري إلى بناء أساس إثباتي جنائي لمواجهة هذا النوع من الجرائم المعلوماتية التي واجهها المشرع بقانون 04-09، و كانت النقطة الفاصلة هنا هي الأدلة الرقمية التي تلعب دورا محوريا في الكشف عن هذه الجرائم سواء كانت بيانات تلقائية من الأجهزة أو مدخلة، و رغم هذا فإنها تواجه تحديات عديدة، إلا أن المشرع الجزائري قد بذل مجهودا لمواجهة هذه التحديات بإنشاء المعهد الوطني للأدلة الجنائية و علوم الإجرام و المعهد الوطني للبحث في علم التحقيق الجنائي، و في الأخير إن مكافحة الجرائم المعلوماتية تتطلب تكاملا بين التطور التشريعي، و تدريب الكوادر على التقنيات الحديثة، و تعزيز التعاون الدولي مع مراعاة التوازن بين فعالية التحقيقات و حماية الخصوصية الفردية.

الفصل الثاني
إجراءات البحث والكشف عن الأدلة الرقمية في الجرائم المعلوماتية

من أبرز الخصائص التي تميز الجرائم المعلوماتية الطابع العابر للحدود، حيث يشير إلى آثار الجرائم تتجاوز حدود الدولة مما يجعلها تشمل دولا أخرى هذا ما يؤدي إلى صعوبة جمع الأدلة اللازمة لإثبات الجريمة وملاحقة مرتكبيها، هذا ما يشكل تحديا كبيرا أمام السلطة القضائية في التصدي له على الرغم من الجهود المبذولة لمكافحتها، وعليه تم التطرق للإجراءات الخاصة بالبحث والكشف عن الأدلة الرقمية في (المبحث الأول) وحجية الدليل الرقمي أمام القاضي الجزائي في (المبحث الثاني).

المبحث الأول: الإجراءات الخاصة بالبحث والكشف عن الأدلة الرقمية

سنتطرق إلى إجراءات البحث والكشف عن الأدلة الرقمية من طرف الأجهزة الأمنية في (المطلب الأول)، أما (المطلب الثاني) فقد خصصناه إلى إجراءات استخلاص الدليل الرقمي للكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

المطلب الأول: إجراءات البحث والكشف عن الأدلة الرقمية من طرف الأجهزة الأمنية

الفرع الأول: على المستوى الدولي.

أولا: المنظمة الدولية للشرطة الجنائية الأنتربول.

المنظمة الدولية للشرطة الجنائية تعد الآلية الفعالة والإطار الأنسب في مكافحة الجرائم المعلوماتية، نظرا لما تقدمه من إمكانية ضبط وتعقب مرتكبي الجرائم بمختلف أنواعها عبر مختلف الدول، وتسليمهم إلى الهيئات المختصة من أجل محاكمتهم ومعاقبتهم. وقد انبعثت الفكرة الأولى لنشأتها من إمارة موناكو، وذلك سنة 1914عندما دعا الأمير ألبرت الأول_ أمير موناكو وقتئذ_حكومات الدول المختلفة للاشتراك في مؤتمر يحضره كبار رجال الشرطة المتخصصون في مضمار الأمن،[1] كي يقوموا بوضع اللبنة الأولى للتعاون الدولي في المجال الشرطي، وكان الاجتماع ناجحا للغاية غير أن كل الخطط علقت جراء اندلاع الحرب العالمية الأولى وفي سبتمبر 1923 دعا يوهانس شوبر رئيس شرطة فيينا إلى عقد مؤتمر دولي وأطلق عليه اسم المؤتمر الدولي الثاني للشرطة القضائية_فيينا وقد نجم عن هذا المؤتمر قيام اللجنة الدولية للشرطة القضائية التي اتخذت من فيينا مقرا لها[2].

1 .د/ عائشة عبد الحميد، النظام القانوني للمنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مجال التعاون القضائي الشرطي، المجلة الاكاديمية للأبحاث والنشر العلمي، العدد11، دكتوراه علوم في القانون الدولي علاقات دولية، جامعة الطارف، الجزائر، 2020.

2_ الموقع الرسمي للمنظمة الدولية للشرطة الجنائية الأنتربول رابط الموقع: https://www.interpol.int/ar

وفي سنة1927 اعتمد المشاركون في الدورة الرابعة للجمعية العامة الأنتربول التي عقدت في أمستردام قرارا يقضي بأن يعين كل بلد عضو جهة اتصال مركزية ضمن بنيته الشرطية، وبحلول سنة 1930 أنشئت أقسام متخصصة لمعاملة السجلات الجنائية وتزييف العملة وتزوير جوازات السفر، وكانت البيانات تسجل وتحلل يدويا قبل الثمانينات عندما بدأ الأنتربول يستخدم الحاسوب لحفظ ملفاته.[1]

وخلال عام1938 اصبحت المنظمة تحت سيطرة النازية، وفي سنة 1941 نقل مقر اللجنة إلى برلين، وبالتالي توقفت أنشطة الأنتربول بشكل أساسي حتى انتهاء الحرب العالمية الثانية، وفي سنة 1946 باشرت بلجيكا إعادة بناء المنظمة بعد انتهاء الحرب العالمية الثانية، واعتمد نظام ديمقراطي لانتخاب الرئيس وأعضاء اللجنة التنفيذية، ونقل مقر المنظمة إلى باريس فرنسا.[2]
وفي سنة 1956 جرى تغيير اسم اللجنة الدولية ليصبح المنظمة الدولية للشرطة الجنائية الأنتربول، وأصبحت مستقلة عن طريق جمع المساهمات من البلدان الأعضاء والتعويل على الاستثمارات المالية، باعتبارها وسيلة التمويل الأساسية.

تعزز وضع الأنتربول كمنظمة دولية في السبعينات بفضل اعتراف الأمم المتحدة به وتوقيع اتفاق المقر مع فرنسا عام1972، وقد اتخذت الأمانة العامة للأنتربول من فرنسا مقرا لها منذ عام 1946، واستقرت أولا في باريس ثم في سان كلو بين عامي 1966 و1989، لتنتقل بعد ذلك إلى ليون.[3]

وازداد عدد بلد الأعضاء في الأنتربول من 20 بلدا عضوا مؤسسا في عام 1923 ارتفع في عام 1955 إلى 50 بلدا عضوا بينما كانت المنظمة تعيد بناء نفسها بعد الحرب العالمية الثانية، وانظمت أمم جديدة إلى المنظمة بسبب تغيير الحدود الجغرافية ولاسيما بفعل

1- شرقي نبيل، المنظمة الدولية للشرطة الجنائية ، مذكرة لنيل الماستر في القانون تخصص: قانون، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2021/2020.
2- ط.د/ بوشارب هانية. ط.د/ شبوعات موسى، الأجهزة الأمنية المختصة بالبحث والكشف عن الأدلة الرقمية في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، مداخلة في ملتقى وطني بعنوان إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال- الصعوبات والتحديات-، جامعة الجزائر1 (بن يوسف بن خدة)، كلية الحقوق، 17 أفريل2025، ص3.

انهيار الإتحاد السوفييتي وجمهورية يوغوسلافيا السابقة مثلا، وفي عام 1967 بلغ عدد البلدان الأعضاء 100 بلد، وفي عام 1989 وصل إلى 150 بلد، بعد ذلك إلى 196 بلد في عام 2023.[1] وفي شهر أوت 1963 انظمت الجزائر إلى المنظمة الدولية للشرطة الجنائية أنتربول ممثلة بالمكتب المركزي الوطني، تعمل تحت الوصاية المباشرة لمديرية الشرطة القضائية المديرية العامة للأمن الوطني، ويباشر مهامه وفقا لنصوص التشريعات الوطنية ملتزما بالأطر القانونية المسيرة للمنظمة الدولية للشرطة الجنائية الأنتربول.[2]

المهمة الرئيسية لمنظمة الأنتربول هو تأمين التعاون المستمر بين الدول، وتحديدا بين أجهزتها الأمنية في مجال مكافحة الجريمة المنظمة، التي تطورت كثيرا لتشمل الجرائم الحديثة لتأثرها بالتطور التكنولوجي حيث تقوم المنظمة وطبقا للمادة الثانية من النظام التأسيسي بالمهام التالية:

1_ تأمين وتطوير أوسع لمساعدة متبادلة بين كل سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان.

2_ إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام وفي مكافحته.[3]

وتستعمل هذه المنظمة وظيفتين رئيسيتين لتحقيق أهدافها:

_ التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم. وتسليمهم للدول التي تطلبهم.

_ جمع المعلومات عن الجرائم المتصلة بالمعلوماتية ويحفظها ويحللها، ويتبادلها مع جميع بلدانه الأعضاء عبر منظومة الأنتربول العالمية للاتصالات، ويتم ذلك التعاون من خلال

1- د. عائشة عبد الحميد، المرجع السابق، ص4.

2- الجزائر في المنظمة الدولية للشرطة الجنائية- الأنتربول منذ 1963، مجلة الشرطة المديرية العامة للأمن الوطني. العدد119، جويلية/ أوت، 2013 ص52.

3- المادة 02 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية الأنتربول المعتمد أثناء الدورة 25 للجمعية العامة للأمم المتحدة بفيينا سنة 1956، الموجود على الرابط:
file:///C:/Users/SAM/Downloads/01%20A%20Constitution_2023.pdf

المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة[1] وذلك عن طريق مايلي:

زيادة تبادل المعلومات بين الدول الأعضاء بشأن الأساليب الإجرامية المتبعة في الجرائم المعلوماتية عن طريق الفرق العاملة الإقليمية وحلقات العمل التدريبية، وقد تم إنشاء نقاط اتصال مستمرة ويمكنها تلقي أو تقديم المعلومات وطلبات المساعدة، وتعتبر شبكة النقاط المرجعية المركزية الوطنية شرطا أساسيا لاستحداث منظومة إنذار مبكر، وقد بادر أكثر من 120 مكتبا مركزيا إلى تعيين نقاط مرجعية مركزية وطنية[2].

تعمل المنظمة الدولية للشرطة الجنائية الأنتربول في مجال الجرائم المعلوماتية بوضع قائمة اسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم محل دراستنا، كما توفر هذه المنظمة للدول الأعضاء المعلومات اللازمة عن الطرق العملية في مجال الجرائم المعلوماتية من خلال خلق فرق عمل وورشات تكوين. ولقد أُنشئت هذه المنظمة خلال عام 2004 وحدة خاصة لمكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في مجال الجرائم المعلوماتية[3].

قامت منظمة الأنتربول بوضع منظومة عالمية للاتصالات الشرطية بهدف توفير اتصال فعال وآني بين أجهزة الشرطة في مختلف الدول.[4]

ثانيا: شرطة الويب الدولية

أُنشئت هذه المنظمة في الولايات المتحدة الأمريكية سنة 1986 لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة الكترونيا، والبحث عن الأدلة التي تدينهم وتقديمهم للمحاكمة،

1- سحر سعد عبد السميع محمد، الحماية الجنائية للتوقيع الإلكتروني ،د.ر.ط، 2022، دار الفكر والقانون، مصر، ص 394،

2- سحر سعد عبد السميع محمد، المرجع السابق، ص 395.

3- محمود سعد عبد المجيد، الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية دراسة تحليلية وصفية مقارنة، د.ر.ط، 2023، دار المطبوعات الجامعية، الإسكندرية-مصر، ص 470.

4- د. عائشة عبد الحميد، المرجع السابق، ص8.

وتضم هذه المنظمة متخصصين من هيئات إنقاذ القانون والمؤسسات الحكومية وضباط الشرطة، ومتطوعين فنيين من عدة دول من العالم، ونظرا لاتساع هذه المنظمة وأهمية النشاطات التي تقوم بها حول العالم بالتعاون مع مؤسسات إنفاذ القانون في الدول الأعضاء فهذا سهل لها عملية تتبع النشاطات الإجرامية التي ترتكب عبر شبكة الإنترنت على مستوى عدة دول وهذا ما تثبته التقارير التي تصدرها هذه المنظمة حول نشاطاتها.

وتعتمد هذه المنظمة على قاعدة بيانات مركزية عملاقة يتم من خلالها تسجيل كافة الحوادث والأنشطة الإجرامية في مجال المعلوماتية، نظرا للمهارات الفنية العالية والقدرات المعرفية والعلمية الخارقة التي يتمتع بها القائمين على هذه المنظمة في مجال التكنولوجيات الحديثة.[1]

الفرع الثاني: على المستوى الإقليمي.

من بين الأجهزة الإقليمية التي تساهم في مجال التعاون لمكافحة الجريمة بصفة ومن بينها الجريمة المعلوماتية اخترنا التطرق إلى الشرطة الأوروبية اليوروبول (أولا) وإلى وحدة التعاون القضائي الأوروبية الأوروجيست (ثانيا)، و(ثالثا) فقد تطرقنا فيه إلى شنجن بينما إلى المنظمة الإفريقية للشرطة الجنائية الأفريبول (رابعا)، ومجلس وزراء الداخلية(خامسا).

أولا: الشرطة الأوروبية اليوروبول

أُنشئت الشرطة الأوروبية اليوروبول أول مرة أمام المجلس الأوروبي من قبل ألمانيا سنة 1991، بمناسبة انعقاد مؤتمر لوكسمبورغ، غير انه تجسد فعليا سنة 1955، وذلك بعد مصادقة دول المجلس الأوروبي على اتفاقية ماستر يخت في 1995/07/29، ليتخذ من لاهاي مقرا له.[2]

1- عميمر عبد القادر، المرجع السابق، ص-ص 374-375،

2 -ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه علوم، تخصص؛ قانون العقوبات والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016/2015، ص152.

مكلف بمكافحة الجرائم المعلوماتية، عن طريق معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الإتحاد الأوروبي، وكذا يقوم بتسهيل تبادل تلك المعلومات عن طريق تزويد المحققين ومدعم بمساعداته التقنية[1] وفي سنة 2010 قام اليوروبول بإنشاء مراكز و وحدات تابعة له لأجل المكافحة الفعالة للجريمة المعلوماتية بهدف توفير منصة لمديري التحقيقات والملاحقات القضائية في مجال الجريمة المعلوماتية[2]. وتطوير وتعزيز نهج منسق داخل الإتحاد الأوروبي لمكافحة الجريمة المعلوماتية لجعل القضاء الإلكتروني مكانا آمنا لمواطني الإتحاد الأوروبي ومؤسساته وحكوماته[3] ويقوم بتقديم المساندة والدعم للدول الأعضاء ومساعدتها في حل القضايا الجنائية بشكل سريع، ويشرف على اليوروبول مجلس الوزراء لشؤون العدل والداخلية الذي يتألف من وزراء العدل والشؤون الداخلية من جميع الدول الأعضاء في الإتحاد الأوروبي.

ثانيا: وحدة التعاون القضائي الأوروبية الأوروجيست

هو هيئة تعمل على مد يد العون والتنسيق بين الجهات القضائية الأوروبية أُنشأ سنة 2002 قبل الإتحاد الأوروبي بتاريخ 2002/02/22، بهدف ضمان مناخ أمني والحرية والعدالة، كما يعمل على تطوير آليات مكافحة الجريمة المعلوماتية من خلال تبادل المعلومات بصفة دورية مع محاكم الإتحاد الأوروبي.

وتجدر الإشارة إلى أن الأوروجيست يمثل دعامة في فعالية التحقيقات والمطاردات والمتابعة من قبل السلطات القضائية الوطنية وخصوصا فيما يتعلق بالأنشطة المرتبطة بالجرائم المعلوماتية، فهو يمهد للأوروبول عمله، في مجال التحقيق من خلال مده بالتحليلات اللازمة، ويتكون هيكله البشري من نواب عامين، ومستشارين قضائيين، وضباط الشرطة القضائية

1- سحر سعد عبد السميع محمد، المرجع السابق، ص 395.

2- رابط الموقع:الموسوعةرابط https://www.aljazeera.net/encyclopedia/2016/2/1

3-الطبعة الأولى، ماي 2022، الجزائر، ص262.شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة، مؤسسة الكتاب القانوني إبن النديم

لمختلف الدول الأعضاء في الإتحاد الأوروبي الذين لهم صفة الاختصاص بحكم ندبهم من قبل كل دولة وفقا لنظامها القانوني.[1]

تختص الأوروجيست بالمتابعة والتحقيق في نفس الجرائم التي يختص بها الأوروبول، مع اختصاصه بمتابعة الجرائم المعلوماتية.

ويحكم عمل الأوروجيست في مجال متابعة الجرائم المعلوماتية (03) أهداف رئيسية هي:

تطوير وتحسين وسائل التنسيق في مجال المتابعة وذلك بين السلطات المختصة للدول الأعضاء.

تسهيل التعاون بين الجهات القضائية في مجال المتابعات من خلال تنفيذ أوامر المساعدة القضائية الدولية، و الاستجابة لطلبات الأبعاد.

دعم السلطات الوطنية من أجل ضمان فعالية المتابعة الجزائية.

ثالثا: شنجن

من خلال التوقيع على معاهدة شنجن في 1985/06/14 تم إنشاء فضاء جماعي من غير حدود سمي بشنجن وعلى اتفاقية تطبيق تلك المعاهدة في 1990/06/19، وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوروبي لمواجهة التحديات الأمنية التي تفرضها الظروف الجديدة منها الجرائم المعلوماتية، وهاتان الوسيلتان هما :

_ مراقبة المشتبه فيهم عبر الحدود وملاحقة المجرمين.[2]

نظام معلومات شنجن يتكون من قسم مركزي مقره مدينة ستراسبورغ وأقسام وطنية في كل دولة من دول المنظمة، كذلك به بنك معلومات كبير تسجل فيه المعلومات التي ترسلها إليه قوات

1 - ربيعي حسين، المرجع السابق، ص-ص 154-155.

2 - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، د.ر.ط.د.س.ن، دار الجامعة الجديدة، الإسكندرية- مصر، ص-ص 261,260.

الشرطة والسلطات القضائية في كل دولة، ومن بين هذه المعلومات عناوين الأفراد سواء أولئك المطلوب تسليمهم من قبل دول أخرى أو من دخول أراضي دولة ما، أو المعلن اختفاؤهم أو المطلوب تقديمهم للعدالة بأمر قضائي لأي سبب كان.[1]

رابعا: المنظمة الإفريقية للشرطة الجنائية الأفريبول

وهي أكبر منظمة شرطة في القارة الإفريقية المكونة من قوات الشرطة ب41 دولة أُنشئت بمبادرة من الدولة الجزائرية يوم 2015/12/13 مقرها الرئيسي الجزائر العاصمة، وتم الإعلان رسميا عن بداية نشاطها يوم 2017/07/06 بمناسبة اجتماع مسؤولي أجهزة الشرطة للدول الإفريقية الأعضاء في الإتحاد الإفريقي المنعقد بالجزائر[2]، وتكمن مهام الأفريبول في مضاعفة رصيد التعاون الشرطي الإقليمي والدولي وتحديد السياسة العامة للشرطة الجنائية، وتوفير تكوين وإعادة تأهيل مختلف أجهزة الشرطة الإفريقية، التي تشهد تأخر وضعف على مستوى الأداء وكذلك تعزيز قيام السلم والأمن و الاستقرار في القارة الإفريقية، وإيجاد الحلول الفاعلة للجرائم التي تواجهها بعض الدول الإفريقية مثل جرائم الإرهاب والمخدرات والجرائم المعلوماتية.[3]

خامسا: مجلس وزراء الداخلية العرب

على المستوى العربي نجد أن مجلس وزراء الداخلية العرب قد أنشأ المكتب العربي للشرطة الجنائية في سنة 1965 بناءا على الاتفاقية الخاصة بإنشاء المنظمة العربية للدفاع الاجتماعي ضد الجريمة، حيث كان مكتب الشرطة الجنائية في دمشق أحد مكاتبها المتخصصة ويمارس

1- سحر سعد عبد السميع محمد، المرجع السابق، ص-ص 397,396.

2- المرسوم الرئاسي رقم 18-140 المؤرخ في 21 مايو 2018، يتضمن التصديق على الإتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية ومفوضية الاتحاد الإفريقي المتعلق بمقر آلية الإتحاد الإفريقي للتعاون الشرطي (الأفريبول) المحرر بالجزائر 14 مايو 2017، ج ر العدد 30 المؤرخة في 27 مايو 2018. أنظر كذلك المادة 24 والمادة 13 من النظام الأساسي المنظم لآلية (الأفريبول).

3- عبد العزيز لزعر، رشيد زياني، آلية الإتحاد الإفريقي للتعاون الشرطي(الأفريبول) ودورها في مكافحة الجريمة الالكترونية، مجلة متون، كلية الحقوق، جامعة مولاي الطاهر، سعيدة، المجلد 14، العدد03، 2021، ص- ص254-256

هذا المكتب نشاطه من خلال ثلاث وزارات الداخلية، العدل والشؤون الاجتماعية، على مستوى الدول العربية.[1]

بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة،[2] بالإضافة الى تقديم المعونة التي تطلبها الدول الأعضاء، من أجل دعم وتطوير أجهزة الشرطة.[3]

وإلى جانب المكتب العربي للشرطة الجنائية يساعده المكتب العربي لمكافحة الجريمة أين يتخذ المكتب من بغداد مقرا له وقد باشر مهامه سنة 1965 في نطاق المنظمة العربية للدفاع الاجتماعي ضد الجريمة وذلك بعد اكتمال تصديقات الدول الأعضاء على الاتفاقية المنشئة للمنظمة بموجب قرار مجلس جامعة الدول العربية رقم 1685 سنة1960.[4]

1- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية دراسة مقارنة، الطبعة الأولى، دار الفكر والقانون، 2015، ص140.

2-عائشة بن قارة مصطفى، المرجع السابق، ص 261.

3- محمد كمال محمود الدسوقي، المرجع السابق، ص-ص 141,140.

4- منصارة يوسف، الدليل الإلكتروني في القانون الجزائي الطريق إلى تحول أدلة الإثبات في المادة الجزائية دراسة مقارنة، د.ر.ط، 2018، دار الخلدونية، الجزائر، ص285.

كما استحدث المشرع الجزائري القطب الجزائي كجهة متخصصة لمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

فقد أثارت مسألة الإختصاص القضائي سواء المحلي أو النوعي تسآءل كبيرا، وعليه حسم المشرع الجزائري هذه المسألة بمنح الإختصاص بالنظر فيها أمام القطب الجزائي الذي وضع له اختصاصا محليا ونوعيا بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، المحددة حصريا ووجوبيا طبقا للتنظيم الخاص به في ظل الأمر 21-11 المتضمن تعديل قانون الإجراءات الجزائية.

أولا: الإختصاص النوعي القضائي للقطب الجزائي الوطني

يقصد بالإختصاص النوعي أن تكون الجهة الجزائية مختصة بالنسبة لنوع محدد من الجرائم، من حيث طبيعتها أو جسامتها جناية أو جنحة أو مخالفة، أو بعبارة أخرى اختصاص كجهة جزائية بنوع محدد من الجرائم.

وفقا للمادة 211 مكرر24: مع مراعاة أحكام الفقرة 2 من المادة 211 مكر22 يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وقاضي التحقيق ورئيس ذات القطب الحصري بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[1] من بين هذه الجرائم:

- ❖ جرائم المساس بأنظمة المعالجة الآلية[2]
- ❖ الجرائم المتصلة بتكنولوجيات الإعلام والإتصال كالمساس بأمن الدولة ، جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين...[3]

ثانيا: الاختصاص الاقليمي

1- نصيرة بوعزة، المحاكم ذات الإختصاص المحلي الموسع كآلية لمكافحة الإجرام الخطير، مجلة ميلاف للبحوث والدراسات، المركز الجامعي عبد الحفيظ بوالصوف ميلة (الجزائر) المجلد7، العدد1، جوان 2021، ص 184.

2 - نصيرة بوعزة، المرجع نفسه، ص 184.

3- سهيل صليحة، سوسي فريدة، القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتعلقة بتكنولوجيات الإعلام والإتصال، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة البشير الابراهيمي. برج بوعريريج، 2022/2021، ص26.

حدد المشرع الجزائري ضمن تعديل الأمر 21-11 في المادة 211 مكرر23 على أن القطب الجزائي المنشئ على مستوى مقر مجلس قضاء الجزائر يمارس فيه كل من وكيل الجمهورية وقاضي التحقيق ورئيس القطب الصلاحيات في كامل التراب الإقليمي الوطني، وما قصده المشرع هنا أن مكافحة الجريمة المعلوماتية يتطلب الخروج عن قواعد الإختصاص العامة المنصوص عليها في قانون العقوبات، وبالرغم من تمديد الإختصاص المحلي لكل من وكيل الجمهورية وقضاة التحقيق ومحاكم ومجالس قضائية بموجب المرسوم التنفيذي رقم 348-06 المتضمن تمديد الاختصاص من الإقليمي إلى الوطني، وهذا راجع لخطورة وطبيعة هذه الجرائم التي قد ترتكب من قبل عدة أشخاص وتقع في أكثر من مكان قد تتعدى حدود الدولة الجزائرية.[1]

والجريمة المتعلقة بتكنولوجيات الإعلام والإتصال بكونها تتسم باتساع مكان وأشخاص ارتكابها فلقد أعطى المشرع الجزائري للقطب الجزائي اختصاصا إقليميا في كامل التراب الوطني وهذا ما نصت عليه المادة 211 مكرر23 من القانون 21-11:" **يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني**".[2]

والمقصود من هذا النص أن المشرع منح للقطب الجزائي المذكور اختصاصا إقليميا وطنيا، حيث يمتد لإقليم كامل الدولة الجزائرية كوحدة إقليمية على اعتبار الجرائم المرتبطة بتكنولوجيات الإعلام والإتصال تتسم باتساع مكان وأشخاص ارتكابها وكما أنها على درجة من الخطورة والتعقيد. هذا وقد نصت المادة 32 الفقرة الأولى نصت على أن الأقطاب الجزائية المتخصصة تتشكل ضمن المحكمة ذات الاختصاص العام.[3]

1- عون فاطمة الزهراء، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري- القطب الجزائي الوطني نموذجا- مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس، المجلد07، العدد02، 2022، ص563

2- القانون رقم 21-11 المؤرخ في 16 محرم 1443 الموافق 25 أوت 2011، الجريدة الرسمية للجمهورية الجزائرية العدد65.

3- المادة 32 من قانون الإجراءات الجزائية.

1- اختصاص حصري

بموجب نص المادة 211 مكرر26 من القانون رقم 21-11 السابق الذكر، خول المشرع القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال اختصاصا حصريا فيما يخص الجرائم التي حددتها المادتين 211 مكرر24 و211 مكرر25، في كافة أنحاء التراب الوطني دون سواه، وذلك بالنظر إلى خصوصية تلك الجرائم التي وجد من أجلها وبموجب تشكيلة قضاة متخصصة في هذا النوع من الجرائم التي تتسم بالخطورة، التعقيد والتي تمتد إلى خارج حدود الدولة الجزائرية.[1]

- الاختصاص الحصري في الجنح الواردة في المادة 211 مكرر24 قانون الإجراءات الجزائية.

- الاختصاص الحصري في الجرائم الأكثر تعقيدا والجرائم المرتبطة بها المادة 211 مكرر 25 قانون الاجراءات الجزائية.

2- الاختصاص التفضيلي

يتمتع القطب المستحدث عند معالجته لباقي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها، التي تخرج من اختصاصه الحصري المحدد بنصوص المواد: 211 مكرر24، 211 مكرر25 مثل ماسبق توضيحه باختصاص مشترك مع باقي الجهات القضائية المختصة إقليميا مع تمتعه بأفضلية معالجتها، حيث يمارس وكيل الجمهورية لدى القطب المستحدث وكذا قاضي التحقيق ورئيس القطب اختصاصا مشتركا مع الجهة القضائية المختصة محليا، بموجب المواد:37، 40، 329 من قانون الإجراءات الجزائية، والتي تضبط معيار الاختصاص المحلي بمكان ارتكاب الجريمة أو محل إقامة أحد المتهمين، أو محل القبض على أحدهم، مع جواز تمديده لدائرة اختصاص محاكم أخرى عندما يتعلق الأمر بالجرائم الستة.[2]

3- اختصاص وجوبي

1- بن عمیور أمینة، بوحالیس إلهام، مرجع سابق، ص 75

2- بن عمیور أمینة، بوحالیس إلهام، المرجع نفسه، ص 77.

إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مع اختصاص مقر مجلس قضاء الجزائر طبقا لأحكام المواد 211 مكرر16 إلى 211 مكرر21 من القانون 21-11 يؤول الاختصاص وجوبا للقطب الجزائي.

المطلب الثاني: إجراءات استخلاص الدليل الرقمي للكشف عن الجرائم المعلوماتية

لم يقتصر دور المشرع الجزائري على تجريم الاعتداء على معطيات الحاسب الآلي بشكل عام بل وضع أيضا إجراءات خاصة باستخلاص الدليل الرقمي وعليه سنتطرق من خلال هذا المطلب إلى الإجراءات التقليدية في (الفرع الأول) وكذا الإجراءات المستحدثة (الفرع الثاني).

الفرع الأول: الإجراءات التقليدية لاستخلاص الدليل الرقمي

أولا: المعاينة

1_تعريفها: عُرفت المعاينة على أنها " **إثبات الحالة التي يكون عليها مسرح الجريمة عند انتقال المحقق إليه، وإثبات ما به من آثار وحالة الأشخاص المتواجدين به، والتحفظ على كل ما من شأنه أن يغير في كشف الحقيقة** " يقصد بها كذلك " **فحص مكان الشيء أو شخص له علاقة بالجريمة**".[1]

من هذين التعريفين نستنتج أن المعاينة إجراء هام تمتلكه سلطات التحقيق طبقا للمادة 79 من قانون الإجراءات الجزائية[2] يقدم صورة حقيقية عن مكان وقوع الجريمة. والمعاينة في الجرائم المعلوماتية هي معاينة الآثار التي يخلفها مستخدم الشبكة المعلوماتية أو الإنترنت وتشمل الرسائل المرسلة منه أو التي استقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة المعلوماتية.

1- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية، دار النشر، المكتب الجامعي الحديث المولى 2012، ص32.

2- نص المادة 79 من ق إ ج أنه:" ويجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته. ويستعين قاضي التحقيق دائما بأمين ضبط التحقيق ويحرر محضرا بما يقوم به إجراءات".

2_ إجراءات معاينة مسرح الجريمة

أول خطوة يقوم بها الضابط القضائي عند وقوع الجريمة هو الانتقال إلى مسرح الجريمة، وينبغي التعامل مع مسرح الجريمة الالكترونية على أنه نوعين مسرح تقليدي ومسرح رقمي.

يقع المسرح التقليدي خارج بيئة الحاسوب و الإنترنت يتكون من جميع المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية يترك فيها الجاني آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية. أما المسرح الرقمي فيوجد داخل العالم الافتراضي لجهاز الحاسب الآلي في ذاكرة الأقراص الصلبة الموجودة بداخله، أي يحتوي على جميع البيانات والمعلومات الرقمية المخزنة فيه والتي تفيد في التحقيق.[1]

وللمعاينة إجراءات نذكرها:

_ القيام بتصوير جهاز الحاسب الآلي الذي تمت من خلاله الجريمة، بالإضافة إلى كل ما يتصل به من أجهزة طرفية، وأيضا محتوياته وأوضاع المكان الذي يوجد فيه بصفة عامة.

_ عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغناطيسية في العالم الخارجي.

_ القيام بحذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسب الورقية.

_ ربط أقراص الكمبيوتر التي ربما تحمل أدلة مع جهاز يمنع الكتابة عليها مما يتيح للمحققين قراءة بياناتها من دون تغييرها.

ثانيا: التفتيش

1- فاطمة زهرة بوعناد، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، الجزائر، 2013، ص68.

يعد التفتيش من إجراءات التحقيق الهامة التي تسعى لكشف الحقيقة في مستودع السر، وتكمن أهمية هذا الإجراء في الوصول إلى الأدلة التي تساهم بشكل كبير في إظهار الحقيقة وكشفها، لكن بالرغم من أهمية التفتيش في كشف الحقائق، إلا انه يعد من أخطر إجراءات التحقيق على الحياة الخاصة للأفراد[1].

يعرف التفتيش بأنه إجراء بحثي مادي يجرى في مكان ما بهدف العثور على أشياء ذات صلة بجريمة قيد التحقيق أو جمع الاستدلالات بشأنها[2]، أو هو إجراء من إجراءات التحقيق ينفذه موظف مختص وفقا للإجراءات القانونية في مكان قد يتمتع بالحرمة، بهدف الوصول إلى أدلة مادية تثبت وقوع جناية أو جنحة وتحدد مرتكبها أو تنسبها إلى متهم معين[3].

أما التفتيش في البيئة الرقمية هو إجراء يستخدم فيه الوسائل الإلكترونية لجمع الأدلة المخزنة أو المسجلة الكترونيا[4]. وللتفتيش 3 أنواع:

1_ تفتيش مكونات الجهاز الإلكتروني المادية

يخضع تفتيش المكونات المادية للأجهزة الإلكترونية بحثا عن أدلة أو أي شيء يتعلق بالجريمة المعلوماتية لنفس الإجراءات القانونية والقواعد العامة المطبقة في التفتيش التقليدي، وذلك لأن الغاية هنا هي تفتيش أجزاء مادية، يعتمد هذا التفتيش على طبيعة المكان الذي توجد فيه هذه المكونات، سواء كان مكانا عاما أو خاصا، حيث أن صفة المكان تلعب دورا هاما في تحديد إجراءات تفتيشه، فإذا كانت المكونات المادية موجودة مع شخص في مكان عام ، تخضع لنفس إجراءات التفتيش في الأماكن العامة، أما إذا كانت المكونات المادية للجهاز

1– سماحي سمية، إثبات الجنائي بالوسائل المستحدثة للجرائم (دليل رقمي)، مداخلة في ملتقى وطني بعنوان: الجرائم الالكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبرياني، كلية العلوم الإنسانية والاجتماعية، جامعة يحيى فارس المدية، 15 مارس 2022، ص164

2- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، 2009، ص91.

3- عبدالفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية،القاهرة،2007. ص244،

4- علي عدنان الفيل، المرجع السابق، ص39.

الإلكتروني موجودة في مكان خاص، فتخضع لنفس إجراءات تفتيش الأماكن الخاصة بنفس الضمانات القانونية المقررة لها[1].

2_ تفتيش مكونات الجهاز الإلكتروني المعنوية

إذا كان تفتيش المكونات المادية للحاسوب أمرا يسيرا من الناحية الإجرائية والتنفيذية مع ضرورة مراعاة الضمانات القانونية اللازمة، فإن الإشكالية الحقيقية تكمن في تفتيش المكونات المعنوية للحاسوب، ويعود هذا الإشكال إلى الطبيعة غير المادية للبيانات والمعلومات المخزنة، وقد انقسم الفقه القانوني في هذه المسألة إلى اتجاهين رئيسيين:[2]

الاتجاه الأول يرى استحالة تطبيق أحكام التفتيش التقليدية المنصوص عليها في القوانين الإجرائية على المعطيات المعلوماتية، يرتكز هذا الرأي على أن التفتيش التقليدي يهدف إلى البحث عن الأشياء المادية الملموسة وضبطها، بينما الأدلة الرقمية هي كيانات معنوية غير مادية، وبالتالي لايمكن تطبيق مفهوم الشيء المادي عليها، ويرى هذا الاتجاه أن عمليات البحث والتنقيب عن الأدلة في الحاسوب باستخدام البرامج تتجاوز مفهوم التفتيش التقليدي.

أما الاتجاه الثاني يرى إمكانية تطبيق أحكام التفتيش على برامج الحاسوب وبياناته، باعتبارها تخضع لخصائص وسمات المادة من حيث وجودها وقابليتها للحفظ والاسترجاع، ويرى هذا الاتجاه أن الغاية من التفتيش هي الحصول على الأدلة الجنائية وكشف ملابسات الجريمة، وهذا يشمل أيضا المعطيات المخزنة على الحاسوب بشكل غير مشروع، والتي تعد دليلا ماديا رقميا يمكن استخدامه كدليل اتهام، بمعنى آخر يوسع هذا الاتجاه مفهوم الشيء ليشمل الكيانات الرقمية باعتبارها أدلة مادية بشكلها الرقمي.[3]

1- بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر مهني في الحقوق، تخصص: قانون الإعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2022/2021، ص-ص 51,50.

2- برا هيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية بجامعة مولود معمري، تيزي وزو، 2018.

3- هلالي أحمد عبد الإله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2006، ص73،

بالرجوع إلى القانون رقم 09_04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، يتبين بوضوح موقف المشرع الجزائري الذي أجاز صراحة تفتيش المنظومة المعلوماتية، وذلك بموجب المادة 05 منه، وفقا للشروط والإجراءات المنصوص عليها في قانون الإجراءات الجزائية.[1]

3_ تفتيش شبكات الجهاز الإلكتروني

مع التطور التكنولوجي وثورة الاتصالات، لم يعد نطاق الاتصالات محصورا داخل حدود دولة واحدة، بل تجاوزها يشمل العالم بأسره بفضل ظهور شبكة الإنترنت، وقد أدى هذا التطور بالإضافة إلى طبيعة التكنولوجيا الرقمية إلى تعقيد عمليات التفتيش والضبط، فإمتداد الأدلة الإلكترونية عبر شبكات الحاسوب إلى مواقع بعيدة عن مكان التفتيش الفعلي يشكل تحديا كبيرا.[2]

على الرغم من إمكانية الوصول إلى هذه الأدلة عبر الحاسوب بعد الحصول على إذن التفتيش، إلا أن الموقع الفعلي للبيانات قد يقع ضمن اختصاص قضائي آخر أو حتى في دولة أخرى، مما يزيد الأمر تعقيدا فشبكة المعلومات تمتد عالميا، وبالتالي يخضع الحاسوب الذي يرتكب عليه أو بواسطته الجريمة الإلكترونية للإجراءات القانونية الخاصة بالمنطقة التي يتواجد فيها أو التي تتبع لها البيانات[3]، مما يطرح تحديات تتعلق بالاختصاص القضائي والتعاون الدولي في مكافحة الجرائم الإلكترونية.

- يوسف الخليل العفيفي، الجرائم الالكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة"، مذكرة لنيل شهادة الماجستير في القانون العام، قسم القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، فلسطين، 2013، ص120.

2- هلالي أحمد عبد الإله، المرجع السابق، ص76

3- علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديث اربد، الأردن، 2004، ص31.

يثير تفتيش الأنظمة المتصلة بالحاسوب محل التفتيش إشكالية الاختصاص، خاصة إذا كانت هذه الأنظمة موجودة في دوائر اختصاص قضائية مختلفة أو خارج البلاد، نفرق هنا بين فرضيتين:

الفرضية الأولى: إذا كان حاسوب المشتبه فيه أو المتهم متصلا بنظام معلوماتي آخر داخل الجزائر، يجيز القانون الجزائري تمديد التفتيش إلى هذا النظام الثاني، شرط توافر أسباب معقولة الاعتقاد بأن البيانات المطلوبة مخزنة فيه ، وأن الوصول إليها ممكن انطلاقا من النظام الأول. في هذه الحالة يجوز تمديد التفتيش بسرعة إلى النظام الثاني أو جزء منه، بعد إعلام السلطة القضائية المختصة، وذلك استنادا إلى نص المادة 5 الفقرة 2 من القانون 09_04.[1]

الفرضية الثانية: إذا كان حاسوب المشتبه فيه أو المتهم متصلا بنظام معلوماتي موجود خارج الجزائر، يجيز القانون الجزائري تفتيش هذه الأنظمة أيضا حتى ولو كانت موجودة خارج إقليم الدولة، ولكن بشرط الحصول على مساعدة السلطات الأجنبية المختصة وذلك وفقا للاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل وذلك استنادا إلى نص المادة 5 الفقرة 3 من القانون 09_04.[2]

ثالثا: الخبرة

نظرا لطبيعة هذه الجرائم يتم فيها الاستعانة بخبير، وهو شخص يتمتع بمؤهلات عملية وقدرة في التحكم في مجال الإعلام الآلي، وهو ما نصت عليه المادة 05 الفقرة الأخيرة من قانون رقم 09_04 المتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيا الإعلام والاتصال[3].

وتخضع الخبرة لمجموعة من الضوابط لتكون لها نتائج أمام القضاء[1] وهي:

1- القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد47، المؤرخة في 16 أوت 2009.

2- القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد47، المؤرخة في 16 أوت 2009.

3- انظر المادة 5 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

_ اختيار الخبير من جدول الخبراء مع أداء اليمين القانونية، والتزامه بأداء مهامه بنفسه.

_ اعتماد الخبير على وسائل علمية متطورة لإنجاز الخبرة.

الفرع الثاني: الإجراءات الحديثة لاستخلاص الدليل الرقمي

هي عبارة عن أساليب محددة قانونا تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها، وقد استحدث المشرع الجزائري وسائل إجرائية تتمثل في التسرب واعتراض المراسلات نص عليهما القانون رقم 06_22 المؤرخ في 2006/12/20 المعدل والمتمم للأمر رقم 66_155 المتضمن قانون الإجراءات الجزائية الجزائري.

وتم استحداث إجراء المراقبة الإلكترونية الذي أتى بها القانون رقم 09_04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها.

1_ التسرب:

يعرف التسرب بموجب المادة 65 مكرر12 من قانون الإجراءات الجزائية الجزائري بأنه " **القيام بمراقبة الأشخاص أو المشتبه في ارتكابهم الجريمة من خلال ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بإيهامهم أنه فاعل معهم أو شريك أو خاف للجريمة**"[2]، وقد حددت شروط القيام بعملية التسرب كالآتي:

° الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق إذا تم فتح تحقيق قضائي.

1- ط.د/ فلاح عبد القادر. د.أيت عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، جامعة الجيلالي بونعامة خميس مليانة، مجلة الدراسات القانونية، والسياسية، المجلد04 ، العدد02، 2020

2- المادة 65 مكرر12، الأمر 66-155، المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، الجريدة الرسمية، العدد48، الصادرة بتاريخ 10 يونيو 1966 ، المعدل والمتمم لاسيما بالقانون رقم06-22، المؤرخ في 20 ديسمبر 2006، الصادر في الجريدة الرسمية العدد 84، الصادرة بتاريخ 24 ديسمبر 2006، وبالأمر رقم 15-02 المؤرخ في 23 يوليو 2015، الصادر في الجريدة الرسمية العدد40، المؤرخة في 23 يوليو2015.

° أن يكون الإذن الصادر عن وكيل الجمهورية أو قاضي التحقيق مكتوبا ومسببا لمدة أقصاها 4 أشهر، قابلة للتجديد مرة واحدة.

° وجوب تضمنه على هوية ضابط الشرطة القضائية التي تتم عملية التسرب تحت مسؤوليته أو عون الشرطة باعتباره مساعدا له.

° أن يكون هذا الإجراء في جرائم محددة التي نصت عليها المادة 65 مكرر5 والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

2_ اعتراض المراسلات:

نستشف من نص المادة 65 مكرر5 من ق ا ج ج المقصود باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهاته المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين و الاستقبال والعرض.[1]

وهي أيضا عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة.

بالرغم من أن عملية اعتراض المراسلات تشكل انتهاكا لحرمة الحياة الخاصة للأفراد، و اعتداء على سرية مراسلاتهم والتي كفلها في دستور2020 المعدل بموجب القانون رقم 16_01 وذلك من خلال المادة 46 فقرة 2 التي نصت على سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة.[2]

1- أجازت الفقرة الأولى من المادة 65 مكرر5 من ق إ ج ج أن يأذن "اعتراض المراسلات التي تتم عن طريق وسائل الاتصال" السلكية واللاسلكية".

2- انظر المادة 2/46 من الدستور الجزائري، المؤرخ في 8 ديسمبر1966 المعدل بالقانون رقم 1601 المؤرخ في 26 جمادى الأولى عام 1437، ل 6 مارس 2016 المتضمن التعديل الدستوري، العدد14.

إلا أن المشرع الجزائري قد وضع شروط قانونية تنص على منع التعسف في استعمالها وكذلك حماية الحرية الفردية وتتمثل هذه الشروط في الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق إذا تم فتح تحقيق قضائي.[1]زيادة على ذلك يجب أن يكون الإذن مكتوب لمدة أقصاها 4 أشهر قابلة للتجديد، وأيضا وجوب تضمنه على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوبة التقاطها والأماكن المقصودة.[2]

ويعتبر البريد الإلكتروني أهم وسيلة تنفيذ في مجال التراسل الإلكتروني ومن ثم فإن عملية الاعتراض تنصب عليه والتي تمثل مصدرا غنيا الأدلة الرقمية للإثبات في الجرائم الإلكترونية.

وكل رسالة إلكترونية يظهر فيها معلومات عامة ولكن هذه المعلومات ليست كافية لمعرفة المرسل، لأنه يمكن لهذا الأخير إرسال رسالة بأسماء وهمية، كما أن هناك وسائل تسمح للمرسل بإرسال رسالته دون أن يظهر فيها بريده الإلكتروني، لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية وسائل البريد وهي أول خطوة للبدء في التحري عن مرسل الرسالة الإلكترونية.[3]

3_ المراقبة الإلكترونية:

تناول المشرع الجزائري هذا الإجراء في المادة 4 من القانون رقم 09_04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها بعنوان مراقبة الاتصالات الإلكترونية.[4]

والمشرع لم يعرف إجراء المراقبة بل ترك أمر تعريفها للفقه ومنه تعرف بأنها "عمل أساسي له نظام معلومات إلكتروني، ويقوم فيه المراقب بالمراقبة بواسطة الأجهزة الإلكترونية أو عبر شبكة

1 - انظر المادة 65 مكرر5 من الأمر 66-155، المرجع السابق.

2- انظر المادة 65 مكرر7 المتضمن ق إ ج ج.

3- مدربل كريم، الإثبات بالدليل الرقمي في المسائل الجزائية، مذكرة الماستر كلية الحقوق، جامعة أكلي محند أولحاج البويرة 2019، ص43.

4- عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، المجلد09، العدد02، 2018. ص41

الإنترنت، لتحقيق غرض محدد وإفراغ النتيجة في الملف الإلكتروني، وتحديد التقارير بالنتيجة".[1]

والمراقبة الإلكترونية وسيلة من وسائل جميع البيانات والمعلومات عن المشتبه فيه، بحيث يقوم بها مراقب إلكتروني يتمثل في ضابط من ضباط الشرطة القضائية ذي كفاءة تقنية عالية وباستخدام تقنيات وبرامج إلكترونية فيها، وبالتالي ومن خلال القانون رقم 09_04 الذي سبق ذكره، نجد أن المشرع لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الرقمي فقط بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة المعلوماتية.

ويمكن استنتاج شروط وآليات المراقبة الإلكترونية في التشريع الجزائري من خلال نص المادة 65 مكرر5 ق ا ج ج وهي أن يتم تنفيذ هذه العملية تحت سلطة القضاء وبإذن منه، وهو ما نصت عليه المادة 4 من ق ا ج ج و القانون رقم 09_04، بحيث لايجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة.[2]

المبحث الثاني: حجية الدليل الرقمي أمام القاضي الجزائي

لاشك أن القانون يترك للقاضي الجنائي الحرية في أن يستمد اقتناعه من أي دليل، لكن هذا لا يعني أن هذه الحرية مطلقة بل يتعين أن يكون هذا الدليل مقبولا، وعليه سنتطرق إلى سلطة القاضي الجزائي في تقدير الدليل الرقمي (المطلب الأول)، و التحديات القانونية في التعامل مع الأدلة الرقمية (المطلب الثاني).

المطلب الأول: سلطة القاضي الجزائي في تقدير الدليل الرقمي

إن الدليل الرقمي يخضع للمبدأ العام في الإثبات الجنائي، وهو حرية القاضي الجنائي في الإقناع، وحريته في هذا الشأن لها أهمية بالغة، باعتبار أن القاضي الجنائي هو الذي يقدر

1- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت(دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية)، دار الكتب القانونية، مصر، 2005، ص191.

2- أوساسي فؤاد، المرجع السابق، ص-ص 22,21.

وحده قيمة الدليل الإلكتروني، وذلك تبعا للأثر الذي يحدثه في وجدانه من ارتياح، ومن جهة أخرى نجد أن دور الإثبات العلمي أصبح له أهمية كبيرة، خاصة مع ظهور الدليل الإلكتروني المطلوب للإثبات في الجرائم الإلكترونية، وهذا ما يجعل من سلطة القاضي الجنائي في الإثبات الجنائي أساسا لتكوين وجدانه الضروري للحكم.[1]

ولقد أخذ المشرع الجزائري بفكرة الاقتناع القضائي في المادة 307 من ق ا ج ج[2] بالإضافة إلى أن المحكمة العليا أكدت على ضرورة مراعاة مبدأ الاقتناع القضائي وتوصي بأعماله أمام المحاكم الجنائية.

وتجدر الإشارة إلى أنه إذا خالفت إجراءات جمع الأدلة المتحصلة من الوسائل الإلكترونية القواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية، وبالتالي فإن القاضي الجزائي عندما يعرض عليه دليلا متحصلا عليه مثلا من التسجيل الصوتي بالهاتف النقال، عليه أن يحكم باقتناعه من أجل الوصول إلى الحقيقة، ويتأكد من توافر شروط صحته لقبوله كدليل إثبات مثل باقي الأدلة.

أولا: مفهوم مبدأ الاقتناع الشخصي للقاضي الجنائي

يعتبر مبدأ حرية الاقتناع الشخصي للقاضي الجزائي، من أهم عناصر الإثبات في الدعوى الجنائية فالقاضي حر بأن يأخذ بالأدلة التي يراها مناسبة للكشف عن الحقيقة وله أن يحتوي بنفيه صدق الأدلة الرقمية، وله الحق في أن يستمد اقتناعه وعقيدته في أي مصدر يطمئن اليه. وكما تطرق المشرع الجزائري إلى مبدأ الاقتناع القضائي في نص المادة 212 من ق ا ج على أنه: " يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال الشخصية التي ينص

1- بن قارة مصطفى عائشة، المرجع السابق، ص 242.

2- الأمر 66-155، المرجع السابق.

فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص..." ويطبق المبدأ أمام جهات الحكم القضائية.[1]

ثانيا: ضوابط قبول اقتناع القاضي بالدليل

1_ الضوابط التي تتعلق بمصدر الاقتناع: وتتمثل في :

أ_ ضابط أن يكون الدليل الرقمي مقبولا: فعلى القاضي أن يستمد اقتناعه من أدلة مقبولة ومشروعة، وتحترم الإنسان وحريته.

ب_ ضابط ضرورة طرح الدليل الرقمي في جلسة المناقشة: يجب على القاضي أن يستمد قناعته من أدلة طرحت بالجلسة، وخصصت المناقشة بين الخصوم تبعا لمبدأ الشفافية المذكور في المواد 300، 304 و305 من ق ا ج ج، ومبدأ العلانية بحسب المواد 285، 342، 355 و399 من ق ا ج ج.

2_ الضوابط التي تتعلق بالاقتناع ذاته: وجب على القاضي أن يصدر حكمه على اقتناع يقيني، بالإضافة إلى ضابط ملائمة الاقتناع القضائي لمقتضيات العقل والمنطق، أي أنه على القاضي استنتاج الحقيقة الواقعة، وما كشف عنها من أدلة لا يخرج عن مقتضيات العقل والمنطق، من غير تعسف في الاستنتاج .[2] بالإضافة إلى ضرورة توفر ضابط مهم حتى لا يستبد القاضي في حكمه، وهو مراقبة المحكمة العليا لسلطة القاضي الجنائي.[3]

المطلب الثاني: التحديات القانونية في التعامل مع الأدلة الرقمية

من خلال ما سبق يتبين لنا أن القضاء يواجه تحديات متعددة عند التعامل مع الأدلة الرقمية، أبرزها ضمان التوازن بين مصلحة العدالة وحماية حقوق الأفراد، لاسيما فيما يتعلق بالحق في

1- القانون رقم 22/06 الصادر في 2006/12/20 يعدل ويتمم الأمر رقم 66-155 المؤرخ 1966/6/8 والمتضمن قانون الإجراءات الجزائية، (الجريدة الرسمية) العدد84 المؤرخ في 2006/12/24، المادة 212 ق إ ج ج.

2- شحط عبد القادر العربي، الإثبات في المواد الجزائية في ضوء الفقه والاجتهاد القضائي، دار الهدى للنشر والتوزيع، الجزائر، 2006، ص29.

3- بن قارة مصطفى عائشة، المرجع السابق، ص281.

الخصوصية، إذ أن جمع الأدلة الرقمية قد يتطلب الوصول إلى بيانات حساسة، مما يثير تساؤلات قانونية وأخلاقية حول مدى مشروعية هذه الإجراءات، من التحديات الأخرى مشكلة التزوير والتلاعب بالأدلة الرقمية، حيث يمكن تعديل البيانات الإلكترونية بطرق يصعب اكتشافها دون أدوات وتقنيات متقدمة، بالإضافة إلى ذلك يواجه القضاة صعوبة في التعامل مع الأدلة الرقمية في القضايا العابرة للحدود، حيث تختلف القوانين بين الدول بشأن كيفية جمع هذه الأدلة واستخدامها أمام المحاكم، مما يستدعي تعزيز التعاون الدولي وتوحيد المعايير القانونية في هذا المجال.

لمواجهة التحديات المرتبطة بالأدلة الرقمية، بدأت العديد من الدول في تحديث تشريعاتها لتشمل قواعد واضحة تحكم الإثبات الرقمي، كما يتم تطوير أدوات متقدمة في مجال التحليل الجنائي الرقمي لاكتشاف التزوير وضمان موثوقية الأدلة الرقمية، من الاتجاهات الحديثة أيضا استخدام الذكاء الاصطناعي لتحليل البيانات الرقمية وتحديد مدى صحتها، علاوة على ذلك تسعى الدول إلى تعزيز التعاون الدولي في مجال تبادل الأدلة الرقمية، خاصة في الجرائم الإلكترونية التي تتطلب تحقيقات تمتد عبر حدود متعددة.

رغم التطور الكبير في الاعتراف بالأدلة الرقمية، إلا أن القضاة يواجهون عدة تحديات عند التعامل معها، من أبرزها:[1]

° عدم وجود إطار قانوني موحد: تختلف القوانين بين الدول في كيفية التعامل مع الأدلة الرقمية، مما يخلق تحديات في القضايا الدولية أو القضايا التي تتطلب تبادل المعلومات بين الأنظمة القضائية المختلفة.

1- د. سويلم محمد/ د.بوحاده محمد سعد، ضوابط اعتماد القاضي الدليل الرقمي في الإثبات، مداخلة في ملتقى وطني بعنوان: إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (الصعوبات والتحديات)،كلية الحقوق،جامعة الجزائر1 (بن يوسف بن خدة)، المنعقد يوم 17 أفريل 2025، ص-ص 11,10.

° سهولة التلاعب بالأدلة الرقمية: يمكن التعديل على البيانات الرقمية بطرق يصعب اكتشافها دون استخدام تقنيات متقدمة، مما يجعل من الضروري وجود خبراء متخصصين في فحص هذه الأدلة.

° مخاوف انتهاك الخصوصية: جمع الأدلة الرقمية قد يستلزم الإطلاع على معلومات شخصية، مما يثير تساؤلات قانونية حول حماية حقوق الأفراد وعدم تعسف السلطات في استخدام هذه الأدلة.

° صعوبة الوصول إلى الأدلة: في بعض الأحيان، تكون الأدلة الرقمية مخزنة في خوادم خارج الدولة، مما يستلزم تعاونا دوليا للحصول عليها، وهو أمر قد يكون معقدا بسبب اختلاف القوانين بين الدول.

خلاصة الفصل

تخضع عملية ضبط الجرائم المعلوماتية للإجراءات الخاصة بالبحث والكشف عن الجرائم المعلوماتية لذلك تناولنا في هذا الفصل إجراءات البحث والكشف عن الأدلة الرقمية من طرف الأجهزة الأمنية على المستوى الدولي والمستوى الإقليمي، وكذلك إجراءات استخلاص الأدلة الرقمية كإجراء المعاينة، التفتيش والخبرة، على اعتبار أن البيئة التي ترتكب فيها جرائم المعلوماتية تختلف عن البيئة التي ترتكب فيها الجرائم التقليدية. أيضا بعض إجراءات البحث الخاصة كالتسرب و اعتراض المراسلات، أما فيما يخص إجراء الترصد الإلكتروني فقد تناولناه ضمن الإجراءات الواردة في القانون 09_04 حيث اصطلح عليه إجراء مراقبة الاتصالات

الإلكترونية، وتطرقنا أيضا إلى حجية الدليل الرقمي أمام القاضي الجزائي فتناولنا فيه سلطة القاضي الجزائي في تقدير الدليل الرقمي والتحديات القانونية في التعامل مع هذه الأدلة.

الخـــاتمـــــة

الخاتمة

من خلال دراستنا لموضوع وسائل إثبات الجريمة المعلوماتية في التشريع الجزائري فلا ريب أن هذه الجرائم من أكثر وأخطر الجرائم في الآونة الأخيرة حيث أنها بلغت حد الغزو وتهديد للمجتمعات، نظرا لكون الإثبات فيها صعب المنال، لاعتبار أدلتها رقمية خفية وغير مرئية.

ومن أبرز ما توصلنا إليه هو أن الجريمة المعلوماتية أحدثت تغييرا جذريا في النظرة العامة للجريمة ومازالت محل خلاف فقهي وقضائي بالنظر إلى قيمة المعلومات وطبيعتها غير المادية. وكذلك من حيث إجراءات التحقيق من التفتيش الذي قد يكون حتى عن بعد، وطبيعة الأدلة الناتجة عنها وتعديها للحدود الجغرافية ومدى شرعية الحصول على الأدلة الناتجة عنها والعمل بها ومدى كفاية النصوص التقليدية الموضوعية والإجرائية لمواجهتها خاصة في ظل الدول التي لازالت لم تعدل بعد قوانينها ولم تصدر بعد قوانين حديثة لمواجهتها.

وعليه نستنتج النتائج والتوصيات التالية:

أولا: نتائج الدراسة

-نظرا لحداثة الجريمة المعلوماتية لايوجد لحد الآن إجماع فقهي على تعريف موحد لها.

- المجرم المعلوماتي رجل يختلف عن المجرم التقليدي فهو رجل ذو علم وكفاءة ويتميز بقدرات عقلية وذهنية تمكنه من الإفلات من العقاب.

- هذه الجرائم لا تترك أثرا ماديا في مسرح الجريمة كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

بالرغم من التعديلات التي قامت بها الجزائر في مجال مكافحة الجريمة المعلوماتية إلا أن هذه النصوص تبقى غير كافية مقارنة بتطور الاحتراف الإجرامي المعلوماتي.

ثانيا: الإقتراحات

من خلال النتائج المتوصل إليها نقترح الإقتراحات الآتية:

– تنظيم حملات توعية قانونية وتقنية لفائدة المجتمع، تبرز خطورة الجريمة المعلوماتية وطرق الوقاية منها، مما يسهم في بناء بيئة رقمية آمنة.

– وجوب الاهتمام بتكوين الخبراء والمحققين والقضاة على التعامل مع الجرائم الإلكترونية.

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

– الاستثمار في التوعية بمخاطر الجرائم الإلكترونية والتنويه بأساليب المجرمين في ارتكابها عن طريق استغلال وسائل الإعلام المختلفة.

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

قائمة المصادر والمراجع

أولا: النصوص القانونية

أ.الدساتير

1. دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2020.

ب. القوانين والأوامر

1. القانون رقم 04-15 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

2. القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

3. القانون رقم 21-11 المؤرخ في 16 محرم 1443 الموافق 25 أوت 2021، الجريدة الرسمية للجمهورية الجزائرية العدد65.

ج. المراسيم الرئاسية

1. المرسوم الرئاسي 04-432 المتخصص بإعداد التقارير الفنية و التدريب و تطوير المعارف في مجال التحقيق الجنائي و التكنولوجيا.

2. المرسوم الرئاسي رقم 04-183.

3. المرسوم الرئاسي 18-140 المؤرخ في 21 مايو 2018 يتضمن التصديق على الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية ومفوضية الاتحاد الإفريقي المتعلق بمقر آلية الاتحاد الإفريقي للتعاون الشرطي (الأفريبول).

د. المراسيم التنفيذية

1. المرسوم التنفيذي رقم 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق.

هـ. القرارات الوزارية المشتركة

1. قرار وزاري مشترك مؤرخ في 2007/04/14 المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي.

ثانيا: الكتب

1. سحر سعد عبد السميع محمد، الحماية الجنائية للتوقيع الالكتروني، د.ر.ط، 2022، دار الفكر والقانون، مصر.

2. محمود سعد عبد المجيد، الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين و الأركان والعناصر المطبوعات الجامعية، الإسكندرية–مصر.

3. شنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية دراسة مقارنة، مؤسسة الكتاب القانوني، ابن النديم، الطبعة الأولى، ماي 2022، الجزائر.

4. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، د.ر.ط.د.س.ن، دار الجامعة الجديدة، الإسكندرية–مصر.

5. محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية، دراسة مقارنة، الطبعة الأولى، دار الفكر والقانون، 2015.

6. منصارة يوسف، الدليل الالكتروني في القانون الجزائي، الطريق إلى تحول أدلة الإثبات في المادة الجزائية دراسة مقارنة، د.ر.ط، دار الخلدونية، الجزائر، 2018.

7. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية، دار النشر، المكتب الجامعي الحديث المولى، 2012.

8. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دارهومة للطباعة والنشر، 2009.

9. عبد الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، القاهرة، 2007.

10. هلالي أحمد عبد الإله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2006.

11. علي حسن أحمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، عالم الكتب الحديث، اربط، الأردن، 2004.

12. مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت (دراسة مقارنة بين المراقبة الأمنية التقليدية و الالكترونية)، دار الكتب القانونية، مصر، 2005.

13. شحط عبد القادر العربي، الإثبات في المواد الجزائية في ضوء الفقه والاجتهاد القضائي، دار الهدى للنشر والتوزيع، الجزائر، 2006.

ثالثا: الأطاريح والمذكرات الجامعية

1. عبد القادر عميمر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم في القانون العام، تخصص القانون الجنائي، كلية الحقوق، جامعة الجزائر1(بن يوسف بن خدة). 2020.

2. د/ عائشة عبد الحميد، النظام القانوني للمنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مجال التعاون القضائي الشرطي، المجلة الأكاديمية للأبحاث والنشر العلمي، العدد11 ، دكتوراه علوم في القانون الدولي، علاقات دولية، جامعة الطارف، الجزائر2020.

3. براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.

4. نهلا عبد القادر المومني، ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع2008، الطبعة الأولى.

5. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة نيل شهادة الماستر، تخصص إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح، ورقلة، 2019.

6. الأستاذ سمير شعبان، الجريمة الالكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم، جامعة باتنة.

7. بن فريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي "دراسة مقارنة"، كلية الحقوق والعلوم السياسية، جامعة بجاية.

8. أوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي، مذكرة لنيل شهادة الماستر تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة.

9. فراحتية خلود، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة ماستر، تخصص قانون إعلام آلي وانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج.

10. شرقي نبيل، المنظمة الدولية للشرطة الجنائية، مذكرة لنيل الماستر في القانون تخصص، قانون، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2021/2020.

11. بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر مهني في الحقوق، تخصص: قانون الإعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022/2021.

12. يوسف الخليل العفيفي، الجرائم الالكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة"، مذكرة لنيل شهادة الماجستير في القانون العام، قسم القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، فلسطين 2013.

13. مدربل كريم، الإثبات بالدليل الرقمي في المسائل الجزائية، مذكرة الماستر كلية الحقوق، جامعة أكلي محند أولحاج، البويرة، 2019.

14. سهيل صليحة، سوسي فريدة، القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتعلقة بتكنولوجيات الإعلام والإتصال، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة البشير الإبراهيمي، برج بوعريريج، 2022/2021.

رابعا: المقالات والمجلات

1.سلطان سليمان الجداني، ماهية الدليل الرقمي، دراسة مقارنة، مجلة international journal of law and politicestudies

2. فاطمة زهرة بوعناد، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، الجزائر، 2013.

3. عبير بعقيقي/فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون09-04، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، المجلد09، العدد02، 2018.

4. عيدة بلعابد، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق، جامعة سعيدة، المجلد11، العدد1، 2019.

5.حمزة خضري/عشعاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد07، العدد02، 2020/06/05.

6.بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، المجلد14، العدد04، جامعة قسنطينة2، 2021/11/12.

7.د. بن مالك أحمد/د. الخال إبراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المركز الجامعي علي كافي تندوف، المجلد05، العدد1، 2021/10/10.

8. صابر بحري/منى خرموش، أهم السيكولوجية وراء الجريمة الالكترونية، مجلة دراسات في سيكولوجية الانحراف "مجلة دولية نصف سنوية"، 2021.

9. عبد العزيز لزعر/رشيد زياني، آلية الاتحاد الإفريقي للتعاون الشرطي(الأفريبول) ودورها في مكافحة الجريمة الالكترونية، مجلة متون، كلية الحقوق، جامعة مولاي الطاهر، سعيدة، المجلد14، العدد03، 2021.

10. الطاهر زخمي، الجرائم المعلوماتية في التشريع الجزائري وتدابير الوقاية منها، مجلة التشريع الإعلامي، المجلد02، العدد01، كلية علوم الإعلام والاتصال، جامعة الجزائر3، 2023/10/23.

11. أحمد فؤاد محمد سليمان، أهمية الدليل الرقمي في الإثبات الجنائي لجرائم الإيذاء الالكتروني، مجلة جامعة أسوان للعلوم الإنسانية، كلية الحقوق، المجلد4، العدد3، 2023.

12. عكوش حنان/خطوي مسعود، خصوصية الدليل الالكتروني، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الأغواط، المجلد7، العدد1، 2023.

13. بن عميور أمينة، بوحاليس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، مجلة البحوث في العقود وقانون الأعمال، جامعة الإخوة منتوري قسنطينة1 (الجزائر)، المجلد07، العدد02، 2022.

14. عون فاطمة الزهراء، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري–بالقطب الجزائي الوطني نموذجا– مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس، المجلد07، العدد02، 2022.

خامسا: المداخلات

1.د/بوقادوم.يحياوي صليحة، الإطار المفاهيمي للأدلة الجنائية الرقمية، مداخلة في ملتقى وطني بعنوان: إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال–الصعوبات والتحديات–، جامعة الجزائر1(بن يوسف بن خدة)، كلية الحقوق،17 أفريل2025.

2. ط.د/بوشارب هانية.ط.د/شبوعات موسى، الأجهزة الأمنية المختصة بالبحث والكشف عن الأدلة الرقمية في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، مداخلة في ملتقى وطني

بعنوان: إثبات الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال-الصعوبات والتحديات-جامعة الجزائر1(بن يوسف بن خدة)، كلية الحقوق،17 أفريل2025.

3. سماحي سمية، إثبات جنائي بالوسائل المستحدثة للجرائم(دليل رقمي)، مداخلة في ملتقى وطني بعنوان: الجرائم الالكترونية في المجتمع الجزائري تشخيص الوقائع وتحديات الأمن السيبرياني، كلية العلوم الإنسانية والاجتماعية، جامعة يحيى فارس المدية، 15مارس2022.

4. د.سويلم محمد/د.بوحادة محمد سعد، ضوابط اعتماد القاضي الدليل الرقمي في الإثبات، مداخلة في ملتقى وطني بعنوان: إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال-الصعوبات والتحديات-، كلية الحقوق، جامعة الجزائر1(بن يوسف بن خدة)، المنعقد يوم 17أفريل2025.

سادسا: المحاضرات

1.بوقطوشة وردة، محاضرات في الإثبات الجنائي، تخصص القانون الجنائي والعلوم الجنائية، جامعة جيجل، كلية الحقوق والعلوم السياسية، 2024/2023.

2. أ. حططاش عمر، محاضرات في مقياس الإثبات الجنائي، تخصص قانون جنائي، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، المسيلة.

3. د. بن دراح علي إبراهيم، محاضرات في مقياس الإثبات الجنائي، المركز الجامعي آفلو، معهد الحقوق والعلوم السياسية،2022/2021.

سابعا: المراجع الالكترونية

1. https://www.arab48.com

2. /https://me-en.kaspersky.com

3. /https://www.rakpolice.gov.ae

4. https://www.interpol.int/ar

5. file:///C:/Users/SAM/Downloads/01%20A%20Constitution_2023.pdf

6. https://www.aljazeera.net/encyclopedia/2016/2/1

الفهـــــرس

إهـــــداء.....

شكر وتقدير.....

قائمة الاختصارات.....

مقـــــدمة:.....[01]

الفصل الأول: الإطار المفاهيمي للإثبات الجنائي في الجرائم المعلوماتية.....[04]

تمهيد:.....[05]

المبـــحث الأول: ماهية الإثبات الجنائي.....**[06]**

المطـلب الأول: مفهوم الإثبات الجنائي و قواعده الإجرائية.....**[06]**

الفـرع الأول: تعريف الإثبات الجنائي.....**[06]**

الفـرع الثـاني: أنظمة الإثبات الجنائي و قواعده النظامية.....**[08]**

المطلب الثاني: مفهوم الجرائم المعلوماتية .....**[10]**

الفــرع الأول: تعريف الجريمة المعلوماتية و خصائصها.....**[11]**

الفـرع الثـاني: دوافع ارتكاب الجريمة المعلوماتية و طبيعتها القانونية.....**[22]**

المبحث الثاني: الأدلة الجنائية الرقمية.....**[27]**

المطـلب الأول: مفهوم الأدلة الجنائية و أهميتها في الجرائم المعلوماتية.....**[27]**

الفـرع الأول: تعريف الدليل الجنائي الرقمي.....**[27]**

الفرع الثاني: أنواع و تقسيمات الدليل الرقمي .....**[29]**

المطلب الثاني: أهمية الدليل الرقمي و صعوبة استخلاصه.....**[31]**

الفـرع الأول: أهمية الدليل الرقمي في إثبات الجريمة المعلوماتية.....**[31]**

الفـرع الثاني: صعوبة استخلاص الدليل الرقمي.....**[32]**

خلاصة الفصل:.....[34]

الفصل الثاني: اجراءات البحث والكشف عن الادلة الرقمية في الجرائم المعلوماتية.....[35]

تمهيد:.....**[36]**

المبحث الأول: الإجراءات الخاصة بالبحث و الكشف عن الأدلة الرقمية..... **[37]**

المطلب الاول: إجراءات البحث والكشف عن الدليل الرقمي من طرف الأجهزة الأمنية **[37]**

الفـرع الأول: على المستوى الدولي.....**[37]**

الفـرع الثاني: على المستوى الإقليمي.....**[41]**

الفـرع الثـالث: القطب الجزائي المستحدث..... **[46]**

المطلب الثاني: إجراءات استخلاص الدليل الرقمي للكشف عن الجرائم المعلوماتية.....**[49]**

الفـرع الأول: الإجراءات التقليدية لاستخلاص الدليل الرقمي.....**[49]**

الفـرع الثاني: الإجراءات الحديثة لاستخلاص الدليل الرقمي.....**[55]**

المبـــحث الثانـــي: حجية الدليل الرقمي أمام القاضي الجزائي.....**[58]**

المطـلب الأول: سلطة القاضي الجزائي في تقدير الدليل الرقمي.....**[58]**

المطلب الثاني: التحديات القانونية في التعامل مع الأدلة الرقمية.....**[60]**

ملخص الفصل:.....**[62]**

الخـــــــاتمة:.....**[65]**

قائمة المصادر والمراجع:.....**[68]**

الفـــــهرس:.....**[75]**

الملخص العام:.....**[78]**

ملخص

يشهد العالم في عصرنا الجاري تقدما عظيما، في مجال المعلوماتية باتت الدول معها تتسارع إلى استخدام التقنية في جميع المجالات، وبقدر ما يحققه تطور التقنيات من فوائد كبيرة في مجال الرقي والتقدم الإنساني فإنها في الوقت ذاته مهدت السبيل إلى بروز أشكال جديدة من الجرائم الالكترونية.

وأصبح هذا النوع المستحدث من الجرائم الالكترونية يرتكب في وسط افتراضي غير متعارف عليه، ولا يشبه الوسط التقليدي للجرائم التقليدية، حيث وجد المجرم تقنية عالية وأساليب حديثة تساعده في ارتكاب العديد من الجرائم دون أن يترك أثرا واضحا لتلك الجرائم.

ولقد قمنا باختيار هذا الموضوع نظرا لأهميته البالغة، فكلما تطورت الوسائل الالكترونية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم، وهذا ما شكل عائقا أمام القائمين على البحث واثبات الجرائم الالكترونية، حيث أن قواعد البحث والتحقيق وأسس الإثبات الجنائي في القوانين التقليدية لا تكفي، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلاءم مع طبيعتها الفنية، لذلك ألقينا الضوء على هذا الموضوع وذلك من خلال: تعريف الجريمة الالكترونية وكذلك وسائل إثباتها وإلقاء الضوء على إجراءات البحث والكشف عن الأدلة الرقمية في الجرائم المعلوماتية وأخيرا حجية الدليل الرقمي أمام القاضي الجزائي.

الكلمات المفتاحية: الجريمة الالكترونية، الأدلة الرقمية، القاضي الجزائي، الإثبات الجنائي، وسائل إثبات الجريمة المعلوماتية.

Abstract

The world is witnessing great progress in the field of information and communications, with which countries are accelerating the use of technology in all fields, and as much as the development of technologies achieves great benefits in the field of advancement and human progress, at the same time it has paved the way for the emergence of new forms of crimes.

This new type of cybercrime has become committed in an unrecognized virtual medium, and does not resemble the traditionalmedium of traditional crimes, where the criminal found high technology and modern methods that help him commit many crimes withoutleaving a clear trace of those crimes.

We have chosen this topic because of its great importance, the mire electronic means develop, the more the method of committing this type of crimes develops, and this is what constituted an obstacle for those in charge research and proof of electronic crimes, as the rules of research and investigation and the foundations of criminal evidence in traditional laws are not enough, but this type of crime needs to develop new legislation that suits its technical nature.

For all that, I saw shedding light on this topic through: the definition of cybercrime and means of proving it, shedding light on the procedures for searching and discovering digital evidence in cybercrimes, and finally the admissibility of digital evidence before criminal judges.

Keywords: cybercrime, digital evidence, criminal judge, criminal evidence, means of proving cybercrime.