وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون إعلام آلي وأنترنت

الموسومة بـ

# خصوصية الجريمة المعلوماتية في ظل التشريع الجزائري

إعداد الطالبتين:

- بن زروق ريان
- بلحاج سهى

إشراف الدكتور:

* هدفي العيد

لجنة المناقشة :

| الاسم و اللقب | الرتبة | الصفة |
|---|---|---|
| رفاف لخضر | أستاذ محاضر – أ – | رئيسا |
| هدفي العيد | أستاذ التعليم العالي | مشرفا |
| بن نوي خالد | أستاذ محاضر – أ – | ممتحنا |

السنة الجامعية 2024/2023

الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

# إذن بالإيـــداع

أنا الممضي أسفله الأستاذ : ..... حمدي العيد .....

الرتبة : ..... أستاذ تعليم العالي .....

المشرف على مذكرة الماستر الموسومة بـ : ..... خصوصية الجرائم المعلوماتية .....

..... في ظل التشريع الجزائري .....

من إعـــداد :

الطالب الأول : ..... بن زروق وليانا .....

الطالب الثاني : ..... بلحاج يسمين .....

**أوافق على إيداع الطالب (الطالبين) لمذكرة التخرج لدى الإدارة من أجل برمجتها للمناقشة.**

إمضاء الأستاذ المشرف

* 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

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): بن زروق ريان الصفة: طالب، أستاذ، باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم 118455178 والصادرة بتاريخ 13 ماي 2019

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم قانون إعلام آلي وأنترنت

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

عنوانها: خصوصية الجرائم المعلوماتية في التشريع الجزائري

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

التاريخ: 2024/06/15

بن زروق ريان

118455178

توقيع المعني (ة)

2024 جوان 04

* 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

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): بلحاج سهى الصفة: طالب، أستاذ، باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم 118756454 والصادرة بتاريخ 2024.03.23

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم قانون الاعلام والانترنت

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

عنوانها: جريمة الجرائم المعلوماتية في ظل التشريع الجزائري

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

التاريخ: 2024/06/05

توقيع المعني (ة)

2024 جوان 04

رئيس المجلس الشعبي البلدي

ضابط الحالة المدنية


بسم الله الرحمن الرحيم

# الشكر والتقدير

قال تعالى: "وَلَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ".

الحمد لله على توفيقه وإحسانه، والحمد لله على فضله وإنعامه، والحمد لله على وجوده وإكرامه، الحمد لله حمدا يوافي نعمه ويكافئ مزيده.

الحمد لله الذي أنعم علينا بنعمة العلم، نشكر الله عز وجل الذي مكننا من تخطي المصاعب وإعانتنا على إتمام هذا العمل على أحسن حال، الحمد لله الذي هدانا لهذا والصلاة والسلام على خير الأنام رسول الله.

"لا يشكر الله من لا يشكر الناس"

نتقدم بجزيل الشكر والتقدير للدكتور المشرف على هذه المذكرة "**هدفي العيد**" على ما أولانا به من اهتمام ونصح وإرشاد، فجزاه الله خير ما جزى به أستاذا عن طالبه.

كما لا يفوتنا أن نشكر اللجنة الموقرة على مناقشة هذا العمل وتقييمهم لمجهوداتنا.

كما أتقدم بفائق الاحترام والتقدير إلى كل الأساتذة وكل الأسرة الجامعية في كلية الحقوق والعلوم السياسة بجامعة محمد البشير الإبراهيمي جامعة برج بوعريريج.

**الله ولي التوفيق**

الإهداء

"فرحين بما آتاهم الله من فضله"

الحمد لله حبا وشكرا وامتنانا على البدء والختام، ها أنا أخطو خطوات تخرجي، نعم بعد عناء طويل وبعد تعب وجهد، لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون، وبعد سنوات طويلة دامت 5 سنوات أو بالأحرى 17 سنة من الدراسة، ها أنا أتخرج، ها أنا اليوم أهدي نجاحي إلى كل من سعى معي بإتمام هذه المسيرة:

* إلى الأموات، الأحياء في القلب، إلى حبيبتي النائمة تحت التراب، اعتدت جميع الغائبين إلا غيابك، رحم الله روحا كانت كالجنة على الأرض، اللهم إن جدتي كانت نوري فلا تطفئ نور قبرها، كانت نعيمي فلا تحرمها لذة نعيمك، أول خريجة في أحفادها: جدتي لويزة رحمها الله

* إلى نبض قلبي الذي به أحيا، إلى القلب الذي يحمل حزني وفرحتي، إلى من كان دعائها سر نجاحي، إلى ملكتي التي كانت السند والعوض كانت لي الأم والأب، داعمتي الأولى، شكرا إلى من هي في الحياة حياة، أرجو من الله أن يطيل في عمرك لتري ثمارا قد حان قطفها بعد طول انتظار، فأدامك الله سندا لنا ومتعك بالصحة والعافية: أمي الغالية

* إلى من كانت يداه مبسوطتان لتربيتي وتعليمي ولنجاحي ولسعادتي وحمايتي، رمز الاجتهاد والكفاح ومعتمدي في الحياة بعد الله، الأخ الحنون على أخته فليحفظ الله قلبك ويحميك من كل شر ومكروه ورزقك من حيث لا تحسب، إلى من شد عضدي به فكان ضلعا وسندا لا يميل: أخي هشام

* إلى مصدر قوتي، الداعمين الساندين، أرضي الصلبة وجداري المتين، إلى من مدت أياديهم في أوقات الضعف، إلى شبهات نبع الحنان، أخواتي: دنيا، لامية، آلاء

* إلى من ساندني بكل حب عند ضعفي، إلى صديقات المواقف والسنين شريكات الدرب الطويل، إلى رفاق الخطوة الأولى: دنيا، منال، عبير، آية, سلمى.

والخطوة ما قبل الأخيرة: سمى و رحاب ، إلى من كانوا خلال السنين العجاف سحابا ممطرا، أنا ممتنة

* إلى تلك التي لو تلدها أمي ولكن كانت أقرب من أي شخص لي: رانيا ولمى

اللهم إنه ليس جهدي واجتهادي إنما بتوفيقك وكرمك وفضلك، فمن قال أنا لها نالها، فأنا لها وإن أبت أتيت بها رغما عنها، واليوم أخطو خطوتي برفق وطمأنينة بعد أن ركضت لوقت طويل خوفا من أن يفوتني شيئا ثم أدركت أنه لن يفوتني شيء قد كتبه الله لي.

"و آخر دعواهم أن الحمد لله رب العالمين"

ريان بن زروق

# إهداء

بسم الله الرحمن الرحيم

"وآخر دعواهم أن الحمدُ للهِ رَبِّ العالَمين"

ما سلكنا البدايات إلا بتيسيره وما بلغنا النهايات إلا بتوفيقه وما حققنا الغايات إلا بفضله فالحمد لله الذي وفقنا لذلك وما كنا عليه بقادرين.

فبكل الحب والتقدير، أقدم هذا الإهداء إلى من كان لهم التقدير الأكبر في حياتي إلى من دعموني في رحلتي الطويلة نحو تحقيق الحلم.

* إلى صاحب السيرة العطرة، إلى الرجل الأبرز في حياتي، إلى من كلله الله بالهيبة والوقار، إلى من أحمل اسمه بكل افتخار، طاب بك العمر يا سيد الرجال وطبت لي عمدا يا أبي الغالي، أرجوا من الله أن يمد عمرك لترى ثمارا قد حان قطافها بعد طول انتظار، فأدامك الله سندا لنا ومتعك بالصحة والعافية.

* إلى سمة الحياة وسر الوجود، إلى من جعل الجنة تحت قدميها، إلى الإنسانة العظيمة التي أستمد منها القوة، إلى الملاك الطاهر وداعمتي الأولى التي لولا تضحياتها لما كنت على ما أنا اليوم، ممتنة لأن الله اصطفاك لي من البشر أمًا يا خير سند وعوض، شكرا على كل شيء يا أعظم أم. أغلى خلق الله "أمي الغالية" متعها الله بالصحة والعافية.

* إلى خلعي الثابت الذي لا يميل، إلى من رزقت به سندا إلى من مد لي يديه في أوقات الضعف، إلى من شد الله به عضدي فكان خير معين "أخي وليد".

* إلى ملائكة رزقني الله بهن، إلى من آمنوا بقدراتي، إلى الأرواح الصافية لقد كنتن مساندتي في كل محنة، وسأظل ممتنة لكن دائما، أشكر الله على وجودكن في حياتي، حبيباتي الغاليات: "أسماء ، رحيمة ، مريم".

* إلى النجوم اللامعة، وإلى الأرواح الجميلة، إلى من هم أقرب إلى من روحي وكن دائما موقع اتكاء صديقات العمر: "هديل ، رحاب ، روميساء ، خولة ، دعاء ، سارة".

* إلى شريكاتي في رحلة العلم، إلى الصديقات الوفيات: "شيماء ، رشيدة".

* إلى الأجمل والأحسن حبيبة مشاركتي في هذا العمل: "ريان".

* إلى العوض الجميل، والذي كان دائما عونا لي، إلى الروح التي جعلت كل لحظة تجمعنا مميزة، دمت لي سندا وشريكا مخلصا: "هشام" حفظك الله، وجزاك الله خير الجزاء.

شكرا لكم جميعا

سمى بلطاج

## قائمة المختصرات:

| الكلمة | المختصرات |
|---|---|
| ق.إ.ج | قانون الإجراءات الجزائية |
| ص | الصفحة |
| ق.ع | قانون العقوبات |
| ج.ر | الجريدة الرسمية |
| د.ط | دون طبعة |
| ط | الطبعة |

# مقدمة

**مقدمة:**

لقد ساهمت التكنولوجيا الحديثة في ظهور عصر جديد وإحداث تغيرات جوهرية في مختلف المجالات وتعزيز الانفتاح بلا حدود على العالم من خلال تقصير المسافة والتواصل بين الناس والمؤسسات ربحا للوقت والجهد وتسريع عملية تبادل المعلومات وتداولها على نطاق واسع دون التنقل، بحيث يصبح العالم قرية صغيرة مع تسهيل التعامل والتواصل فيها باستمرار، وهذا ما أدى إلى ثورة تكنولوجية معلوماتية، مما فتحت آفاقا جديدة في العديد من المجالات: اقتصادية، اجتماعية، وتجارية، حيث تستخدم تقنيات متطورة تدفع إلى إحداث تحولات وتغيرات مستمرة في مختلف جوانب الحياة، ولذلك حاول العالم التصدي لهذه الظاهرة من خلال سن تشريعات قانونية محلية.

وفي ظل هذه التطورات للمعلومات والاتصالات أصبحت الجرائم الإلكترونية تهدد العالم بما في ذلك الجزائر، ومع تزايد الاعتماد على الأنترنت والتقنيات الرقمية أصبحت الجزائر عرضة لمجموعة واسعة من الجرائم المعلوماتية ولقد حذى المشرع الجزائري حذوى لمواجهة هذه الجرائم من خلال وضع إطار قانوني يهدف إلى تنظيم ومكافحة هذه الأخيرة، تتضمن هذه التشريعات قوانين خاصة بتكنولوجيا الإعلام والاتصال بالإضافة إلى إجراءات وقائية وعقابية تهدف لحماية البيانات الشخصية والأمن السيبراني، وتتطلب هذه الجرائم جهود لتحديث القوانين بشكل مستمر لمواكبة التطورات التكنولوجية الشريعة ونشر الوعي الثقافي حول مخاطر الجرائم المعلوماتية وسبل الوقاية منها.

ويمكننا تعريف هذه الجرائم بأنها كل نشاط أو دخول غير مصرح به إلى الشبكة الخاصة، أو التلاعب أو إتلاف أو محو البيانات الرقمية الواردة فيها أو جميع الإجراءات الغير مصرح بها حول المعالجة الآلية للمعطيات.

**الإشكالية:** ولتناول هذا الموضوع طرحنا الإشكالية فحواها كالآتي:

- **ما مدى خصوصية الجريمة المعلوماتية في ظل التشريع الجزائري؟**

ومن هنا نطرح عدة تساؤلات فرعية تتمثل في:

– ما المقصود بالجرائم المعلوماتية؟

– ما هي أهم العناصر المتطلبة للتحقيق في الجرائم المعلوماتية؟

– إلى أي مدى يتم الاعتداء على الحق في الخصوصية المعلوماتية؟

– ما هي قواعد الاختصاص القضائي في الجرائم المعلوماتية؟

– فيما تتمثل الآليات المتخصصة في التحقيق والإثبات في الجرائم المعلوماتية؟

**أسباب اختيار الموضوع:**

*** الأسباب الذاتية:**

– الاهتمام بكل ما هو جديد في تكنولوجيا الإعلام والاتصال وكذلك رغبتي في دراسة والإطلاع على مجال الجرائم الالكترونية وآليات التحقيق.

– الميول الشخصية الذي يتعلق بالفضاء الالكتروني ومعرفة الجرائم التي تتعلق بهذا الفضاء كوننا في عصر الثورة المعلوماتية.

*** الأسباب الموضوعية:**

– لحداثة الموضوع والتطورات والتغيرات التي أدخلتها التكنولوجيا الحديثة على النظام القانوني، وتعميق المعرفة بمجال التحقيق في الجرائم المعلوماتية ومعالجته من خلال إبراز أهم مميزاته يشمل هذا النوع من الجرائم على أهم عناصر وأساليب التحقيق في الجريمة المعلوماتية ودور الجهات المختصة في حسن سيرها وأهم الإجراءات وآليات التعاون الدولي في التحقيق في هذه الجرائم....

– قلة الدراسات التي تناولت الجانب الخاص بالاختصاص القضائي للجرائم الإلكترونية والقانون الواجب التطبيق.

*** أهمية الموضوع :**

من وجهة نظرنا العلمية سيشار إلى أهمية موضوعنا من خلال:

1- حداثته لأنه يتعلق بالجريمة في البحث الأكاديمي الحديث والتحليل القانوني لا يزال النص القانوني مقسما إلى قسمين.

2- تثير القضايا الموضوعية والإجرائية العديد من الأسئلة التي تتطلب المناقشة والبحث العلمي.

3- تسعى هذه الدراسة إلى تسليط الضوء على طبيعة الجريمة المعلوماتية وخصوصيتها وكذا الآليات المعتمدة في التشريع الجزائري لمكافحتها.

4- تتطلب الجريمة المعلوماتية دراسة تفاصيلها المتعلقة بجرائم الأنترنت كأساس لموضوعات التحقيق الجديدة وعناصر التحقيق الفردية والآليات القانونية والتقنية.

5- تحتل هذه القضية أيضا مكانا مهما جدا في العمل ودراسة الجهاز بطريقة متكاملة ومنسقة للحصول على الأدلة وتأمينها من التلف أو الضياع أو المحو واستخدام طرق وأساليب محددة للوصول إلى مرتكبي الجرائم المعلوماتية ومنعهم من الإفلات من العقاب.

6- تكمن أهمية دراسة موضوعنا أيضا لمنع انتشار الجريمة الإلكترونية عبر الحدود.

- **أهداف الموضوع:**

**تهدف هذه الدراسة إلى:**

1- تحديد طبيعة وخصوصية الجريمة المعلوماتية وكيفية تعامل المشرع الجزائري معها.

2- محاولة التعامل مع الأنواع الجديدة من أنماط الجريمة المعلوماتية المستحدثة والمعقدة لانعكاساتها على جميع المجالات.

3- تسعى هذه الدراسة إلى تحقيق الهدف الرئيسي المتمثل في توفير البحث الذي يرصد الجوانب المختلفة لظواهر إجرامية معلوماتية من الناحية الموضوعية والإجرائية.

4- اتخاذ خطوات فعالة في المجال التشريعي لمكافحة الجرائم المعلوماتية.

5- الاعتماد على بعض القوانين الخاصة الجديدة وإجراء بعض التعديلات على قانون العقوبات وقانون الإجراءات الجزائية وبعض القوانين الخاصة لملئ الفراغ القانوني في هذا المجال.

- **المنهج المتبع:**

بالنظر إلى طبيعة الموضوع وخصوصيته، فقد اعتمدنا على المنهج التحليلي الذي يهدف إلى بيان مفهوم الجريمة المعلوماتية وأهم عناصرها، بالإضافة إلى التطرق إلى خصوصية الجرائم المعلوماتية ودراسة الجوانب الإجرائية الخاصة بها.

بالإضافة إلى المنهج الاستقرائي تم التطرق إلى بعض القوانين والنصوص القانونية مدعمة للمنهج الوصفي التحليلي.

- **تقسيم الموضوع:**

وللإجابة على الإشكالية ارتأينا اعتماد خطة ثنائية متوازنة مقسمة إلى فصلين على أن يتضمن كل فصل مبحثين.

حيث تناولنا في الفصل الأول المعنون **بماهية خصوصية الجرائم المعلوماتية** والذي من خلاله تم التطرق إلى مبحثين: المبحث الأول يخص ماهية الجرائم المعلوماتية، أما المبحث الثاني خاص بالحق في الخصوصية.

أما في الفصل الثاني خصصناه لخصوصية الجرائم المعلوماتية على المستوى الإجرائي، تناولنا في المبحث الأول: إجراءات التحقيق في الجرائم المعلوماتية، أما المبحث الثاني فتناولنا فيه الآليات المتخصصة في التحقيق والإثبات في الجرائم المعلوماتية.

# الفصل الأول:

# ماهية خصوصية الجرائم المعلوماتية

## الفصل الأول: ماهية خصوصية الجرائم المعلوماتية.

الجرائم المعلوماتية التي تعرف أيضا بما يسمى الجرائم السيبرانية التي تشمل أفعالا مبتكرة تتمثل في الأعمال التي تستخدم فيها أجهزة الكمبيوتر أو أي جهاز متصل بالشبكة بهدف الوصول إلى المعلومات والبيانات بطريقة غير شرعية أو إلحاق الضرر بالأجهزة او إتلافها، ويعتبر الدافع الأساسي لهذه الجرائم هو تحقيق المصلحة الشخصية.

وسنتطرق في هذا الفصل إلى كل ما يخص الجريمة المعلوماتية بحيث قسمناه إلى ما يلي:

**تناولنا في المبحث الأول: ماهية الجرائم المعلوماتية.**

**والمبحث الثاني: الحق في الخصوصية المعلوماتية.**

## المبحث الأول: ماهية الجرائم المعلوماتية.

أثار مفهوم الجريمة المعلوماتية الكثير من التساؤلات والغموض بسب تطورها وحداثتها، مما انعكس ذلك على تحديد تسمية موحدة ودقيقة لهذه الجرائم، فتعددت التسميات التي أطلقت عليها "جرائم الكومبيوتر، "جرائم الاتصالات الإلكترونية" وغيرها [1]، فذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب مختلفة ووضعوا تعاريف متعددة فبالتالي لا نجد تعريفا موحدا للجريمة المعلوماتية، كما أن التطور المستمر لتكنولوجيا المعلومات والاتصالات حال دون ذلك إلى وضع تعريف شامل، فالبعض من الفقهاء وسع من مفهوم الجريمة المعلوماتية والبعض منها ضيق فيه، لذا ستتطرق إلى تعريف الجريمة المعلوماتية وموقف المشرع الجزائري منها.

### المطلب الأول: مفهوم الجريمة المعلوماتية .

يتكون مصطلح "الجريمة المعلوماتية" من كلمتين هما: الجريمة، المعلوماتية، فمصطلح "المعلوماتية" هو العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها وتخزينها واسترجاعها عند الحاجة وكذلك تحويلها واستخدامها. [2]

#### الفرع الأول: تعريف الجريمة المعلوماتية وموقف المشرع منها .

وسنتطرق في هذا الفرع إلى تعريف الجريمة المعلوماتية بشقيها التعريف الضيق والموسع وموقف المشرع الجزائري منها.

**أولا: التعريف الفقهي للجريمة المعلوماتية .**

**1- التعريف الموسع:** كل سلوك إجرامي يتم بمساعدة الكومبيوتر، أو كل سلوك غير مشروع أو غير أخلاقي غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها. [3]

---

[1] بن مالك أحمد، خصوصية الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 8، العدد 1، الجزائر، سنة 2023، ص 946.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية، 2006، ص 87.

[3] إبراهيم ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، ط 1، سنة 2009، ص 74.

وقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، وعرف الجريمة المعلوماتية على أنها "جريمة يمكن ارتكابها بواسطة نظام معلوماتي أو شبكة معلوماتية وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي ترتكب في فضاء معلوماتي".[1]

وقد توسع الخبير الأمريكي " Poker " في تعريف الجريمة المعلوماتية، واعتبارها: "كل فعل إجرامي معتمد في بيئة رقمية، تلحق ضررا بالمجني عليه مع كسب يحققه الفاعل".

وعليه فإن أنصار هذا الإتحاد، أكدوا أن العامل الرئيسي لارتكاب الجريمة هو "الكمبيوتر" فيعتمدون عليهم في تعريف الجريمة المعلوماتية "فهو كل سلوك إجرامي يقوم به الفاعل بواسطة الحاسب الآلي أو جهاز الكمبيوتر".[2]

**2- التعريف الضيق:** أما أنصار الاتجاه الضيق فعرفوا الجريمة المعلوماتية على أنها: "كل فعل غير مشروع يكون بجهاز الحاسب الآلي بقدر كبير لازما لارتكابه من ناحية وملاحقتها من ناحية أخرى".

ويعرف الفقيه الفرنسي " Mass " جريمة الكمبيوتر على أنها: "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح" [3]. وجرائم الكمبيوتر لدى هذا الفقيه تعتبر جرائم خاصة بالأموال فمن خلال هذا التعريف تم الجمع بمعيارين هما "الوسيلة والهدف تحقيق الربح "، المستمد من محل الجريمة المتمثل في الأموال.

ومن خلال التعاريف السابقة نلاحظ أن مفهوم الجريمة المعلوماتية مرتبط إما بموضوع الجريمة أو وسيلة ارتكابها أو على فاعلها.

ويلاحظ على هذه التعاريف أنها ضيقت مفهوم الجريمة المعلوماتية حيث جاءت كلها قاصرة على ظاهرة الإجرام الالكتروني مع الاختلاف في المعيار المعتمد في ارتكاب

[1] مؤتمر فيينا في الفترة من 17/10 نيسان 2000.

[2] زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى، عين مليلة الجزائر ، 2011، ص 42.

[3] إبراهيمي سهام، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2004-2007، ص 7.

الجريمة، بالإضافة إلى حصر مفهوم الجريمة المعلوماتية والتوجه إلى المفهوم الضيق. مما قد لا يسعف في التوصل إلى تعريف شامل وجامع.

**ثانيا: موقف المشرع الجزائري.**

لم يتطرق المشرع الجزائري إلى تعريف الجريمة المعلوماتية في قانون العقوبات، بحيث اكتفى ببعض الأفعال التي تشكل جرائم الأنترنت، في المواد من 394 مكرر إلى394 مكرر 7 تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات".[1]

غير أن المشرع الجزائري اعتمد في تسمية الجرائم المعلوماتية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب المادة 2 من قانون 04/09 على أنها "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية" [2]. وعليه فإن مفهوم الجريمة المعلوماتية في التشريع الجزائري لم يعد مقتصرا فقط على الأفعال التي تكون فيها منظومة معلوماتية هي الوسيلة لارتكابها. [3]

ومن استقراء نص المادة 2 من قانون 04/09، فإن المشرع الجزائري اعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية بين النظام الخاص بالاتصالات الالكترونية والمساس بالأنظمة المعالجة الآلية للمعطيات، والقانون الواجب التطبيق للجريمة المنصوص عليها في قانون العقوبات.

---

[1] القانون 15/04 المؤرخ في 2004/11/10، يعدل ويتمم الأمر 155/66، المؤرخ في 1966/6/08، المتضمن قانون العقوبات، الجريدة الرسمية الجزائر ، العدد 71، سنة 2004.

[2] نص المادة 2 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، 16 أوت 2009.

[3] بوحادي صليحة، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص، جامعة حسيبة بن بوعلي الشلف الجزائر ، المجلد 7، العدد 1، سنة 2021، ص 2530.

كذلك لم يتطرق إلى مفهوم الجريمة المعلوماتية في القانون 05/18 المتعلق بالتجارة الإلكترونية [1]، رغم أنه تطرق إلى بعض الجرائم الإلكترونية والعقوبات المقررة لها، والفصل فيها في الفصل الثاني من الباب الثالث، تحت عنوان "الجرائم والعقوبات".

**الفرع الثاني: طبيعة الجريمة المعلوماتية .**

على اعتبار أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة إلى بروز أشكال جديدة من الإجراء، دفع ذلك بالتشريعات الجنائية إلى النص على معاقبة هذا النوع من الجرائم، يهدف توفير الحماية الجزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، فقام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون 15/04 مستعملا في ذلك التسمية التي سبق ذكرها أي "المساس بأنظمة المعالجة الآلية للمعطيات".

وقدر المشرع من خلال هذا التعديل أن جوهر المعلوماتية هي المعطيات التي تدخل إلى الحاسوب فتحولها إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من عدة زوايا [2]، وبصدور القانون رقم 09-04 السابق الذكر عبر المشرع الجزائري على الجريمة المعلوماتية بتسمية "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال".

وما يلاحظ في هذا الشأن أن المشرع الجزائري لم يستقر على تسمية واحدة حيث اعتمد على تسميات مختلفة بين قانون العقوبات والقوانين المكملة في المجال الجنائي فسماها جريمة المساس بأنظمة المعالجة الآلية للمعطيات في القانون رقم 04-15 في حين أعطاها تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في القانون 09-04 ورغم هذا الاختلاف فإن هاتين التسميتين وغيرها من التسميات الأخرى تصب في هدف واحد وهو مجابهة الجريمة الالكترونية.

[1] القانون 05/18 المؤرخ في 2018/5/10، المتعلق بالتجارة إ، الجريدة الرسمية الجزائر ، العدد 28، ص 2018.

[2] عشاش حمزة، خضري حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة المجلد 06، العدد 02 جوان 2020، ص 172.

فمن حيث التكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة إذا لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، وتطبيق النصوص التقليدية على الجرائم المعلوماتية يثير العديد من المشاكل والتي في مقدمتها صعوبة إيجاد دليل مادي يدين مرتكب الجريمة. [1]

أما عن محل الجريمة المعلوماتية فيتميز عن محل الجريمة التقليدية، فمحل الجريمة الأولى هو المال المعلوماتي تمييزا لمالية المغايرة للمال التقليدي في الجريمة الثانية بكل مكوناته، فالجريمة المعلوماتية تشمل كل من أفعال السرقة أو التغيير و حذف المعلومات مثل النشاط الإجرامي الذي يستهدف اختراق البريد الالكتروني والعبث بمحتوياته والذي يحمل في طياته انتهاك الخصوصية وحقوق الملكية الفكرية وأنماط جريمة أخرى. [2]

**الفرع الثالث: أسباب ارتكاب الجريمة المعلوماتية .**

الدافع الباعث أو الغاية تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة [3]، فالدافع لا يعتبر عنصرا من عناصر الجريمة إلا في الأحوال التي يحددها القانون، فالجريمة تقوم بتحقق عناصرها و أركانها أيا كان الباعث من وراء ارتكابها فمن بين الدوافع التي تدفع بالمجرم الالكتروني إلى ارتكاب جريمته تتنوع ومن أهمها:

**أولا: الدوافع المادية .**

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل، وهي من بين أكثر الدوافع لاقتراف الجريمة المعلوماتية [4]، ويتم اللجوء لارتكاب هذه الجريمة إما عن طريق

---

[1] بوضياف إسماهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، العدد 11، سبتمبر 2018، ص 352-353.

[2] عشاش حمزة، خضري خضرة، المرجع السابق، ص 173.

[3] خالد دوادي، الجريمة المعلوماتية، ط1، دار الإعصار العلمي، الجزائر، سنة 2018، ص 37.

[4] نهلا عبد القادر المومني، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، ط2، دار الثقافة، سنة 2010، ص 90.

المساومة على البرامج أو المعلومات المتحصلة عليها عن طريق الاختلاس من جهاز الحاسوب.

**ثانيا: الدوافع الشخصية .**

الرغبة في التعلم يكرس مرتكبو هذه الجريمة وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية، وهناك من يرتكب جرائم الحاسوب بغية الحصول على الجديد من المعلومات، وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم. [1]

**ثالثا: الدوافع الذهنية أو النمطية .**

غالبا ما يكون الدافع لدى مرتكب الجرائم المعلوماتية هو الرغبة في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية دون أن تكون لهم نوايا خبيثة. ويرجع ذلك لوجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم [2]، بحيث يظهر المجرم المعلوماتية قدراته وتميزه في المجال الالكتروني، وإرادتهم في التفوق على كل الأنظمة المعلوماتية المستحدثة، وغالبا ما يتم استدراج هذه الفئة من الشباب واستمالتهم للقيام ببعض الجرائم المعلوماتية. [3]

**رابعا: دافع الانتقام وإلحاق الضرر.**

تعد من أخطر الدوافع التي يمكن أن تنفع شخص يملك معلومات كبيرة عن مؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته، ويقصد به الدافع الذي يدفع الأفراد في

[1] نهلا عبد القادر المومني، المرجع نفسه، ص 90.

[2] خالد داودي، المرجع السابق، ص 39.

[3] سفيان سوير، الجرائم المعلوماتية، مذكرة شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011/2010، ص 28.

الانتقام، فهو من أخطر الدوافع المتعلقة في ارتكاب الجرائم المعلوماتية وتزيد خطورتها عندما يمتلك هؤلاء الأفراد معلومات كبيرة عن شركات أو مؤسسات معينة. [1]

**خامسا: الدوافع السياسية .**

ويقصد بذلك قيام الأفراد بارتكاب الجرائم المعلوماتية، بهدف تلفيق الأخبار والمعلومات أو حتى الاستناد إلى أجزاء بسيطة من الحقيقة، وبالتالي يتم نسخ الأخبار الملفقة وتتم هذه الجرائم في المواقع السياسية المعادية للحكومات، مع أهمية التركيز على قدراتهم في إبراز المحاولات الدولية لاختراق الشبكات الحكومية في مختلف أنحاء العالم .

**سادسا: الدوافع الأخرى.**

تعتبر الدوافع السابقة التي تم تناولها ليست الأسباب الوحيدة لارتكاب الجريمة المعلوماتية بل هناك العديد ومثال ذلك: مناهضة العولمة التي تعتبر أهم الدوافع لارتكاب جريمة معلوماتية حيث تم اختراق النظام المعلوماتي الاقتصادي العالمي في سويسرا، وتمت سرقة المعلومات التي تتعلق بالشخصيات الثرية المؤثرة التي شاركت في المؤتمرات، وأرسلت إلى إحدى الصحف السويسرية. [2]

كما أن المنافسة التجارية أو التجسس العسكري والصناعي أحد الدوافع التي تدلي لارتكاب الجرائم المعلوماتية إما من طرف الأشخاص أو من الدول.

ويعد التسابق العسكري والفضائي القائم بين الدول دافعا للجرائم المعلوماتية، بحيث قام القراصنة بترصد شبكات معلوماتية تابعة لوكالة الفضاء ومواقع خاصة بالأسلحة الذرية التابعة لحكومة الولايات المتحدة. [3]

[1] https://e3arabi.com

[2] www, news, bbc, co.uk/hi/arabic/news/newsied1153000/1153/24.stm.

[3] نهلا عبد القادر المومني، المرجع السابق ، ص93-94.

**المطلب الثاني: العناصر المتطلبة للتحقيق في الجريمة المعلوماتية .**

تناولنا في هذا المطلب فرعين:

الفرع الأول بعنوان العناصر الرئيسية للتحقيق في الجرائم المعلوماتية، حاولنا تسليط الضوء على بعض الأفكار الأساسية وهي وجود جريمة من الجرائم المعلوماتية والتي لا تقوم إلا بقيام جميع أركانها مجتمعة.

أما الفرع الثاني بعنوان العناصر الثانوية للتحقيق في الجريمة الإلكترونية، وخصها هذا الفرع لتوضيح أهم العناصر لصحة إجراء التحقيق والتي تستدعي وجود فعلي للجرائم المعلوماتية ويجب استظهار وقت ومكان ارتكابها.

**الفرع الأول: العناصر الرئيسية للتحقيق في الجرائم المعلوماتية .**

**01- وجود جريمة من الجرائم المعلوماتية لمباشرة إجراءات التحقيق .**

إن أهم عنصر للتحقيق في الجرائم المعلوماتية هو الوجود الفعلي للجريمة، لم يشر المشرع الجزائري إلى المصطلح "الجرائم المعلوماتية" إلا أنه عالج بعض أنماط هذه الجرائم وأطلق عليها تسمية "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات" سنة 2004 وقام بتعديلات سنة 2006 على كل من قانون العقوبات والإجراءات الجزائية [1]. بوضع مجموعة من الترتيبات في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. [2]

إلا أن هذا المفهوم بقي مبهما إلى حين صدور القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. [3]

---

[1] قانون 09-04 المؤرخ في 5 أوت 2009، تتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، عدد 47، الصادرة بتاريخ 16 أوت 2009، ص 5.

[2] قانون 09-04 المؤرخ في 15 أوت 2009، تتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، عدد 47، الصادرة بتاريخ 16 أوت 2009، ص 5.

[3] قانون رقم 18-07 مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات، ج.ر، عدد 34 الصادر في 2018/07/10، ص 11.

**02- أنواع الجريمة المعلوماتية.**

تتعلق الجرائم المعلوماتية بأي نوع يرتكب على أو عن طريق نظام الكمبيوتر أو متصل بشبكة الانترنت وبالتالي يصنف السلوك الإجرامي إلى 3 فئات:

- فئة المجرمين الذين يستخدمون التقنيات الرقمية باعتبارها الهدف الأساسي للجريمة.
- فئة المجرمين الذين يستخدمونها كوسيلة لإعداد أو مساعدة أو صور الجريمة التقليدية كالاحتيال، التزوير و تبييض الأموال.
- فئة المجرمين الذين يستخدمون التقنيات الرقمية كوسيلة للجرائم التي تنطوي على محتوى غير قانوني كالمواد الإباحية للأطفال، العنصرية... .

وقد صنعت الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية بودابست نوفمبر 2001 الجرائم المعلوماتية إلى عدة أنواع وهي:

- الجرائم ذات الصلة بالكمبيوتر تشمل التزوير بواسطة الحاسوب.
- الجرائم ذات الصلة بالمحتوى وتشمل الدعارة المتعلقة بالأطفال.
- الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة. [1]

**03- أركان الجرائم المعلوماتية.**

**أولا: الركن الشرعي:**

هو الزمن الذي يجرم الفعل ويعاقب عليه وذلك تأسيسا على أول مبدأ في قانون العقوبات وهو مبدأ الشرعية الذي يقضي بأن "لا جريمة ولا عقوبة أو تدابير أمن إلا بنص قانوني".[2]

ولقد خصص المشرع الجزائري منذ تعديل 2004 وتبعته تحديات 2006 القسم السابع مكرر من ق. العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات والذي يندرج

[1] الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، مجلس أوروبا، مجموعة المعاهدات الأوربية، رقم 105، بودابست، 2016.

[2] عبد الرحمن خلفي، محاضرات في القانون الجنائي العام دراسة مقارنة ، دار الهدى، الجزائر، 2012، ص 48.

ضمن الباب الثاني الجنايات والجنح ضد الأفراد، الفصل الثالث الجنايات والجنح ضد الأموال، المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري . [1]

**ثانيا: الركن المادي:**

يعتبر الركن المادي من ماديات الجريمة التي تبرز بها إلى العالم الخارجي كأثر للسلوك الإجرامي.

فلا تتوافر الجريمة إلا بتوافره مع بقية العناصر الأخرى، يرتكب في بيئة تكنولوجيا. [2]

**أ- جريمة الدخول أو البقاء عن طريق الغش في المنظومة المعلوماتية .**

يتمثل السلوك الإجرامي إما في الدخول أو في البقاء حيث يعتبر الدخول سلوكا إيجابيا يتمثل في الولوج إلى النظام المعلوماتي.

الغير مفتوح للجمهور عند رغبة المسؤول عن هذا النظام المعلوماتي وأشارت المادة 394 مكرر من قانون العقوبات الجزائية أنه "كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" لم يشترط المشرع صفة معينة في الشخص ولم يشترط وسيلة أو طريقة معينة أيضا وأوجب أن يكون مخالفا لإرادة صاحب النظام أي لا يوجد ترخيص، أما البقاء يتمثل في الامتناع عن المغادرة والخروج من النظام عن انتهاء التصريح وهو سلوك سلبي، حيث أن الدخول مشروع والبقاء غير مشروع، ليست كل النتائج محل اعتبار بل فقط ما تنص عليه المادة المذكورة سلفا المادة 394 مكرر من نفس القانون وهي: حذف المعطيات، تغيير المعطيات، تخريب نظام اشتغال المنظومة. [3]

---

[1] المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري.

[2] محمد عمر مصطفى، النتيجة وعناصر الجريمة، مجلة العلوم القانونية والاقتصادية، العدد 2، ، كلية الحقوق، جامعة عين شمس، القاهرة، السنة 1965، ص 324.

[3] أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، جامعة محمد البشير الإبراهيمي برج بوعريريج، سنة 2020-2021، ص 22.

**ب- جريمة التلاعب بالمعطيات .**

يتمثل السلوك الإجرامي في الإدخال والتعديل والإزالة، ورغم أن معظم الجرائم الواقعة على المعطيات هي جرائم خطر لا يشترط أن يترتب على السلوك الإجرامي اعتداء فعلي على المعطيات وتكون هنا جرائم مادية ذات نتيجة ويشترط التغيير في حالة المعطيات.

**ج- جريمة التعامل في معطيات غير مشروعة .**

السلوك الإجرامي له صورتين، إما التعامل في معطيات صالحة لارتكاب جريمة أو التعامل في معطيات متحصلة من جريمة سابقة أي متحصلة من جريمة الدخول أو البقاء غير المصرح بهما أو من جريمة التلاعب بالمعطيات ولا يعتد بنتيجة فيكفي قيام الجاني بأحد الأفعال المنصوص عليها في المادة 394 مكرر 2، فالغاية من هذا التجريم هنا وقائية. [1]

**ثالثا: الركن المعنوي .**

وهي العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني وجوهره الإرادة الإجرامية ويتخذ الركن المعنوي إحدى صورتين: القصد الجنائي والخطأ غير العمدي، فيعرف الأول على أنه علم الجاني بالعناصر المكونة للجريمة واتجاه إرادته إلى إحداث هذه العناصر أو إلى قبولها والقصد المتطلب هنا لقيام الجرائم الإلكترونية هو القصد الجنائي العام.

- جريمة الدخول البقاء غير المصرح بهما: جريمة عمدية تشترط توفر القصد العام المتمثل في العلم والإرادة .
- جريمة التلاعب بالمعطيات: جريمة عمدية .
- جريمة التعامل في معطيات غير مشروعة: جريمة عمدية . [2]

[1] أومدور رجاء، المرجع نفسه، ص 24.

[2] خالد ممدوح إبراهيم، في التحقيق الجنائي في الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009، ص12.

**04- تحديد وقت ومكان ارتكاب الجرائم الإلكترونية .**

إن تحديد مكان ارتكاب الجريمة هو بالأركان وليس بأثرها فيتوقف على هذا الجانب قدر كبير من عملية البحث عن مكان الجريمة الذي يوجد به الأثر والأدلة الجنائية المتعلقة بها ونتيجة لذلك يعمد كثير من المجرمين إدراكا منهم لهذه الحقيقة إلى نقل هدف الجريمة إلى مكان إتمامها وإلقائه في مكان آخر لتضليل المحقق وتعقيد عملية البحث وتظهر إشكاليتها في القانون الواجب تطبيقه لأنه هناك بعد دولي في هذا المجال لأن طبيعة الجريمة أنها جريمة عابرة للحدود ويعني ارتكاب الجريمة في مكان ما وزمان ما أو تتحقق النتيجة في مكان آخر وزمان آخر. [1]

**05- خصوصية الجرائم المعلوماتية.**

- الجرائم المعلوماتية عابرة للحدود الوطنية ذات طابع دولي .
- الجرائم المعلوماتية صعبة الاكتشاف والإثبات.
- الجرائم المعلوماتية تتسم بالجاذبية.
- الجرائم المعلوماتية مرنة لها سلبيات وخيمة. [2]

**الفرع الثاني: العناصر الثانوية للتحقيق في الجرائم المعلوماتية .**

خصصنا هذا الفرع لتوضيح أهم العناصر لصحة إجراء التحقيق والتي ستتبع الوجود الفعلي للجرائم المعلوماتية حيث يستوجب استظهار وقت ومكان ارتكابها.

**أولا: تحديد حيز الجرائم المعلوماتية .**

إن تحريك الدعوى العامة لا يكون من فراغ ويبنى على أسباب معقولة باكتشاف الجريمة ومعرفة فاعلها وجمع الأدلة، فيمكن أن تثار مشاكل وقت تحقيق النتيجة الإجرامية،

[1] محمد صلاح محمد عبد المنعم، الجرائم الالكترونية وتحدياتها، أطروحة دكتوراه، جامعة المنصورة، كلية الحقوق، القانون الجنائي، سنة 2017، ص246.

[2] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة، ط 1، مصر، 2011، ص53.

تتمثل في الوقت ومكان ارتكاب الجريمة باعتبارها عابرة للحدود الوطنية، إضافة إلى مشكلة القانون الواجب التطبيق. [1]

**1- القانون الواجب التطبيق:**

يتم تحديد الاختصاص بالنظر في الجرائم من خلال تحديد القانون الواجب التطبيق في الجرائم المعلوماتية والتطرق إلى مبادئ التي يعتمد عليها ومن بين هذه المبادئ:

أ- **مبدأ الإقليمية:** عالج المشرع الجزائري مسألة القانون الواجب التطبيق من خلال نص المادة 03 من قانون العقوبات "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية".

ب- **مبدأ الشخصية:** تبنى المشرع الجزائري مبدأ الشخصية كمكمل لمبدأ الإقليمية وفي ذلك لا يمكن إفلات المجرم المتمتع بالجنسية الجزائرية من العقاب، ويصعب تطبيق هذا المبدأ في الجرائم المعلوماتية نتيجة طبيعة المعلومات وإمكانية تخزينها مما يجعلنا أمام إشكالية تنازع الاختصاص القضائي الدولي. [2]

ج- **مبدأ العينية:** حصر المشرع الجزائري بعض الجرائم في المادة 588 من قانون الإجراءات الجزائية، والتي ينظر فيها وفقا لمبدأ العينية وتتمثل في جناية أو جنحة ضد سلامة الدولة الجزائرية، أو أي جناية أو جنحة ترتكب بحق المواطن الجزائري، وتكمن المشكلة هنا في حالة تنازع الاختصاص بين دولة ارتكبت فيها الواقعة وفقا لمبدأ الإقليمية ودولة تعتبر الفعل جريمة يختص بها قضاؤها ووفقا لمبدأ العينية. [3]

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 53.

[2] محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، دراسة مقارنة ، دار الجامعة الجديدة، الإسكندرية، 2018، ص 200.

[3] محمد كمال شاهين ، مرجع سابق، ص190.

**د- مبدأ العالمية:** يخول مبدأ العالمية للقضاء الجنائي الوطني حق النظر في الجرائم المرتكبة في الخارج من حامل لجنسية ضد ضحية أجنبية، ويبقى هذا المبدأ غير مقنن في القانون الجنائي الجزائري بشقيه قانون عقوبات وقانون إجراءات جزائية.

**2- مسألة الاختصاص القضائي في الجرائم المعلوماتية .**

بالرجوع إلى القانون 09-04سالف الذكر، نجد أن المادة 15 منه ضمن الفصل السادس المتضمن التعاون والمساعدة القضائية الدولية تناولت مسألة الاختصاص القضائي، وأكدت المادة 53 من القانون 18-07 سالف الذكر اختصاص الجهات القضائية الجزائرية بمتابعة الجرائم المتعلقة بمعالجة المعطيات ذات طابع شخصي التي ترتكب خارج إقليم الدولة.

**ثانيا: شروط التحقيق في الجرائم المعلوماتية .**

لا يمكن إثبات التحقيق إلا بتوفر الكتابة كشرط أساسي لصحة إجراء التحقيق، وسنتناول في هذا العنصر مجموعة من العناصر:

**1- العلنية بالنسبة للخصوم والسرية بالنسبة للجمهور:**

**أ- الأصل:** العلانية المطلقة في مرحلة التحقيق النهائي أي مرحلة المحاكمة بهدف توضيح حسن سير إجراءات الدعوى [1]، وتكون إجراءات التحري والتحقيق سرية ما لم ينص على خلاف ذلك، ودون أضرار بحقوق الدفاع.

أما العلانية بالنسبة لأطراف الدعوى فهو ضرورة حتمية، ولابد أن حضور المتهم يمليه حق إحاطته بالتهمة المنسوبة إليه.

**ب- الاستثناء:** قد تباشر إجراءات التحقيق دون حضور الخصوم، في حالة الضرورة والاستعجال، غير أنه يبقى لمحامي المتهم حق الإطلاع على ملف القضية. وفي حالة

[1] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة ، المكتب الجامعي الحديث، مصر، 2011، ص 67.

استمرارية منع المتهم من حضور إجراءات التحقيق بعد زوال الضرورة والاستعجال، يعد إخلالا بحقوق الدفاع وتبطل الإجراءات. [1]

**2- وجوب تدوين إجراءات التحقيق:**

والمقصود بها هو إثبات إجراءات التحقيق عن طريق الكتابة التي تعد حجة تتبني عليها النتائج، ويكون التدوين في محضر واحد أو عدة محاضر، ولابد من ذكر الوقائع بدقة مع تفادي حذف الكلمات أو الأقوال كما يلزم إعطاء الوصف القانوني للواقعة بدقة.

**3- الحق في الدفاع عند استخدام تقنية المحادثة المرئية عن بعد:**

ويكون حق الدفاع مكفول قانونيا في جميع مراحل القضية، ولم يعط القانون 15-03 المتعلق بعصرنة العدالة [2]، أهمية للحق في الدفاع عند إجراء التحقيق والمحاكمة الإلكترونية، ونص المشرع صراحة على إمكانية استعمال وسائل الاتصال المسموعة والمرئية أثناء الإجراءات، وذلك لمقتضيات حسن سير العدالة أو الحفاظ على الأمن أو الصحة العمومية. [3]

ففي مرحلة التحقيق القضائي، أجاز المشرع لجهات التحقيق استعمال تقنية المحادثة المرئية من بعد في استجواب أو سماع شخص أو عند إجراء مواجهة بين الأشخاص التي يستوجب القانون تحرير محاضر لأجلها.

---

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 58.

[2] قانون رقم 15-03، مؤرخ في 01 فيفري 2015، متعلق بعصرنة العدالة، ج ر، عدد 06 الصادرة بـ 10 فيفري 2015، ص 05.

[3] أمر رقم 66-155، 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بالأمر رقم 20 الموافق لـ 30 أوت 2020، ج ر، عدد 51، الصادرة بتاريخ 31 أوت 2020، ص 12.

## المبحث الثاني: الحق في الخصوصية المعلوماتية.

فالحق في الخصوصية المعلوماتية هو مبدأ يهدف إلى حماية خصوصية الأفراد فيما يتعلق بالمعلومات الشخصية التي يتم جمعها ومعالجتها، ويعتبر الحق في الخصوصية المعلوماتية جزءا أساسيا من حقوق الأفراد والحريات الأساسية بما أننا في العصر المعلومات، وسوف نتطرق في هذا المبحث إلى مايلي :

### المطلب الأول: ماهية الحق في الخصوصية المعلوماتية.

سنتطرق في هذا المطلب إلى التعريف بالخصوصية المعلوماتية من خلال الإشارة إلى آراء الفقهاء وصولا إلى محاولة لإيجاد مفهوم دقيق للخصوصية، وانسجاما مع وقفة المشرع في إيداع صور هذا الحق من خلال نطاقه.

فالحق في الخصوصية من أحد أهم المبادئ التي تحكم المجتمع فقد تم تكريسه في معظم الدساتير والقوانين الداخلية للدول، ومن أهمها الدستور الجزائري. وبعد التطورات التي شهدها العالم في المجال المعلوماتي، أصبح الاعتداء على هذا الحق من أكثر المخاطر التي تضر الفرد بالدرجة الأولى وتكنولوجيا المعلومات بالدرجة الثانية.

#### الفرع الأول: مفهوم الحق في الخصوصية المعلوماتية .

يعتبر الحق في الخصوصية من الحقوق اللصيقة بالشخصية، ففي ظل التطور الرهيب للأنظمة المعلوماتية تم التمكن من تجميع أكبر قدر ممكن من المعلومات والبيانات الشخصية، مما أصبح يشكل خطرا كبيرا على حياة الفرد الخاصة، ومن خلال ما تم تناوله سنتطرق لتعريف الحق في الخصوصية المعلوماتية.

**أولا: التعريف الموسع .**

في الحقيقة لم يرد لها تعريف في الدستور أو القانون ( التشريع ) ، على الرغم من وجود النصوص القانونية التي تحمي مظاهره وكثرة الأحكام القضائية المتعلقة بحالات الاعتداء عليه. [1]

ويعرف الحق في الخصوصية في المجال المعلوماتي هو "حق الفرد في تقدير متى وكيف يمكن للمعلومات الشخصية الخاصة به أن تصل للغير عبر شبكة المعلومات".[2]

وتتضمن خصوصية المعلومات القواعد التي تحكم إدارة المعلومات أو البيانات الخاصة، وهذا الحق ليس محصور فقط على الأشخاص، إنما يتعدى أيضا المؤسسات وغيرها، ولهم الحق أن يحددوا لأنفسهم متى وكيف وإلى أي مدى يمكن للمعلومات الخاصة أن تصل إلى العالم الخارجي.

**ثانيا: التعريف الضيق .**

تعددت التعاريف الفقهية، ومن أشهر التعريفات للحق في الخصوصية التعريف الذي أسنده معهد القانون الأمريكي، فأصبحت له قيمة هامة في الولايات المتحدة، بحيث تم حصرها في حالة التجسس على الحياة الخاصة، فهي "كل شخص ينتهك بصورة مباشرة وبدون وجه حق، حياة شخص آخر وإيصاله للغير".

وعرفه البعض على أنه "حق الفرد في اختيار سلوكه الشخصي وتصرفاته ومشاركتها مع الغير".[3]

---

[1] علي احمد عبد الزعبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، المؤسسة الحديثة للكتاب، ط 1، طرابلس، لبنان، 2006، ص 116.

[2] فتحي بن جديد، حماية الحق في الخصوصية أثناء التعاقد عبر الانترنت، مجلة القانون، العدد الثالث، 2012، ص 256.

[3] محمد نصر محمد، مرجع سابق، ص 26.

وكذلك يرى البعض الآخر: "حق الفرد في أن ينسحب انسحابا اختياريا بجسمه أو فكره من الحياة الاجتماعية ", أي بمعنى أن يمارس الشخص شؤونه الخاصة دون تدخل الغير وهو الحق في الخصوصية".

ويرى آخرون: "أن الحياة العائلية والزواج وما يتعلق بالحالة الصحية، بل أن بعضهم ذهب إلى أوسع من أنها تشمل الحياة الأسرية والعاطفية بل يمكن أن تشمل الحالة المالية".

ومقابل ذلك تبنى بعض الفقهاء تعريفا للخصوصية على نجد يجعل معناها مرادفا للحرية، وأن يكون للفرد اختيار سلوكه الشخصي وتصرفاته في الحياة عندما يمارسها مع الآخرين داخل المجتمع. [1]

**الفرع الثاني: نطاق الاعتداء على الحق في الخصوصية المعلوماتية .**

تعد الخصوصية عنصرا ضروريا للحياة في المجتمع الحديث، كما تعد حماية المعلومات الشخصية جزءا لازما للخصوصية، فيمكن تحديد نطاق الاعتداء على الحق في الخصوصية في عدة مواضع.

**أولا: في شبكات التواصل الاجتماعي .**

تعتبر شبكات التواصل الاجتماعي محل لمعرفة معلومات شخصية للمستخدمين مثلا: إقامة، منطقة، هوية، نشاطات، رقم الهاتف وغيرها من المعلومات فإن نقاط الاتصال والدخول إلى هذه الشبكة عملية مراقبة مستمرة.[2]

كما أن شبكات التواصل الاجتماعي تملكها شركات تجارية خاصة، وعائداتها ترجع من البيانات الخاصة بالأفراد، وبالتالي فإن كل ما يتعلق بالمعلومات الشخصية المعروضة عبر الموقع تكون معرضة لمخاطر الخصوصية. [3]

---

[1] علي أحمد عبد الزعبي، مرجع سابق، ص 120.

[2] عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية، دار الخلدونية، الجزائر، 2017، ص 123.

[3] محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، ط1، مركز الدراسة العربية، مصر، 2016، ص 52.

**ثانيا: في وسائل الاتصال الإلكترونية .**

يعتبر البريد الالكتروني أحد الوسائل الحديثة في المعاملات الإلكترونية التي تقدمها شبكة الانترنت، وبهذا فإن اختراق البريد الالكتروني من أهم المخاطر التي تواجه الحق في الخصوصية وانتهاك سرية المعاملات، ولهذا وفقا للقواعد العامة فإن تكريس ضمانات لحماية سرية المراسلات في حدود وضوابط معينة بغض النظر عن الأساليب المستخدمة.[1]

**ثالثا: في محركات البحث .**

مع انتشار المعاملات التجارية الالكترونية، أصبحت معظم الشركات تلجأ إلى تجميع البيانات والمعلومات الشخصية للأفراد عبر موقعها ودون التصريح عن الغرض من ذلك.

كما تقوم محركات البحث بجمع أكبر عدد ممكن من المعلومات الشخصية فيما يتعلق بطلبات البحث ومن الممكن تحديد هوية الشخص من خلال ذلك.

**رابعا: في المعاملات التجارية الإلكترونية.**

تعتبر المعاملات التجارية من أهم المواضع الخاصة في المجال المعلوماتي كالبيع والشراء أو عرض الخدمات، فقد تشكل مساسا بالحق في الخصوصية فهي علاقة تبنى على الثقة بين التاجر والزبائن خاصة عند تقديم معلومات شخصية، بحيث قد يتم استغلال هذه البيانات مما يجعل هذه المعاملات خطرا للحياة الخاصة، كما أن وسائل الدفع هي مصدر أخطر، وقد تستخدم البيانات الشخصية للمتعامل لأغراض إجرامية تمس الحياة الخاصة. [2]

**خامسا: في قواعد بيانات الحاسب .**

إن تسيير المؤسسات يتم عبر الأنظمة المعلوماتية، مما يتطلب تبني قواعد البيانات التي تحتوي على المعلومات الشخصية وتكون محمية.

---

[1] خدوجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الالكترونية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الأول، العدد 08، الجزائر ، 2017، ص 149.

[2] صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل، المجلد 24، العدد 2، عنابة، 2018، ص 130.

فمن الضروري إيجاد تقنيات حديثة لأمن الشبكات والأجهزة المتصلة لحمايتها، أن تقوم هذه التقنيات بتشفير جميع الاتصالات للتصدي للتحديات الجديدة، فمن المتوقع ظهور تهديدات جديدة يستوجب من خلالها تحديث البرمجيات الخاصة بهذه الأجهزة حتى تعمل بكفاءة طول مدة خدمتها. [1]

**المطلب الثاني: صعوبة التحقيق في الجرائم المعلوماتية .**

لقد واجهت عملية التحقيق في الجريمة المعلوماتية صعوبات كثيرة في كشف غموض هذه الجرائم التي يتطلب لارتكابها وسائل ذات تقنية عالية إضافة إلى ذكاء وخبرة المجرم في مجال الانترنت والحاسب الآلي، الأمر الذي قد يخلف آثار غير مادية فيصعب بذلك كشف الجريمة والقبض على الجاني، هذا الوضع دفع إلى ضرورة تطوير عملية التحقيق واستعمال أساليب ذات تقنية عالية. [2]

**الفرع الأول: انعكاسات خصوصية الجرائم على إجراءات التحقيق .**

تتميز الجرائم المعلوماتية عن بقية الجرائم التقليدية لما لها من الخصوصية، ولها عدة إشكالات متعلقة بها مما يثير العديد من المشاكل التي تعيق سير التحقيق.

هناك مشكلة متعلقة بالسيادة لأن من خصوصية الجريمة المعلوماتية أنها عابرة لحدود الدولة الواحدة وأيضا إشكالية الاختصاص القضائي والقانون الواجب تطبيقه ومدى قبول الأدلة المتحصل عليها ومدى صحتها في دولة ما أمام قضاء دولة أخرى، متطلبات التحقيق، الملاحقة, التفتيش والضبط.

ولنوضح العناصر السابقة لدينا قضية Thompson RN حيث قام مبرمج إنجليزي يعمل في بنك بالكويت بالتلاعب في معطيات نظام الحاسب الآلي للبنك، عن طريق الخصم من أرصدة العملاء والإيداع في حسابه الخاص ثم بعد عودته لبلاده طلب من البنك تحويل

[1] أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، 2015، ص 551.

[2] بدودة عزيزة، علالي سعاد، التحقيق الجنائي في الجرائم المعلوماتية، مذكرة ماجستير، جامعة غرداية، كلية الحقوق، سنة2017-2018، ص 49.

الحساب الخاص إلى عدة حسابات بنكية في إنجلترا، وبعدها حكم عليه بالسجن بتهمة الحصول على أموال الغير بالاحتيال، فقام بالطعن في الحكم استنادا إلى عدم اختصاص القضاء الإنجليزي لأن فعل السحب والإيداع كان بالكويت غير أن محكمة الاستئناف رفضت طعنه على أساس أن النشاط الإجرامي للمتهم لم يكتمل إلا بعد طلب التحويل ثم حصوله على الأموال محل النشاط الإجرامي، وبالتالي المكافحة تتطلب تعاونا كثيفا بين الدول وتوافقا كبيرا بين تشريعاتها. [1]

زيادة على ذلك قد ينعكس أثر خصوصية الجرائم المعلوماتية في إعاقة سير إجراءات التحقيق وتفسير ذلك.

عدم ترك الجرائم المعلوماتية لأثر خارجي، فلا توجد جثث قتلى ولا آثار دماء، ولا آثار عنف كما في الجرائم التقليدية، وهذا بسبب ارتكاب الجرائم المعلوماتية باستخدام تقنيات تكنولوجية عالية تعتمد على نقل المعلومات المعالجة آليا بالنبضات الإلكترونية. [2]

كذلك ضخامة حجم وكم البيانات والملفات المتواجدة في البيئة المعلوماتية، يصعب من إمكانية تحديد الملفات والبيانات المجرمة مما يؤدي في الغالب إلى اصطدام مهمة الاكتشاف بحق الفرد في الخصوصية الشخصية. [3]

أما بالنسبة إلى خصوصية الجرائم المعلوماتية حسب شخصية المجرم المعلوماتي، فمن الصعوبات التي تواجه السلطات المختصة بالتحقيق هي قدرة الجاني على محو الأدلة القائمة ضده أو تدميرها في زمن قصير.

---

[1] محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، المجلد 1، العدد 1، الجلفة،2009، ص 376.

[2] طاهر محمود أبو قاسم، الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، 2019، ص 158.

[3] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة ، المكتب الجامعي الحديث، الإسكندرية، 2018، ص 61.

كما أن البحث في ملفات الحاسب الآلي تقابله صعوبة غير عادية لاستطاعة الجاني تحريك الملفات من جهاز لآخر بسرعة فائقة وإخفائها في مساحة ضئيلة جدا على ذاكرة الحاسب، أو تخزينها في سيرفر يقع في دولة ذات اختصاص قانوني مختلف في تجريم هذه الجرائم، كذلك صعوبة تتبع المعلومات والبرامج والملفات المخزنة التي يتعين فحصها ولها ارتباط بالجريمة لكشف أدلة الجريمة، وتكمن الصعوبة إما في طبيعة المعلومات أو في نقص الخبرة الفنية. [1]

وفي هذا السياق نذكر دور الضحية في إعاقة سير التحقيق في الجريمة المعلوماتية، وهو كل من أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع للتقنيات الإلكترونية الرقمية. [2]

لكثرة استعمال وسائل التواصل الاجتماعي وقلة خبرة الضحايا وكشفهم لبعض المعلومات الشخصية عن حياتهم الخاصة يؤدي إلى زيادة ارتكاب الجرائم المعلوماتية خاصة جرائم السب والشتم، والابتزاز الإلكتروني والاعتداء على حرمة الحياة الخاصة وسرقة المعلومات الشخصية.

ومن أسباب عدم مباشرة إجراءات التحقيق في الجرائم المعلوماتية يكون امتناع الضحايا عن التبليغ عند التعرض لأحد أنواع الجريمة المعلوماتية.

ومن أهم الأسباب هو عدم معرفة الضحية بالإجراءات التي يمكن إتباعها في حالة التعرض للجرائم المعلوماتية كعدم معرفته الجهة التي يلجأ إليها للتبليغ وكيفية التبليغ عن الجريمة ويعود كل هذا إلى الجهل بالقانون: حيث أن عدم الإدراك بوجود نصوص تجرم وتعاقب على أشكال الجرائم المعلوماتية.

خوف الشركات والمؤسسات على سمعتها وكيانها وخشيتهم بسبب أن التبليغ يكون فرصة ذهبية للمجرم المعلوماتي لمعرفة مختلف نقاط الضعف فيها وجميع ثغرات النظام

[1] طاهر محمود أبو قاسم، مرجع سابق، ص 159- 160.

[2] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة، القاهرة، 2009، ص50.

المعلوماتي للمؤسسة يؤدي إلى امتناعها على التبليغ، وأيضا تخوف المؤسسات التجارية من استغراق التحقيق لفترة زمنية طويلة مع احتمالية احتفاظ جهات التحقيق بأجهزة الحاسب الآلي مما يؤثر على حسن سير العمل بتلك الشركات والمؤسسات.

أما امتناع الشركات والمؤسسات المالية كالبنوك عن التبليغ خشية من اهتزاز ثقة المتعاملين معها وبالتالي سحب ودائعهم واستثماراتهم ويتطور الأمر إلى الامتناع عن تقديم أية مساعدة لجهات التحقيق إذا عملت السلطات بالجريمة وليس فقط الامتناع عن التبليغ، وبهذا يصعب اكتشاف الجريمة من ناحية وصحة إثباتها من ناحية أخرى.[1]

وفي هذا السياق تعرض بنك Marchant Bank city في بريطانيا إلى سرقة 08 مليون جنيه إسترليني من أحد أرصدته إلى رقم في سويسرا، وتم ضبط الفاعل متلبسا بسحب المبلغ المسروق وبدلا من محاكمته قام البنك بدفع مليون جنيه له شرط التزام الفاعل بعدم الإعلام عن جريمته وإعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي. [2]

تخوف الضحايا من الإساءة للسمعة والفضيحة خاصة في الجرائم الإباحية والتشهير بالنساء أو في حالات الاعتداء الجنسي على الأطفال وعرض صور إباحية لهم في مواقع الأنترنت كما أن تخوف الموظف من الحرمان من خدمة الأنترنت قد يكون سببا في امتناعه عن التبليغ حين يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لمواقع غير مؤمنة أو غير مسموح له بزيارتها. [3]

وتوجد صعوبة في تحديد نطاق الضحايا كونهم في الكثير من الأوقات لا يعلمون شيئا عن الجريمة إلا بعد وقوعها ومن الحكمة يرون أنه عدم الإبلاغ عنها لفوات الأوان ولا

[1] فهد عبد الله العبيد العارمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016، ص 130.

[2] حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط01، دار النهضة العربية، القاهرة، مصر،2017، ص 34.

[3] طاهر محمود أبو قاسم، مرجع سابق، ص 174.

يحبون الاعتراف بأن نظامهم الإلكتروني قد اخترق ووقع ضده اعتداء وهذا السلوك يعتبر مغريا لمرتكبي الجريمة المعلوماتية للاستمرار في أنشطتهم وهذا تصرف سلبي. [1]

**الفرع الثاني: وسائل التقليل من الصعوبات المتعلقة بالجرائم المعلوماتية.**

تنوعت وسائل التقليل أو الحد من الجرائم المعلوماتية، بحيث تتباين هذه الوسائل بدرجة فاعليتها وتعقيدها، ومن بين هذه الوسائل:

– تحسيس أفراد المجتمع بالجانب السلبي للتكنولوجيا الحديثة ووجوب حماية القاصر عبر الأنترنت. [2]

– وجوب التبليغ عن التهديدات التي يتعرض لها الفرد عبر شبكة الأنترنت وبأي شكل من الأشكال.

– التكوين المستمر للأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية وكيفية التعامل مع الأدلة الإلكترونية.

– الاستعانة بالخبرات الفنية في المجال المعلوماتي، لتحديد نوعية الأدلة الإلكترونية التي يستوجب ضبطها والتحري عنها، كما يمكن الاستعانة بنظم المعالجة الآلية للبيانات من أساليب الفحص والتدقيق والمراجعة لاستخراج الدليل الإلكتروني. [3]

– تفعيل دور الإعلام ووسائله المختلفة من أماكن تلقي البلاغات في الجرائم المعلومات مع اتخاذ سلطات في المجال المعلوماتي تدابير رصد كل الشبكات المستخدمة للحاسب الآلي، ورصد مختلف المواقع المشبوهة، إضافة إلى متابعة المسجلين في جرائم التزوير والاحتيال. [4]

---

[1] فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2003، ص 34.

[2] قامت وزارة البريد والاتصالات السلكية واللاسلكية في الجزائر بنشر دليل عملي للأولياء والأوصياء والمربين يتعلق بحماية الأطفال عبر الانترنت في 15 جويلية 2020.

[3] فهد عبد الله العبيد العازمي، مرجع سابق، ص 139.

[4] طاهر محمود أبو القاسم، مرجع سابق، ص 176.

**خلاصة الفصل الأول:**

الجرائم المعلوماتية هي أنشطة إجرامية تتم باستخدام التكنولوجيا الرقمية كما تستهدف الأنظمة الحاسوبية والشبكات والأجهزة الإلكترونية ولا يمكن القول بتحقق الجريمة المعلوماتية إلا بوجودها فعلا تحقق أسباب ارتكابها وطبيعتها.

ورغم الالتزام بتحديد كافة العناصر اللازمة للتحقيق إلا أن طبيعة الجرائم المعلوماتية تعيق إجراءات التحقيق ومواجهة صعوبات بسبب خصوصية هذه الجرائم وقدرتها على تجاوز حدود الدولة، بالإضافة إلى قيام مرتكبي هذه الجرائم حيلا لتحريك البيانات ومحو الأدلة وإخفائها، مما يتطلب توعية الناس بوسائل تعزز فعالية التحقيق في هذه الجرائم.

أما الحق في الخصوصية هو حق الأفراد في حماية بياناتهم الشخصية وعدم الكشف عنها دون موافقتهم، كما أن هذا الحق محمي عبر التشريعات.

وتظهر أهمية التحقيق في مواجهة الجرائم المعلوماتية من خلال احترام الأجهزة المكلفة بالتحقيق والمبادئ المعترف بها قانونا وضمان التوازن بين فعالية التحقيق وضمان حقوق الدفاع، بالإضافة إلى الالتزام بتوثيق الإجراءات واحترام ما يخص الجريمة المعلوماتية.

# الفصل الثاني:

# خصوصية الجرائم المعلوماتية على المستوى الإجرائي.

## الفصل الثاني: خصوصية الجرائم المعلوماتية على المستوى الإجرائي.

إن خصوصية الجرائم المعلوماتية تشمل العديد من الجوانب التي تتعلق بحماية البيانات والمعلومات الرقمية أثناء الإجراءات الجنائية وسنتناول في هذا الفصل مبحثين:

تناولنا في **المبحث الأول: إجراءات التحقيق في الجرائم المعلوماتية.**

**والمبحث الثاني: الآليات المتخصصة في التحقيق والإثبات في الجرائم المعلوماتية.**

## المبحث الأول: إجراءات التحقيق في الجرائم المعلوماتية.

تعتبر طبيعة الجرائم المعلوماتية سواءا بطبيعتها أو خصوصيتها أو الوسيلة في ارتكابها، قد تدفع العديد من التشريعات لإعادة النظر في الكثير من المسائل المتعلقة بهذه الجرائم التي تلحق أضرارا، مع وضع سبل للتعامل مع هذه الأخيرة سواء في مرحلة التحقيق الأولية أو مرحلة التحقيق الابتدائية. [1]

ومن الصعب التحقيق في الجرائم المعلوماتية لصعوبتها وتعقيداتها، مما يستوجب وضع حلول تقنية ذات طبيعة خاصة تتماشى مع طبيعة هذه الجرائم، مما أثرت هذه الأخيرة على القانون الجنائي وخصوصا في ظل عدم وجود نصوص للتجريم والعقاب، هذا من جهة وعلى المستوى الإجرائي فإن النصوص الإجرائية تحدث عرقلة في جهاز العدالة وسير الدعوى خاصة في مرحلة التحقيق الابتدائي، ولقد قسمنا هذا المبحث إلى مطلبين أولهما يتم التطرق إلى مرحلة التحقيق الابتدائي، أما المطلب الثاني سنتناول فيه الجرائم المعلوماتية في مرحلة التحقيق النهائي. [2]

### المطلب الأول: خصوصية الجرائم المعلوماتية في مرحلة التحقيق الابتدائي

لم يحدد تعريف التحقيق الابتدائي في النصوص القانونية، بل تمت الإشارة إلى إجراءاته، غير أنه يمكن أن نقول أن هذه المرحلة هي "مجموعة من الإجراءات والتدابير تقوم بها السلطة المختصة بغرض التنقيب على أدلة الجريمة ومواجهتها ومعرفة فاعلها، لتقدير مدى كفايتها لإحالة المتهم إلى المحاكمة". [3]

ويجرى التحقيق الابتدائي إما بناءا على طلب الادعاء العام أو بناءا على شكوى

---

[1] بوعرعارة إبراهيم زياد، خصوصية الجرائم المعلوماتية، مذكرة لنيل شهادة ماستر، تخصص جنائي، جامعة غرداية، سنة 2021-2022، ص 56.

[2] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، أطروحة ماجستير، كلية الدراسات العليا في جامعة النجاح الوطنية، فلسطين، 2017، ص53.

[3] نداء نائل فايز المصري، المرجع نفسه، ص 54.

ونظرا لأهمية التحقيق في الجرائم المعلوماتية فقد منح القانون 09-04 دورا إيجابيا للأجهزة الخاصة بهذا النوع من الجرائم، من خلال تقديم كافة المساعدات في مواجهة الجرائم الماسة بأنظمة الاتصال والمعلوماتية وكشف فاعلها، وتعتبر هذه المرحلة بمثابة مرحلة تمهيدية للمرحلة التي بعدها. [1]

ويتمثل التحقيق الابتدائي في إجراءات متنوعة للوصول إلى الهدف المبتغى، وسنعرض إجراءات التحقيق في الفرع الأول، ويسلط الضوء على كافة الإجراءات التي يمكن أن تتوافق مع الطبيعة القانونية الخاصة بالجرائم المعلوماتية.

**الفرع الأول: إجراءات التحقيق الابتدائي.**

وهي تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق المحددة التي تقوم بإثبات وقوع الجريمة المعلوماتية وتحدد شخصية مرتكبيها، وهناك إجراءات واحتياطات يستوجب على الضبطية القضائية مراعاتها قبل الشروع في عمليات التحقيق الابتدائي. [2]

**أولا: الإجراءات التي يجب على الضبطية القضائية مراعاتها قبل البدء في التحقيق .**

ونذكر الأهم منها:

1- تحديد نوع النظام الخاص بالمعالجة الآلية للمعطيات.

2- وضع خطة تفصيلية للمكان الذي ستحدث فيه الجريمة والكشف عنها.

3- الأخذ بعين الاعتبار صعوبة حفظ الأدلة على المدى الطويل في الجرائم المعلوماتية.

4- وجوب قطع التيار الكهربائي من موقع التفتيش أو جمع الاستدلالات مع مراعاة إمكانية تدخل المجرمين عبر الشبكة لتدمير كافة المعلومات المخزنة.

---

[1] http://www.Startimes.com ; 26/04/2924 ; 10 :21

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، مصر، دار الكتب القانونية، المجلة الكبرى، ط 1، ص 84.

5- فصل خطوط الهاتف لمنع سوء استخدامها من قبل الجاني، مع التحفظ على الهواتف المحمولة لتجنب طمس البيانات.

6- يجب إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول على كلمة السر والشفرات في حال وجودها.

7- تصوير الأجهزة التي تخص الجريمة ذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في إجراءات التحقيق.

**ثانيا: الإجراءات التي يجب مراعاتها أثناء التحقيق .**

يستوجب على رجال الضبطية القضائية والخبراء المرافقين لهم إتباع بعض الإجراءات عند البدء في عملية التحقيق الابتدائي وخاصة عند تفتيش أجهزة الكمبيوتر: [1]

1- القيام بنسخة احتياطية من محركات الأقراص الثابتة والأقراص المرنة قبل استخدامها والتأكد من دقة النسخ.

2- القيام بإزالة غطاء الكمبيوتر المستهدف والتأكد من عدم وجود أقراص أخرى.

3- ويتم العمل على دراسة هذه البرامج وتطبيقاتها.

4- العمل على فحص كل ما يتعلق بالتطبيق وعلاقته بملفات المعلومات.

5- الحفاظ على المعدات المعدلة بشكل صحيح.

6- نسخ محتويات الأقراص لتحليل ما يوجد وكافة المعلومات حتى يمكن الوصول إلى الملفات المحدودة مع إمكانية استرجاعها.

**الفرع الثاني: الدليل الرقمي .**

نتناول في هذا الإطار تعريف الدليل الرقمي وخصائصه أولا، وخصوصية الأدلة ونطاق تطبيقه ثانيا.

[1] بوبقرة خيرة، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر، كلية الحقوق، قسم القانون العام، جامعة عبد الحميد بن باديس، مستغانم، السنة الجامعية 2019-2020، ص 56-57.

**أولا- تعريف الدليل الرقمي :**

يعرف الدليل بصفة عامة بأنه "الوسيلة التي يستعين بها القاضي في تكوين قناعته القضائية للوصول إلى الحقيقة. [1]

ولقد وردت عدة تعريفات للدليل الرقمي أو الإلكتروني تدور كلها حول مفهوم واحد، منها أنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برنامج وتطبيقات وتكنولوجيا خاصة. [2]

يكمن الفرق بين الدليل الرقمي والدليل المادي كون الأول يتكون من بيانات ومعلومات، ذات صفة الكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية، فهو يحتاج إلى مجال تقني يتعامل معه وهو ناتج من بيئة رقمية وهي بيئة افتراضية له سرعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال. [3]

**ثانيا- خصائص الدليل الرقمي .**

الأدلة الرقمية هي نتاج البيئة الإلكترونية الحديثة في العالم الافتراضي، وبسبب صلتها بالجريمة السبرانية واختلافها عن الجريمة التقليدية، فإنها تتميز بعدد من الخصائص التي تميزها عن أنواع الأدلة الأخرى، بها في ذلك:

**1- الدليل الرقمي دليل يصعب التخلص منه:**

من أهم خصائص الدليل الإلكتروني التي يتمتع بها عن باقي الأدلة التقليدية، لأن الأوراق والأشرطة المسجلة يمكن التخلص منها بسرعة وسهولة إذا كانت تحتوي على

---

[1] عائشة بن قارة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، د ط، دار الجامعة الجديدة، الإسكندرية، 2010، ص 51.

[2] إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة 2، العدد 10، ص 86.

[3] عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة ماستر، جامعة محمد خيضر، بسكرة، سنة 2014/2013، ص 7-8.

اعتراف شخص وذلك بتمزيقها أو حرقها ويمكن أيضا التخلص من بصمات الأصابع بمسحها أو تهديد الشهود أو قتلهم، أما بالنسبة للأدلة الإلكترونية يمكن استرجاعها بعد محوها وإصلاحها بعد تلفها، وإظهارها بعد اختفائها. [1]

**2- الدليل الرقمي دليل علمي وتقني:**

الدليل الرقمي هو حقيقة شيء، بوقوع جريمة أو فعل غير مشروع، ويستند إلى أن المباني في العالم الرقمي أو الافتراضي هي مبان علمية يشغلها علماء وفنيون، وتشير هذه الخاصية إلى أنه لا يمكن استخدام الأسلوب العلمي للحصول على الأدلة الرقمية أو الوصول إلى محتوياتها وهذه الخاصية مفيدة أيضا لرجال الضبط القضائي والاستدلال وكذلك سلطات التحقيق والمحاكمة عند التعامل مع الأدلة الرقمية في محاولة لإثبات الحقيقة. [2]

**3- الدليل الرقمي دليل متنوع ومتطور قابل للفسخ.**

يعتبر الدليل الإلكتروني دليلا قابلا للفسخ ويرجع ذلك إلى إمكانية استخراج نسخة من الأدلة الجنائية الإلكترونية لها نفس القيمة العلمية للأدلة الأصلية، وهي خاصية لا تتوافر في الأدلة الجنائية التقليدية الأخرى، وبالإضافة إلى ذلك، فإن الضمانة الفعالة للغاية لحماية هذا النوع من الأدلة من الضياع أو التلف أو التلاعب عن طريق النسخ المطابق للأصل من الدليل. [3]

---

[1] هلال آمنة، الإثبات الجنائي بالدليل الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2014-2015، ص 12.

[2] فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون للنشر والتوزيع، ط 1، مصر، 2010، ص 648.

[3] ممدوح عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006، ص 80.

أما فيما يتعلق بالتنوع المرتبط بالأدلة الإلكترونية، فنحن نعلم أنها يمكن أن تتجلى بشكل علني في أشكال مختلفة، مثل البيانات الغير المقروءة والصور الثابتة والصور المتحركة، وهذه الخاصية تحتاج إلى مواكبة التطورات في عالم التكنولوجيا. [1]

ومن الواضح أيضا أن الأدلة الإلكترونية تتميز بسعة تخزينها الكبيرة، حيث يمكن لكاميرات الفيديو الرقمية تخزين مئات الصور ويمكن للأقراص الصغيرة تخزين مكتبات صغيرة، وعلاوة على ذلك، تتمتع الأدلة الإلكترونية بالقدرة على رصد وتحليل المعلومات المتعلقة بالجاني في آن واحد ولذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

**4- الدليل الرقمي وعلاقته بانتهاك الخصوصية المعلوماتية .**

وقد أثارت مسألة انتهاك الخصوصية في سياق الحصول على أدلة إدانة المتهم عن طريق التنصت على مكالماته في الماضي الكثير من الاجتهادات من قبل المدافعين عن الخصوصية، مما أدى إلى ظهور الكثير من الاجتهادات التي تقرر عدم شرعية هذه الأدلة، إن هذه الدائرة من الجدل حول الدليل التقليدي انتقلت إلى الدليل الرقمي حيث يختلف الوسيط الافتراضي عن الوسيط المادي، وقد يتطلب استخراجه التعدي على مجالات الخصوصية المعلوماتية، لذا يجب أن يخضع قبوله لمزايا استدلالية لا تخرج عن ضوابط كثيرة حتى يكون ذا حجية. [2]

**ثالثا- الخصوصية المعلوماتية كأحد مظاهر الحق في حرمة الحياة الخاصة .**

إن فكرة الحياة الخاصة مفهوم مرن يتغير ويتطور في كل مجتمع، فهو يتمتع بالنسبية ويتغير حسب الروح السائدة في المجتمع وظروف كل فرد ويمكن أن تكون نظرة كل مجتمع إلى نطاق الحياة الخاصة أضيق أو أوسع حسب نظرته إلى نطاق الحريات التي يتمتع بها

[1] فتحي أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجاري، مرجع سابق، ص651 ص 652.

[2] إلهام شهرزاد روابح، مرجع سابق، ص 191.

لأفراد في المجالين العام والخاص، وعلى الرغم من صعوبة الاتفاق على تعريف واحد لأن الفقه يرفض تحديد الحقوق في هذا الإطار من الحياة ويترك مسألة تحديد الحقوق للقضاء. [1]

وذلك تبعا للظروف والأحوال والعادات والتقاليد القائمة في كل مجتمع وما يطرأ عليها من تطورات وتغيرات لاحقة، إلا أنه قد جرت بعض المحاولات الفقهية لتعريف موجودة، وتعتبر محتوية على عناصر الحقوق وخصائصها الثلاث: السرية، الحرية والنسبية. [2]

**رابعا- نطاق تطبيق الدليل الرقمي .**

عن الحديث عن الأدلة الرقمية كأدلة جنائية، من الضروري ذكر نطاق عمل هذا النوع من الأدلة، عند الحديث عن الأدلة الرقمية من الضروري الآن الحديث عن الجريمة الإلكترونية التي تعتبر نطاق للعمل بالدليل الرقمي وهي ظاهرة حديثة نسبيا وتعتبر الجريمة الإلكترونية ظاهرة حديثة نسبيا مقارنة بالجرائم التقليدية الأخرى في العالم بشكل عام وفي العالم العربي بشكل خاص ويرجع ذلك إلى أن الدول العربية حديثة العهد بتكنولوجيا الحاسوب. [3]

سنتناول تعريف الجريمة الإلكترونية بالنسبة للمشرع الجزائري ثم الحديث عن خصائصها وأخيرا سنتطرق إلى أثر خصوصية الجريمة الإلكترونية على الإثبات.

**1- الجريمة الإلكترونية بالنسبة للمشرع الجزائري:**

فقد قام بتجريم أفعال المساس بأنظمة الحاسوب الآلي، نتيجة للتأثير بالثورة المعلوماتية وهذا الأمر دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون 15/04 المؤرخ في 2004/11/10 المتمم الأمر رقم 156/66 والمتضمن قانون العقوبات، ونص أيضا

---

[1] عصام أحمد البهجي، حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية، دار الجامعة الجديدة، الإسكندرية، سنة 2005، ص 68-72.

[2] عصام أحمد البهجي، المرجع السابق، ص 73.

[3] https://www.asjp.cerist.dz/en/downArticle/272/5/2/30452 ; 01/05/2024 ; 22:28 PM.

عليها في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات وتضمن ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 07، كما ذكر سالفا. [1]

**2- خصائص الجريمة الإلكترونية .**

- ازدواجية محل الجريمة الإلكترونية.
- صعوبة اكتشاف وإثبات الجريمة الإلكترونية.
- الدليل الرقمي غير مرئي.
- سهولة محو وتعديل الدليل الرقمي.
- صعوبة الحصول على الدليل الرقمي.
- الصعوبات المتعلقة بالخبرة.
- الجريمة الإلكترونية عابرة للحدود. [2]

**3- أثر خصوصية الجريمة الكترونية على الإثبات .**

تتسم الجريمة السيبرانية بطبيعتها الخاصة التي تثير عددا من الإشكاليات ومن الصعوبة الإمكان إثبات الجريمة الالكترونية وترجع هذه الصعوبة إلى العديد من الأسباب منها أن الجريمة الإلكترونية ترتكب في بيئة غير تقليدية، فهي تقع خارج إطار الواقع المادي وتقوم أركانها في بيئة الحاسوب والانترنت مما يسهل محو وطمس الأدلة، لذلك يجب السماح في الحالات الطارئة بالسماح لرجال السلطة العامة بالقيام بضبط الأدلة عند وقوع الجرائم الالكترونية وبدون إذن مسبق لتفادي وحماية الأدلة من التعديل أو المحو من قبل الفاعل. [3]

ومنها نستطيع القول أن الجريمة الإلكترونية تنشأ عنها عدة معوقات تعيق إثباتها في إطار الإثبات الجنائي والعائق الكبير هو نقص الخبرة الفنية والتقنية.

---

[1] الأمر رقم 156/66 المؤرخ في 2004/11/10، يتضمن قانون العقوبات، ج.ر.

[2] بن فريدة محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم جنائية، جامعة الجزائر، كلية حقوق، ، 2015، ص 214.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص 46.

**المطلب الثاني: خصوصية الجرائم المعلوماتية في مرحلة التحقيق النهائي.**

إن المحاكمة هي المرحلة الأخيرة من الإجراءات العامة، ولذلك تسمى بمرحلة التحقيق النهائي وهي: "مجموعة من الخطوات التي يتم اتخاذها لمراجعة جميع الأدلة في القضية، سواء كانت لمصلحة المدعى عليه أم لا، بل أيضا لتقصي الحقيقة القانونية الفعلية المتعلقة بالادعاء ومن ثم إصدار الحكم". [1]

ولذلك فإن عملية التحقيق النهائية تخضع لمجموعة من القواعد العامة التي تختلف من مرحلة إلى أخرى، والغرض منها التحقيق الأولي هو يقتضي الحقيقة من خلال أدلة قاطعة أو حتى حاسمة وقد تكون سلطة الدولة في العقاب محدودة، لذا فإن هذه المرحلة لها خصائص أو ضمانات وضعها المشرع، فضلا عن منح المتشكي أو الجميع الثقة في العدالة.

تكون جلسة المحكمة علنية، وتكون إجراءات المحكمة شفهية، ويكون الخصوم حاضرين في إجراءات المحكمة، وتقتصر المحكمة على نطاق القضية ويتم تسجيل إجراءات المحاكمة[2] .

وبما أن بحثنا يركز على خصوصية الجرائم المعلوماتية فإن هذه المرحلة من البحث فمن ناحية نولي اهتماما لقواعد الاختصاص القضائي، ومن ناحية أخرى نولي اهتماما لسلطة القاضي في قبول الدليل الرقمي، فإن إجراءات المحاكمة في درجات التقاضي الخاصة بالجرائم الالكترونية هي نفسها إجراءات الجريمة التقليدية التي لا تكشف ببساطة عن أي خصوصيات في هذا الموضوع على مختلف الأصعدة.

**الفرع الأول: قواعد الاختصاص القضائي.**

ويعرف الاختصاص القضائي على أنه: "منح القانون الأجهزة القضائية صلاحية المراجعة في أنواع معينة من الدعاوى القضائية، يتبع المشرع قواعد وإجراءات معينة لتحديد

[1] الغافري حسين بن سعيد، السياسة الجنائية في مواجهة جرائم الأنترنت، دار النهضة العربية، القاهرة، 2009، ص 575.

[2] نمور محمد سعيد، أصول الإجراءات الجزائية، ، دار الثقافة للنشر والتوزيع، الأردن، 2005، ص 459-470.

مصيرهم، فالقاضي ملزم في البداية بالحكم على الاختصاص القضائي الدولي، أي أن يكشف أولا أن عما إذا كانت الهيئة القضائية الوطنية تتمتع بالاختصاص القضائي، ثم يقوم بعد ذلك بدراسة الاختصاص الداخلي، لأن تحديد المحكمة المختصة للفصل في النزاع أمر مهم لأنه يترتب على ذلك تحديد القانون الواجب التطبيق، ولذلك لابد من تحديد المعايير المعمول بها والتي تتناسب مع خصوصية الجرائم المعلوماتية. [1]

**أولا: مبدأ الاختصاص الإقليمي.**

شهد مفهوم الإقليمية في الآونة الأخيرة تطورا ملحوظا في تفسيره، ونلاحظ أن أغلب التشريعات تأخذ بمبدأ الإقليمية وله الأولوية في تطبيق قواعد الاختصاص، فالجريمة لم تعد تتطلب حدوث فعل مادي أو تشكيل أحد مكونات ذلك الفعل، وبالتالي تعتبر مجرد مكالمة هاتفية مع شخص في دولة أخرى يمكن أن تثبت وقوع جريمة داخل حدود تلك الدولة ولذلك فإن أي محاولة لوضع معايير قضائية إقليمية لمحاكمة الجرائم السيبرانية يجب أن تعكس هذا الاتجاه. [2]

ولذلك نقول أن مبدأ الإقليمية يقوم على مكان الجريمة أو أحد عناصرها المادية هذا هو المعنى الضيق لهذا المعيار.

ونظرا لخاصية الجرائم المعلوماتية، فإن هذا المبدأ لا يتوافق مع خصوصية الجريمة المعلوماتية فهي من ناحية غير ملموسة، ومن ناحية أخرى نظرا لصعوبة تحديد مكان وزمان الجريمة، فإن التقدم العلمي ومع تطور وسائل الاتصال، أصبح من الضروري الخروج على مبدأ الإقليمية، لأنها لم تعد كما كانت وبدلا من ذلك، تقل أهمية المعيار الوحيد، بينما تزداد

[1] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، المرجع السابق، ص 87-88.

[2] المقصودي محمد بن أحمد بن علي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا، الخليج العربي، دار المنظومة، 2015، ص 28-29.

أهمية المعايير الأخرى التي تعتبر نسخا احتياطية على سبيل المثال: المعايير العينية ومعيار العالمية. [1]

**ثانيا: مبدأ الاختصاص الشخصي.**

ويعني هذا المبدأ "تتم متابعة مرتكب الجريمة حامل الجنسية للدولة المعنية إذا ارتكب الجريمة في الخارج، ويشكل جريمة عند عودته للوطن". وهذا ما نصت عليه المادة 7 من قانون العقوبات السوداني، ويسري مبدأ الشخصية الجنائية على الجرائم المنصوص عليها في قانون الجرائم المعلوماتية. [2]

تمت الموافقة على هذا المبدأ أيضا بسبب مخاوف من وجود خلل في مبدأ الإقليمية، فمن الممكن أن يهرب المواطن من البلد الذي ارتكبت فيه الجريمة، ويعتمد هذا المبدأ بشكل أساسي على جنسية الجاني وهويته ومحاكمته لارتكاب جريمة في الخارج، وتكون الإجراءات طويلة ومعقدة ومكلفة، ويجب معرفة هوية الجاني غالبا ما يكون هذا الأمر صعبا في الجرائم المعلوماتية لأنه غالبا ما يستخدم التشفير والألغاز المعقدة وأسماء مستعارة.

**ثالثا: الاختصاص العيني.**

ويعني هذا المبدأ أن القانون الجنائي الوطني ينطبق بغرض النظر على جنية الجاني وهذا انتهاك للسيادة الوطنية، حيث يحرص كل دولة على حماية مصالحها الخاصة، مثل حماية نظامها القضائي، وعلى سبيل المثال وتترك أي هيئة تشريعية الجرائم التي تؤثر على سلطتها القضائية الوطنية لأنها لا تثق في قيام أي دولة بمعاقبتها. [3]

ومن الجدير بالذكر أن التشريعات الجنائية في الكثير من الأحيان لا تعطي الأولوية للمعايير التذكارية، بل تلجأ بدلا من ذلك إلى المؤسسات القضائية الوطنية استنادا إلى مبدأ الشخصية وتعتبر تكملة لهذا المبدأ، ولقد وقعت جرائم خطيرة تمس الأمن القومي وتهدف

---

[1] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، المرجع السابق، ص 90.

[2] طه إبراهيم قسم السيد أحمد، الجريمة المعلوماتية في القانون السوداني، ط1، السودان، 2015، ص 25.

[3] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، المرجع السابق، ص 92.

إلى الإضرار بمؤسسات الدولة: الاقتصادية، والعسكرية، والسياسية لأنه إذا حدثت الجريمة في الخارج، فقانون الدولة لا يجرم ذلك خاصة الجرائم التي تقع إقليميا، وإن الاستثناء الوارد على هذه الجرائم نظرا لخطورتها لأنها تهدد الدولة ومصالحها الأساسية ومكانتها. [1]

ومبدأ العينية من المبادئ المناسبة لطبيعة الجرائم المعلوماتية، وخاصة إذا كانت هذه الجرائم قد تؤثر على السيادة الوطنية، ومن هذا: نلاحظ أن الكثير من التشريعات تستند في الجريمة المعلوماتية إلى مبدأ العينية.

**رابعا: الاختصاص العالمي .**

يمنح هذا المبدأ القانون الجنائي نطاقا واسعا من التطبيق، فهو يغطي العالم بأكمله ولا يقتصر على المكان الذي ارتكبت فيه الجريمة، ولا جنسية مرتكبيها، ولا بطبيعة هذه الجريمة ولا انتهاكها لسيادة الدولة. [2]

ونلاحظ أن معظم التشريعات تتبنى هذا المبدأ بشكل تبعي وأنه يتعارض مع طبيعية القانون الجنائي، لأنه في الأصل قانون محلي أو إقليمي، وهو ليس عالمي، فهو مبدأ ثانوي فقط عندما يكون من المستحيل معاقبة المجرم دون اللجوء إليه [3] ، ولا شك أن مبدأ العالمية ينطبق على الجرائم المعلوماتية التي تتوزع معظم الأنشطة الإجرامية بالنسبة للعديد من الدول، نظرا لأن شبكة المعلومات لا تخضع لسيطرة دولة معينة، فيمكن لمستخدميها الوصول إليه من أي مكان في العالم عبر أي موقع من خلال جهاز الكمبيوتر المتصل به.

وأهم نقطة تثيرها مشكلة جرائم المعلوماتية هي أن المقر الرئيسي للأنترنت لا تقع في دولة واحدة محددة، لا تنتمي إلى شخص معين وبالتالي لا تخضع لإشراف أو رقابة دولة معينة كما يتم جمعها بالنسبة لعدد كبير من الشبكات ذات الأصول المختلفة، مثل شبكات

---

[1] الحلبي محمد علي سالم، شرح قانون العقوبات، مكتبة دار الثقافة للنشر والتوزيع، عمان، سنة 1997، ص 69-71.

[2] محمد لموسخ، تنازع الاختصاص بالجرائم المعلوماتية، دفتر السياسة والقانون والجزائر، دار المنظومة، الجزائر، عدد 2، 2009، ص 150.

[3] الحلبي محمد علي سالم، شرح قانون العقوبات، مرجع سابق، ص 79.

التوظيف، لا يوجد قانون جنائي موحد يربط بينهما، أي وكما هو الحال مع التجريم فإن قواعد الإباحة تختلف باختلاف عدد الدول التي ترتبط بها هذه الجريمة وهنا تكمن المشكلة.[1]

**الفرع الثاني: سلطة القاضي في قبول الأدلة الرقمية.**

سنتطرق في هذا الفرع لمدى مقبولية الدليل الرقمي للإثبات الجزائي، وهل يعتبر الدليل الرقمي دليلا كاملا للإثبات يتعين على القاضي الأخذ بها كلما توفرت شروطه أم أنه مجرد طريق يمكن لرجال التحقيق من إتباع إجراءات تحقيق معينة ومن الخطأ أن يعتمد عليه القاضي دليل وحيد للإدانة.

إن الدول التي تتبنى نظام الإثبات المقيد لا يمكن الاعتراف للدليل الرقمي بأي قيمة إثباتية، ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، وبذلك إن لم يذكر المشرع الأدلة الرقمية كأحد الأدلة الممكن الاستناد عليها لإصدار حكم قضائي فستهدر قيمته الإثباتية.[2]

أما إذا لم يصدر القانون اعتماد الأدلة الرقمية في الإثبات، فإن الأدلة في هذا النظام تحكمها من حيث المبدأ قاعدتان:

**1- قاعدة استبعاد شهادة السماع:** ويقصد بها الشهادة التي سمعها الشاهد الذي شهد بها ولم يشارك بإحدى الحواس الخمس في إنشائها وتعتبر الأدلة الرقمية بشهادة سمعية لأنها تحتوي على أقوال أو مواد تم إنشاؤها بواسطة إنسان في جهاز كمبيوتر.[3]

---

[1] الغافري حسين بن سعيد، السياسة الجنائية في مواجهة جرائم الأنترنت، مرجع سابق، ص 576.

[2] بن لاغية عقيلة، حجية أدلة الإثبات الجنائية الحديثة، رسالة ماجستير، فرع القانون الجنائي والعلوم الجنائية، الجزائر، السنة 2011-2012، ص 130.

[3] بن لاغية عقيلة، المرجع السابق، ص 135.

**2- قاعدة الدليل الأفضل:** ولكن مع ظهور المستندات الإلكترونية حدث تغيير في القانون الذي يتبع هذا النظام وأصبح من المعترف به الآن أن الأدلة الإلكترونية لها نفس الأهمية. [1]

الجزائر تأخذ بنظام الإثبات الحر نصت المادة 212 من قانون الإجراءات الجزائية على مبدأ جواز الإثبات بجميع طرق الإثبات.

وقد نصت المادة 307 من نفس القانون على أنه "يتلو الرئيس قبل مغادرة الجلسة التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان في غرفة المداولة.

إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها، ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي". [2]

كما قد خلف السلطة التشريعية أيضا لحماية المعاملات الرقمية من خلال القانون رقم 04/09

المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [3] ، أدرج المشرع في المادة 06 من نفس القانون

---

[1] بلجراف سامية، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، المجلد 67، العدد 61، سنة 2021، ص 689.

[2] المادة 307 من القانون 04/09، مرجع السابق.

[3] القانون 04/09 المؤرخ في 14 شعبان عام 1430 الموافق 5 سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة في 25 شعبان عام 1430، ص 07.

طريقة ضبط والحصول على الأدلة الرقمية والتي تتضمن شكلين: يكمن الأول في نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية وتكون قابلة هاته المعطيات لحجزها حسب ما هو مقرر في تحرير الدليل المنصوص عليها في قانون الإجراءات الجزائية, فالشكل الثاني هو استخدام التكنولوجيا المناسبة لمنع المستخدمين المصرح لهم لنظم المعلومات من الوصول إلى البيانات الموجودة في النظام أو نسخها عندما يصعب الحصول على أدلة وفقا لشكل الأول. [1]

حيث نصت المادة 07 من هذا القانون على: "إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه، لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المحتويات التي تتضمنها المنظومة المعلوماتية، أو نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة". [2]

إن الأدلة الرقمية بطبيعتها، لا يمكن أن تترك للقاضي لاتخاذ قرار بشأنها بل يجب أن يترك الأمر لتقدير القاضي ولا علاقة لإرادة المشرع برفض أو تحديد قيمة الدليل، ومن هنا فإن للقاضي كامل التقديرية ومع ذلك حرية القاضي في الاقتناع ليست مطلقة وإنما مقيد بشروط معينة. [3]

- يجب التوصل للدليل الرقمي بطريقة مشروعة ومع ذلك فإن مجرد تقديم الأدلة الإلكترونية يمنح المحكمة سلطة مطلقة لتقييم الأدلة وهو أمر يدخل ضمن السلطة التقديرية

[1] المادة 06 من نفس القانون السابق.

[2] القانون 04/09، المرجع نفسه، ص 08.

[3] بلجراف سامية، سلطة القاضي الجزائي في قبول وتقدير القاضي الرقمي، مرجع سابق، ص 691.

للقاضي "لا يمكن للقضاة استبعاد الأدلة الرقمية بخلاف دليل رقمي آخر يقنعهم بصحة الأدلة المقدمة". [1]

وأخيرا، تجدر الإشارة إلى أنه لا ينبغي للقاضي أن يخلط بين الاشتباه في تزوير أو اللعب بالأدلة الرقمية أو الخطأ في استخراج الأدلة بسبب عطل أو خلل في الأجهزة والمعدات التي استخرجت منها الأدلة الرقمية وبين قوتها كدليل مقنع يبني عليه قراره.

فالحالة الأولى كما سبق شرحه لا تدخل ضمن اختصاص القاضي لأنها مسألة فنية متروكة لتقدير الخبير، بينما إذا لم يتم التلاعب بالأدلة فإن القاضي يقبلها كدليل مقبول وتكون ضمن اختصاصه. [2]

مما لا شك فيه أن الأدلة الرقمية يمكن أن تلعب دورا فعالا ولا غنى عنه في الكشف عن الجريمة نظرا لانخفاض هامش الخطأ فيها ولكن من ناحية أخرى، لا يمكن تجاهل التأثير على خصوصية المعلومات بسبب الطبيعة التقنية للأدلة الرقمية وكونها قائمة على المراقبة الالكترونية، وهذه المراقبة تمس بالحق في الخصوصية المعلوماتية كثيرا في الحالات التي يتم الحصول على الأدلة الإلكترونية يتم الولوج إلى البريد الالكتروني للمشتبه فيه أو الاطلاع على محتوى رسائله الإلكترونية وبعد جمع الأدلة تبين أن المشتبه به ليس بريء من هذه الجريمة وتبرير ذلك هو الحاجة إلى الإثبات الجنائي وضرورة التصدي للجريمة الماسة بحياة الأفراد والمجتمع وخاصة الجرائم الماسة بأمن الدولة، وهذا يستلزم استخدام هذا النوع الأدلة الجنائية. [3]

---

[1] أحمد حمو وآخرون، الأدلة الإلكترونية من الناحيتين القانونية والتقني "دراسة تحليلية مقارنة"، هيئة مكافحة الفساد، جامعة بيزيت، فلسطين، 2015، ص 43.

[2] بلجراف سامية، مرجع سابق، ص 691.

[3] عيدة بلعاد، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة الآفاق العلمية، جامعة سعيدة، المجلد 11، العدد 1، سنة 2019، ص 145.

## المبحث الثاني: الآليات المتخصصة في التحقيق والإثبات في الجرائم المعلوماتية.

سن المشرع الجزائري سلسلة من الإجراءات لمساعدة سلطات التحقيق على الكشف في الجرائم المعلوماتية، وإيجاد الدليل الرقمي الذي من خلاله يتم متابعة مرتكبي الجريمة، ومن بين هذه الإجراءات نجد أن إجراءات الفحص هي تلك المتعلقة بالجرائم التقليدية، ويمكن تطبيقها على البنية الرقمية مع مراعاة بنية الخصوصية وطبيعة الأمر، إضافة إلى ذلك استحدث المشرع إجراءات أخرى للكشف عن جرائم المعلوماتية كإجراء الاختراق الالكتروني الذي تقوم به الشرطة القضائية دعما لسلطات التحقيق، بالإضافة إلى اعتراض المراسلات والمراقبة الالكترونية والحفظ والكشف عن المعلومات المعلوماتية، بالإضافة إلى إنتاج المعطيات المعلومات وتجميع كافة البيانات الالكترونية في وقتها الفعلي. [1]

### المطلب الأول: الآليات المتخصصة في التحقيق في الجرائم المعلوماتية .

حدد المشرع الجزائري في نص المادة 14 من قانون الإجراءات الجزائية صفة المسؤولان عن التحقيق والاستدلال هما الشرطة القضائية، وأعوان الضبط القضائي والأعوان والوكلاء المنوط بهم قانونا بعض مهام الضبط القضائي [2]، ولا يجوز لأي شخص آخر أن يباشر إجراءات التحقيق لأن المشرع قد سبق أن حدد الحاجة لذلك يتمتع الأشخاص الذين يقومون بالتحقيق بصفات معينة لضمان احترام الحقوق الفردية في هذه المرحلة. [3]

---

[1] مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المجلد 6، العدد 3، الجزائر، سنة 2023، ص 193.

[2] المادة 14 من قانون الإجراءات الجزائية المعدل والمتمم بموجب الأمر رقم 02/15 ج.ر، ج.د.ش، العدد 40.

[3] عبد العالي خراشي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الإسكندرية، 2006، ص 106.

ويعرف التحقيق في الجرائم الالكترونية بأنها إجراءات قانونية التي تتخذها الشرطة ويعين القضاء مرتكبي الجرائم الالكترونية ويقدم الأدلة الرقمية، وتتولى أجهزة التحقيق القضائي على وجه تحديد مسؤولية العمل القضائي لمثل هذه الجرائم. [1]

وتم تقسيم هذا المطلب إلى ثلاث فروع، الفرع الأول خاص بالأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية، أما الفرع الثاني يتم التطرق إلى الوسائل المستخدمة في التحقيق في الجرائم المعلوماتية، أما الفرع الثالث فيخص التفتيش في الجرائم المعلوماتية.

**الفرع الأول: الأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية .**

**أولا: جهاز الضبطية القضائية .**

تعتبر الضبطية القضائية ذات اختصاص عام في عمليات التفتيش والتحقيق في الجريمة بمختلف أشكالها، إلا أن ذلك لا يمنع من سن بعض القوانين المتخصصة واستثناء من ذلك فيتم منح هذا الدور لبعض الجهات والمؤسسات الخاصة نظرا لخبرتها في مجالات محددة وهم أكثر ندرة من غيرهم في الكشف في الجرائم التي تقع ضمن اختصاصهم التقني أو الفني [2]، والحقيقة أن هذا لا يمنع من ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال الضبط القضائي.

ولقد حرص المشرع الجزائري للتصدي على هذه الجرائم من خلال توقيع صلاحيات الضبطية القضائية وذلك بإمكانية استعانته بوضع آليات تقنية للكشف السريع عن الجرائم الالكترونية وملاحقة فاعليها. [3]

---

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، ط1، القاهرة، 2009، ص 169.

[2] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء قانون رقم 09-04، رسالة مقدمة لنيل شهادة ماستر قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة ورقلة، 2012-2013، ص 66.

[3] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، الجزائر ،العدد 04، سنة 2018، ص 53.

**1- تشكيل الضبطية القضائية.**

ونقصد بهم الموظفون الذي خولهم القانون للقيام بالإجراءات الخاصة بالتحقيق، ويستمدون اختصاصهم من القوانين المنصوص عليها على سبيل الحصر. [1]

**أ- ضباط الشرطة القضائية:**

وتتمثل في:

* رؤساء المجالس الشعبية البلدية.

* الموظفون التابعين للأسلاك الخاصة وضباط الشرطة للأمن الوطني.

* رجال الدرك ذوي الرتب، والذين قضوا أكثر من 3 سنوات. [2]

* مفتشو الأمن الوطني.

**ب- أعوان الضبط القضائي:** تم تحديدهم في قانون الإجراءات الجزائية في المادة 19:

- أعوان خدمة الشرطة، وأعوان الدرك الوطني، وأعوان الخدمة والأمن العسكري.

- التقنيين والمتخصصين في مجال الغابات والحفاظ على الأراضي واستصلاحها.

- موظفون المصالح العمومية الذين يباشرون بعض مهام الضبط القضائي.

**ثانيا: دور مقدمي خدمات الانترنت في التحقيق عن الجرائم المعلوماتية.**

وتم تعريفهم في القانون 09-04:

- أي مؤسسة عامة أو خاصة توفر لمستخدمي خدماتها إمكانية التواصل من خلال النظام الخاص بالمنظومة المعلوماتية أو الاتصالات.

[1] عبد العالي خراشي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الإسكندرية، 2006، ص 107.

[2] المادة 15 من قانون الإجراءات الجزائية المعدل والمتمم بموجب أمر 02/15، المرجع السابق.

– أو أي جهة تقوم بمعالجة أو تخزين أي بيانات معلوماتية لصالح خدمة الاتصالات المذكورة أو لمستخدميه. [1]

ويتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحقيق وكذلك كتمان سرية العمليات.

ونذكر أهم المهام التي يقوم بها مقدمي الخدمات في التحقيق في الجرائم المعلوماتية:

**01: تقديم مساعدات للسلطات المكلفة بالتحقيق.**

نصت المادة 10 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها فإن مزور الخدمات عليه الالتزام بـ:

– تقديم المساعدات للجهات المسؤولة عن التحقيقات القضائية في جمع وتسجيل الديانات في الوقت المناسب حول محتوى الاتصالات والتمكن من مراقبة وفهم جميع الخطوات التي يتبعها المستخدم وتوعيته بالمواقع الإلكترونية التي زارها، والمعلومات التي تم تخزينها والاتصالات التي قام بها. [2]

– الحفاظ على السرية من خلال إخفاء كامل التصرفات التي قاموا بها بناء على أوامر المحققين والمعلومات المتعلقة بذلك التصرف.

**02: حفظ المعطيات المتعلقة بحركة السير.**

وفقا للمادة 11 من قانون 09-04 فإن مقدمي الخدمات عليهم الالتزام بـ:

– حفظ المعلومات التي تساعد بالتعرف على مستخدمي الخدمة.

– حفظ كافة المعطيات التي تتعلق بالتجهيزات التي تخص الاتصالات.

– الحفاظ على الخصائص التقنية وتاريخ ووقت ومدة الاتصال.

---

[1] القانون 09-04، الصادر في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47.

[2] المادة 10 من قانون 09-04، الصادر في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، العدد 47.

– الحفاظ على كافة المعطيات التي تسمح بالتعرف على المرسل والمرسل إليه ومعرفة كافة المواقع التي تم الإطلاع عليها. [1]

**ثالثا: التزامات خاصة بمقدمي خدمات الانترنت.**

نصت المادة 12 من قانون 09-04 فيتعين على مقدمي خدمات الانترنت:

* التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها.

* وضع ترتيبات تقنية تسمع بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة وإجبار المشتركين لديهم بوجودها. [2]

**الفرع الثاني: الوسائل المستخدمة في التحقيق في الجرائم المعلوماتية.**

عندما يتعلق الأمر بإجراء التحقيق في جريمة ما، يجب على المحققين الالتزام بالقانون والتشريعات المعمول بها، والتي تحتوي على لوائح وقواعد تتضمن مبدأ الشرعية وسهولة الوصول إلى الجاني ومكان ارتكاب الجريمة.

تتمتع الجرائم المعلوماتية بخصائص فريدة وبالتالي فإن التحقيق في هذه الجرائم يتطلب معرفة شاملة والحصول على معلومات خاصة بوقوع الجريمة من أجل كشف غموضها والتواصل مع المتهمين، ولتحقيق ذلك يعتمد الباحثون على مجموعة متنوعة من الوسائل لإجراء التحقيق في هذه الجرائم.

**أولا: الوسائل المادية.**

وهي أدوات تقنية تستخدم بشكل متكرر في بنية نظم المعلومات ويمكن استخدامها لتنفيذ إجراءات وأساليب التحقيق المختلفة وإثبات وقوع الجرائم والمساهمة في الكشف عنها، مع تحديد هوية مرتكبيها. [3]

---

[1] المادة 11، من قانون 09-04.

[2] المادة 12، قانون 09-04.

[3] عز الدين عثماني، المرجع السابق، ص 54-55.

– عناوي IP ، والبريد الالكتروني، برامج المحادثة.

– البروكسي: حيث يعمل هذا الأخير بمثابة وسيط بين الشبكة ومستخدميها وتمكين الشركات التي تقدم خدمات الاتصال بالشبكات من التأكد من قدرتها على إدارة الشبكات وضمان الأمان وتقديم خدمات الذاكرة الجاهزة.

– برامج التتبع: حيث تحدد هذه البرامج عمليات الاختراق التي يتم تنفيذها وتقدم بيانات شاملة للمستخدمين الذين تم اختراق أجهزتهم، ويحتوي البيان على المعلومات التالية: **اسم** الحدث، تاريخ حدوثه، عنوان IP التي تمت فيه عملية الاختراق، اسم الشركة المقدمة لخدمات الانترنت التي تستضيف المخترق.

وأرقام الدخول والخروج الخاصة بها على شبكة المعلومات مثل غيرها من المعلومات.

– أنظمة لكشف الاختراق: وهي برامج تراقب عمليات معينة، والقيام بتحليلها في جهاز الحاسبة الآلية الإلكترونية، ومقارنة النتائج بحثا عن أي إشارة إلى وجود مشكلة تهدد أمان الشبكة. [1]

– أدوات لتدقيق ومراجعة عمليات الكمبيوتر.

– أدوات فحص ومراقبة الشبكة: تستخدم هذه الأدوات للتحقق من البروتوكولات وذلك لتحديد المشكلات التي قد تؤثر على الشبكة وفهم العمليات التي تتعرض لها، وتتمثل وظيفة هذه الأدوات في تحديد الموقع الفعلي للحاسبة الآلية على الشبكة. [2]

**ثانيا: الوسائل الإجرائية .**

تهدف هذه الإجراءات إلى تنفيذ طرق التحقيق المحددة والغير محددة التي تثبت وقوع الجريمة وتحدد شخصية المرتكب ويمكن تحقيق ذلك من خلال عدة طرق أهمها:

[1] بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة لاستكمال متطلبات نيل شهادة الماستر، كلية الحقوق، جامعة البشير الإبراهيمي، برج بوعريريج، سنة 2021–2022، ص 43.

[2] عز الدين عثماني، المرجع السابق، ص 55.

1- تتبع الأثر: وهو تتبع الأثر الرقمي للجريمة، مثل تحديد البريد الإلكتروني أو تتبع أثر الجهاز المستخدم في الاختراق.

2- الإطلاع على عمليات النظام المعلوماتي وحمايته.

3- الاستعانة بالذكاء الاصطناعي لاستنتاج النتائج من خلال التحليل الذي يتم تنفيذه بواسطة الحاسوب وبرامج مخصصة لهذا الغرض.

4- مراقبة الاتصالات الالكترونية، لم يتم تنظيم عملية مراقبة الاتصالات الإلكترونية في التشريع الجزائري. [1]

**الفرع الثالث: التفتيش في الجرائم المعلوماتية .**

ويمكن تعريف التفتيش على أنه: أحد إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية تثبت ارتكاب جريمة في مكان محمي كالمسكن أو على شخص معين، يتم ذلك لإثبات تورط المتهم وفقا للإجراءات القانونية أو للعثور على أشياء متعلقة بالجريمة لضبطها، ويجب أن يتم وفقا للقانون. [2]

ومن خلال ما تم التعريف يتضح أن التفتيش ينطبق على الجرائم التي تترك آثارا مادية، وبالتالي لا توجد مشكلات تعيق إجراؤه، حيث يتم البحث عن الأدلة المادية الملموسة. [3]

**أولا: نطاق تفتيش مكونات النظام المعلوماتي في جرائم الانترنت .**

يتكون النظام المعلوماتي من عناصر مادية وغير مادية، بالإضافة إلى الشبكات المحلية والإقليمية والدولية التي تستخدم للتحقيق والحصول على الدليل الجنائي الالكتروني، يتم تخزين المعلومات في أجهزة الحاسوب وأجهزتها الفرعية ووسائل تقنية أخرى، بالإضافة إلى

[1] عز الدين عثماني، المرجع السابق، ص 55.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص 182.

[3] دلال مولاي ملياني، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة الدكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018/2017، ص 41.

شبكات الاتصال التي تستخدم برامج وتطبيقات وتقنيات خاصة لتحقيق الدليل وتثبت الجريمة وتحديد مرتكبيها. [1]

**01- تفتيش مكونات النظام المعلوماتي.**

يتكون النظام المعلوماتي من مكونات مادية وأخرى معنوية.

**أ- تفتيش مكونات النظام المعلوماتي المادية.**

ليس من المثير للجدل فحص المكونات المادية لنظام المعلومات بحثا عن مشكلات معينة تتعلق بالجريمة التي وقعت، وتساعد على كشف الحقيقة وفاعلها، وتخضع للإجراءات القانونية التي تخص التفتيش، وتعني مشروعية التفتيش أن قرار فحص تركيبة هذه المواد يعتمد عليها طبيعة المكان الذي تقع فيه هذه المكونات، لأن خصائص المكان مهمة وطبيعته حاسمة إذا كان في مكان خاص مثل مسكن المدعى عليه، فلا يجوز تفتيشه إلا إذا كان تفتيش مسكنه مسموحا به وبنفس الضمانات والإجراءات التي يحددها القانون. [2]

ويتضمن التشريع الجزائري الإجرائي نصوصا قانونية قابلة للتطبيق من حيث المبدأ على تفتيش وفحص مكونات أجهزة النظام المعلوماتي، وأهم هذه النصوص المادة 64 من ق.إ.ج.ج والمواد 37- 40- 42 من نفس القانون والمواد من 44 إلى 47. [3]

**ب- تفتيش مكونات النظام المعلوماتي المعنوية.**

يرد التفتيش على مكونات نظام المعلومات المتمثلة في المعلومات المعالجة تلقائيا، ربما تكون الصور والأمثلة العملية التي يمكن الإبلاغ عنها عادة هي عمليات فحص البرامج، وتعتبر أحد الوسائل الأساسية للكشف عن الجرائم الأكثر شيوعا ضد أنظمة المعالجة الآلية المعطيات، لوجود برامج غير مصنفة تعمل في بيئة الاختراق أو تساعد فيها، على سبيل

---

[1] دلال مولاي ملياني، المرجع السابق، ص 215.

[2] خالد ممدوح، المرجع السابق، ص 195.

[3] المادة 64، والمواد من 44 إلى 47 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155، العدد 84، الصادرة في 24-12-2006.

المثال يمكن أن تكون برامج المسح المستخدمة للكشف عن الأبواب المفتوحة مجالا للمشاكل إذا تم استيفاء الشروط، حيث يكون الشخص مذنبا أيضا بجريمة الدخول الغير مشروعة إلى نظام المعالجة الآلية وهذا يتطلب الاعتراف اللفظي بافتعال الجريمة.

**ثانيا: شروط إجراء التفتيش وتنفيذه**

**01- الشروط الموضوعية لتفتيش نظام المعلوماتية.**

ويجب أن يقوم التفتيش وفقا لشروط معينة ونذكر أهمها:

**أ- سبب تفتيش نظم المعلوماتية .**

- وقوع جريمة معلوماتية: لإجراء أي عملية في مرحلة التحقيق كالتفتيش للنظم المعلوماتية أن تكون الجرائم واقعة فعلا، فلا يمكن أن يقع التفتيش من أجل احتمال وقوع جريمة، وهذا الشرط الأساسي لقيام عملية التفتيش باعتباره عملا من أعمال التحقيق. [1]

- توجيه التهمة وإسنادها إلى شخص معين: للقيام بإجراء التفتيش يستوجب أن يكون هناك شخص موجهة له التهم، بعدما تم جمع القرائن والأدلة التي تفيد وقوع الجريمة ونسبتها إلى فاعلها. كما يجب أن يكون الاتهام مبنيا على أدلة قانونية تثبت ذلك.

**ب- محل تفتيش نظم المعلوماتية .**

- يرد محل التفتيش على المكونات المادية والمعنوية للنظم المعلوماتية، بحيث تأخذ كافة البيانات والمعلومات والبرمجيات المخزنة في الحاسوب.

فالمشرع الجزائري ميز بين تفتيش المنظومة المعلوماتية داخل التراب الوطني وخارج الإقليم الوطني. [2]

[1] عثمان جبر محمد عاصي، ضمانات المشتكي عليه في التحقيق الجزائي الابتدائي، رسالة ماجيستير، جامعة آل البيت، كلية الدراسات الفقهية والقانونية، الأردن، 1998، ص 149.

[2] المادة 5، الفقرة 2 و3، من قانون 09-04.

← **الحالة الأولى: داخل إقليم الدولة الجزائرية.**

في حالة ما إذا كانت البيانات المراد إيجادها مخزنة في منظومة أخرى، فيمكن الدخول إلى هذه الأخيرة من خلال المنظومة السابقة، ويمكن تفتيشها دون إصدار إذن قضائي.

← **الحالة الثانية:** في حالة ما إذا كانت المعلومات المراد تفتيشها مخزنة داخل منظومة خارج الإقليم الوطني.

**02- الشروط الشكلية لتفتيش النظم المعلوماتية.**

يجب مراعاة الشروط الشكلية التي أقرها القانون عند مباشرة عملية التفتيش لحماية حرية المتهم وحماية الحريات الفردية والحقوق الخاصة للأفراد.

**أ- أن يجري التفتيش بحضور أشخاص يحددهم القانون وضرورة تحرير محضر التفتيش:** للحد من نطاق الاعتداءات على حرمة الحياة الخاصة للشخص وحرمة مسكنه المحمي قانونا تكفل معظم التشريعات الإجرائية عدم جواز التفتيش إلا بحضور المدعى عليه أو من يشوبه بحجة أن ذلك من القواعد الأساسية التي يترتب على انتهاكها البطلان. [1]

وقد وضع المشرع الجزائري هذا الشرط وفقا للمادة 1/45 من قانون الإجراءات الجزائية على النحو التالي: "إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب جناية فيجب أن يحصل التفتيش بحضوره، وإذا تعذر عليه الحضور وقت إجراء التفتيش، فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هارب استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته".

[1] براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص القانون، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، الجزائر، جوان 2012، ص 173.

ويجب على القائم على التفتيش بعد إجرائه أن يكتب تقريرا يتضمن كافة الإجراءات المتخذة لهذا الغرض حقائق موثقة مع تاريخ النشر توقيع المحرر [1] . ولا يشترط القانون أي شكل أو شروط خاصة يكفي أن يتضمن تقرير التفتيش ما تقتضيه القواعد العامة في تقرير عام، كأن يكون مكتوبا باللغة الرسمية.

ويجب تسجيل تقرير التفتيش من قبل كاتب مرافق للمفتش من أجل تسجيل وتوثيق جميع الإجراءات، وفقا لنص المادة 68 فقرة 2 من قانون الإجراءات الجزائية.

**المطلب الثاني: الآليات المتخصصة في الإثبات في الجرائم المعلوماتية.**

تتضمن الآليات المتخصصة في الإثبات في الجرائم المعلوماتية استخدام تقنيات فنية متطورة لجمع الأدلة الرقمية، مثل تحليل البيانات وجمعها وتتبع الأنشطة الرقمية ويجب استخدامها بعناية لضمان أن الأدلة التي تم جمعها وتحليلها قابلة للقبول قانونيا وتعطى صورة دقيقة للجريمة المرتكبة. [2]

**الفرع الأول: المعاينة في الجريمة الالكترونية .**

يتم تنظيم المعاينة بموجب المادة 43 من قانون الإجراءات الجزائية، وتعتبر جزءا مهما من عملية جمع الأدلة في الجرائم الالكترونية وفقا للتشريع الجزائري يتم تنظيم عمليات المعاينة بشكل دقيق لضمان توثيق وجمع الأدلة وكل التفاصيل بشكل قانوني وصحيح وتنص هذه المادة على الإجراءات التي يجب إتباعها أثناء عمليات المعاينة بما في ذلك الحقوق والواجبات للمعنيين بالتحقيق. [3]

ومن ذلك قوله تعالى: "قال هي راودتني عن نفسي وشهد شاهد أهلها إن كان قميصه قُدَّ من قبل فصدقت وهو من الكاذبين....".

---

[1] صالح شنين، الحماية الجنائية للتجارة الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد، كلية الحقوق، ، تلمسان، 2012-2013، ص 237.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص 149.

[3] المادة 43 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

وتشير هذه الآية إلى ضرورة الانتقال والمعاينة للتثبت من الوقائع. [1]

تكون المعاينة في الجريمة الإلكترونية غير مرتبطة بالانتقال عبر العالم المادي بالضرورة بل تتم عبر العالم الافتراضي فقط وهي عبارة عن مشاهدة مسرح الجريمة وإثبات الحالة فيها أي مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة للمساعدة على اكتشاف الحقيقة. [2]

عند الانتقال إلى المعانية يحرر محضرا يسجل فيه ما تم معاينته من قبل القاضي مع توقيعه وتوقيع كاتب الضبط والغرض من كتابته هو السماح للخصوم بمناقشة المحضر والرجوع إليه والتعليق على محتواه. [3]

وهناك عدة طرق ينتقل بها أعضاء هيئة التحقيق إلى العالم الافتراضي للمعاينة وذلك عن طريق:

– من مكتبه في المحكمة بحاسوبه الخاص.

– من خلال اللجوء إلى مزود خدمة الانترنت وهو أفضل مكان تتم المعاينة فيه، أو اللجوء إلى مقهى انترنت.

– ويمكن للمحقق المعانية في المسرح التقليدي ولا يكون في منظومة الحاسوب ويعتبر مكونات مادية محسوسة لمكان وقوع الجريمة كالبصمات... [4]

يجب على فريق المعاينة مراعاة مجموعة من الضوابط أثناء إجراء المعاينة وضبط جريمة الحاسب الآلي لسهولة الحصول على الأدلة وتأمينها كالتالي:

---

[1] سورة يوسف، الآيات 26–28 .

[2] يعقوبي زهرة، المعاينة والخبرة في الإثبات الجنائي، رسالة لنيل شهادة الماستر، جامعة عبد الحميد بن باديس، كلية الحقوق والعلوم السياسية، مستغانم، السنة 2022/2021، ص 09.

[3] مأمون عبد الكريم، محاضرات في طرق الإثبات وفقا لآخر النصوص، كنوز للنشر والتوزيع، ط02، الجزائر،سنة 2011، ص 96– 97.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط 1، دار الفكر الجامعي، الإسكندرية، مصر، سنة 2009، ص 156–157.

- تحديد نوع نظام المعالجة الآلية للمعلومات كمبيوتر معزول أو متصل .
- معرفة الطريقة التي يتم بها نقل المعلومات من موقع لآخر حصر الطرفين .
- معرفة المختصون لكل آلة وماركتها وموديلها وقدرتها على نقل المعطيات.
- اتخاذ الحيطة والحذر لمشكلة إخفاء الدليل الإلكتروني بتعديله أو محوه في ثوان.
- منع الجاني من التدخل من وحدة طرفية أخرى لإتلاف المعلومات المخزنة.
- التعامل مع التيار الكهربائي بحيلولة لعدم التلاعب في المعلومات من طرف الجاني.
- فصل خطوط الهاتف وإبعاد أي شخص عن أجهزة الحاسب الآلي. [1]
- إعداد فريق بحث من المختصين والفنيين.

**الفرع الثاني: الاستجواب والخبرة في الجرائم الالكترونية.**

يعد الاستجواب في الجرائم الالكترونية جزءا مهما وحساسا من عملية التحقيق، نظرًا للطبيعة التقنية والتعقيد الكبير لهذه الجرائم، سنذكر فيما يلي بعض النقاط التي تبرز كيفية إجراء الاستجواب في هذا النوع من الجرائم الالكترونية:

- إعداد محكم للأسئلة، الأسئلة يجب أن تكون محددة ومرتبطة بالتقنيات والأدوات المستخدمة في طبيعة الجريمة الالكترونية.
- فهم الجوانب التقنية، المحققون يجب أن يكونوا على دراية تامة بالتكنولوجيا والبرمجيات المستخدمة.
- التعاون مع خبراء تقنية المعلومات. [2]
- التركيز على التوقيت والنشاطات، يجب أن تشمل الأسئلة توقيت الأنشطة الإلكترونية وتفاصيل العمليات مثل توقيت تسجيل الدخول والخروج.

---

[1] بن فريحة رشيد، ميهوب يوسف، التحري الجنائي في مسرح الجريمة الالكترونية، جامعة عبد الحميد ابن باديس، الجزائر، سنة 2015، ص 55.

[2] أيمن عبد الله فكري، الاستجواب الجنائي الالكتروني، مجلة البحوث الفقهية والقانونية، ، جامعة الأزهر، كلية الشريعة والقانون بدمنهور، غزة، العدد 43، سنة 2023، ص 995.

– استجواب شهود العيان الإلكترونيين. [1]

إن الضوابط المقدرة للاستجواب في الجرائم الالكترونية تتطابق مع تلك المعتمدة للجرائم العادية، ولكن الاختلاف يكمن في الحاجة لتأهيل الجهات المختصة التي تتولى إجراءات الاستجواب إذ يتوجب على أجهزة التحقيق أن تكون مؤهلة بشكل خاص للتحقيق في جرائم الانترنت، بهدف فهم وقائع الجريمة والتعامل مع تفاصيلها بكفاءة، ذلك لأن مرتكبي هذه الجرائم ليسوا مجرمين عاديين. [2]

تعتبر الخبرة من أهم التدابير التي يجب مراعاتها عند التحقيق في الجرائم الإلكترونية وذلك لصعوبة التعامل مع هذا النوع من الجرائم، وقلة المعرفة بمجالها الفني، ويجب على الخبراء الذين يرتكبون جرائم عبر الانترنت التنسيق مع المحققين الجنائيين الذين يجب عليهم أيضا أن يشرحوا للخبراء الجوانب القانونية لطبيعة عملهم، مع التركيز على ربط الأدلة والخبرات العلمية بالعناصر والمضمون وأركان الجريمة المقام عنها الدعوى الجنائية. [3]

**الفرع الثالث: الشهادة في الجريمة الالكترونية .**

تعد الشهادة جزءا مهما من عملية الإثبات في القضايا المتعلقة بهذا النوع من الجرائم نظرا للطبيعة المعقدة والتقنية للجرائم الالكترونية .

**1- تعريف الشهادة الالكترونية.**

لم ينص المشرع الجزائري بتعريف للشهادة الالكترونية غير تلك القواعد المقررة لحماية الشهود حيث تعد مصطلح حديث خاص في مجال الانترنت وهي دليل من أدلة الإثبات بتسخير منظومة معلوماتية توضع تحت تصرف الشخص لينقل وقائع شهدها بحواسه،

[1] أيمن عبد الله فكري، المرجع نفسه، ص 996.

[2] وهيبة رابح، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، جامعة عبد الحميد بن باديس، مستغانم، العدد 04، 2014، ص 328.

[3] وهيبة رابح، المرجع نفسه، ص 328-329.

وتعتبر الشهادة الالكترونية هي ذاتها الشهادة التقليدية ولا تختلف إلا من حيث الوسيلة المستخدمة. [1]

**2- الشروط الواجب توافرها في الشهادة الإلكترونية لاعتبارها آلية للإثبات.**

- أن يكون الشاهد متمتع بالأهلية القانونية وحر الإرادة، المادة 1/228 من قانون الإجراءات الجزائية. [2]

- أن يكون الشاهد من الغير وألا يكون ممنوع من أداء الشهادة.

- يحب أن تكون الشهادة الإلكترونية في الخصومة القضائية. [3]

- أن تؤد الشهادة الالكترونية أمام المحكمة عبد الاتصال المرئي والمسموع أمام القاضي. [4]

- أن يتم التأكد من صحة الشهادة الالكترونية من أي تزوير أو تلاعب.

**3- سلطة القاضي في الإسناد إلى الشهادة الالكترونية .**

الشهادة الالكترونية دليل من الأدلة التي يستند إليها القاضي في الإثبات باعتبار أن المشرع الجزائري أجاز وأخذ بالنظام الإثبات الحر وهذا الأمر أعطى للقاضي السلطة التقديرية للاستناد إلى هاته الأدلة بقبولها أو رفضها. [5]

**4- طوائف الشاهد الالكتروني الرئيسية .**

يمكن تصنيف الشهود الالكترونيين إلى عدة طوائف بناء على دورهم في القضية ونوع المعلومات التي يقدمونها، إليك طوائف الشاهد الإلكتروني الرئيسية:

---

[1] عادل بوزيدي، دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية، مجلة النبراس للدراسات القانونية، جامعة العربي التبسي، تبسة، المجلد 1، العدد 1، سبتمبر 2016، ص137.

[2] المادة 01/228 من قانون الإجراءات الجزائية.

[3] محمد نظمي صعبانة، مدى حجية الشهادة عبر الوسائل الإلكترونية في قانون البيانات الفلسطيني، مجلة جامعة الأزهر، غزة، المجلد 9، العدد 5، سنة 2016، ص 217-219.

[4] المادة 222 من قانون الإجراءات الجزائية.

[5] المادة 212 من قانون الإجراءات الجزائية.

- مشغلو الحاسب الآلي.
- خبراء البرمجة شهود الخبرة التقنية .
- المحللون خبراء تحليل الأدلة الرقمية .
- مهندسو الصيانة والاتصالات شهود الشركات التقنية ومقدمي الخدمات .
- مديرو النظام مهندسو الشبكات وأمن المعلومات . [1]

**الفرع الرابع: ضبط الأدلة الالكترونية.**

**1- تعريف الضبط في مجال الجريمة المعلوماتية.**

يعرف الضبط في البيئة المعلوماتية بأنه وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية أو المعلومات التي تتصل بالجريمة الالكترونية للكشف عن الحقيقة ومرتكبها ومحل الضبط هو الدليل الرقمي. [2]

* وسط التعقيدات والصعوبات التي تواجهها الجهات المختصة في استخراج الأدلة الإلكترونية، لابد من مواكبة التطورات التكنولوجية ووضع إجراءات خاصة متكيفة للتعامل مع خصوصيات البيئة التقنية من أجل العثور على مرتكبي الجرائم المعلوماتية وجمع الأدلة ضدهم، وفي هذا السياق كثيرا ما تشترط الاتفاقيات الدولية ومعظم التشريعات الأخذ بهذه الإجراءات الخاصة، مع مراعاة إقامة التوازن بين الحق في استخدام الوسائل الحديثة لكشف الجرائم، وجريمة الأفراد واحترام خصوصيتهم [3] ، ومن هنا نذكر بعض الإجراءات المستحدثة للكشف عن الجريمة المعلوماتية:

---

[1] مرابطين علاء الدين ومحمادي مراد، خصوصية الجريمة الالكترونية في التشريع الجزائري، مذكرة لاستكمال متطلبات نيل شهادة الماستر، جامعة البشير الإبراهيمي، كلية الحقوق، برج بوعريريج، سنة 2022-2023، ص 48-49.

[2] نبيلة هبة هرول، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات- دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2006، ص 266.

[3] مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المجلد 6، العدد 03، الجزائر، سنة 2023، ص 199.

**1- التسرب القانوني:**

عرفه المشرع من خلال المادة 65 مكرر 12 ق.إ.ج على أنه "قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمرافقة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم!

مدته لا تتجاوز 4 أشهر ويكون بإذن مكتوب. [1]

**2- اعتراض المراسلات والمراقبة الالكترونية:**

عملية مراقبة المراسلات هي: "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية" حسب المادة 65 مكرر 05.

عرفت عملية اعتراض المراسلات بأنها تلك العملية التي تسمح بمراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري على الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه بهم. [2]

[1] القانون رقم 01/06 المتعلق بالوقاية من الفساد ومكافحته 06/01، المؤرخ في 20 فبراير 2006 المادة 56.

[2] المادة 65 مكرر 05 عملية مراقبة المراسلات.

**خلاصة الفصل :**

تتميز الجريمة المعلوماتية سواء على المستوى المحلي أو الدولي بطابع خاص عن الجرائم التقليدية التي توجد فيها خلافات حول اختصاص الجريمة المعلوماتية وتخضع لمبادئ الإقليمية في بعض الأحيان وفي أحيان أخرى تكون عينية وعالمية وشخصية ولهذا السبب هناك العديد من الدول التي تعزز التعاون لمكافحة هذه الجرائم وتبرم اتفاقيات دولية مثل: اتفاقية بودابست والاتفاقية العربية لمكافحة الجريمة المعلوماتية.

لقد المشرع الجزائري أساليب تحقيق متخصصة، منها التأكيد على دور الشرطة القضائية ومقدمي الخدمات في التحقيق في الجرائم المعلوماتية وكذا استعمال كافة الأساليب المادية والإجرائية أثناء تفتيش مسرح الجرائم المعلوماتية وكذا أساليب وآليات الإثبات ومنها: المعاينة، الشهادة والخبرة وأخيرا ضبط الأدلة الالكترونية بالإضافة إلى الآليات المستحدثة كالتسرب الالكتروني ومراقبة الاتصالات.

تتطلب هذه التحقيقات في الجرائم المعلوماتية مزيجا من الخبرة التقنية والقانونية، وكذلك التعاون المحلي والدولي لضمان جمع الأدلة بطريقة صحيحة ومقبولة قانونيا.

# الخاتمة

**الخاتمة :**

بناء على ما سبق ذكره في دراستنا للجريمة المعلوماتية نخلص أن هذه الأخيرة من أخطر الجرائم المستحدثة لما لها من خصائص ومميزات في مجابهة القوانين والقضاء وكافة الوسائل القانونية لمواجهتها.

ونظرا لخصوصية الجريمة المعلوماتية، فقد اختلفت المفاهيم حولها لذلك يصعب وضع تعريف عام وشامل وموحد فإن المفاهيم المحيطة بها تعتمد على الجهة التي ترى منها وبعضها يعرف على أساس ارتكاب الجريمة، والبعض الآخر على أساس مكان أو موضوع الجريمة، أو صفة الفاعل، وما يميزها أنها جرائم عابرة للحدود وترتكب في فضاء الكتروني ويتم تنفيذها بسرعة، ويتميز الفاعل الالكتروني بالذكاء والمهارات والمعرفة. ولم تتمكن القوانين والأنظمة القانونية لمواجهتها نظرا للعدد الهائل من هذه الجرائم المستحدثة، حيث أصبح مبدأ لا جريمة ولا عقوبة إلا بنص "لا يتسع لمحاربة هذا النوع من الجرائم".

وبالرغم من اهتمام المشرع الجزائري بالجرائم المعلوماتية والعقوبات المنصوص عليها فإن القانون الجنائي أو القانون 09-04 وحده لا يكفي لمواجهة انتشار هذا النوع من الجرائم المعلوماتية، بل يستوجب سن نصوص قانونية خاصة بهذه الجريمة، مع مراعاة خصوصية مرتكبيها ووسائل ارتكابها وتحديد شروط هذه الجرائم والعقوبات المقررة لها، مع تشديد العقوبات نظرا لسلبية هذه الأخيرة وتأثيرها على خصوصية الشعب وأمن الدولة.

**النتائج:**

1- تنعكس الطبيعة الخاصة للتحقيق في هذه الجرائم لأهمية الأجهزة المخصصة لها والاعتماد على الوسائل الحديثة للمساعدة في الكشف عن الجرائم وتحقيق أهدافها.

2- تستخدم الجريمة المعلوماتية تقنيات علمية وأخرى عملية تتطلب نطاقا واسعا من المعرفة المعلوماتية والخبرة الكافية في أجهزة الكمبيوتر.

3- قلة الخبرة لدى المسؤولين القضائيين وأجهزة العدالة وخاصة الأجهزة الأمنية وبشكل عام، ويرجع ذلك إلى النقص أو عدم الملائمة فيما يتعلق بالثقافة الرقمية، وأنظمة الاتصالات التقنية والبنية التحتية الحديثة التي تساعد في كشف الجرائم الالكترونية ومحاكمة مرتكبيها.

4- تجلب الجرائم المعلوماتية العديد من الصعوبات للحصول على أدلة جنائية فاعتاد المحققون على أن تكون مسرح الجريمة أشياء مادية ملموسة.

5- سهولة إتلاف واختفاء الدليل الرقمي.

6- عدم اكتمال القواعد والتشريعات الإجرائية التي يجب إتباعها أثناء مرحلتي التحقيق والمحاكمة، كما أن قدرة القاضي في تقدير الدليل غير كافية.

**التوصيات:**

1- الدخول في اتفاقيات دولية ثنائية لتسليم المجرمين المعلوماتيين.

2- لابد من تأهيل ضباط الشرطة والمحققين حتى يتمكن كل منهم على التعامل مع مثل هذه الجرائم.

3- ضرورة قيام المشرعين بصياغة تشريعات خاصة بجرائم الكمبيوتر وصياغة القواعد والإجراءات الجنائية لطبيعتها الخاصة.

4- تشديد العقوبات والغرامات على جرائم المعلوماتية والتعامل مع الجرائم العمدية والغير عمدية.

5- التركيز على الموارد البشرية المخصصة لمكافحة الجرائم المعلوماتية.

6- توحيد القوانين الوطنية في الولايات القضائية لمكافحة الجرائم المعلوماتية على النحو المنصوص عليه في الاتفاقيات الدولية.

7- وضع المزيد من النصوص والتشريعات الخاصة بالجرائم المعلوماتية.

8- ضرورة تأهيل وتدريب القضاة لتمكينهم من التعامل مع الأدلة الرقمية الناتجة عن الجرائم المعلوماتية حتى تكون الأحكام أكثر عدلا.

# قائمة المصادر والمراجع

## قائمة المصادر و المراجع :

*** القرآن الكريم :**

1)- سورة يوسف – الآية 26.

**أولا : المصادر :**

*** الاتفاقيات :**

*** القوانين و الاوامر:**

1) الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، بودابست، 2016.

2) أمر رقم 66-155، 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بالأمر رقم 20 الموافق 30 أوت 2020، ج.ر، عدد51، الصادرة بـ 31 أوت 2020.

3) قامت وزارة البريد والاتصالات السلكية واللاسلكية في الجزائر بنشر دليل علمي للأولياء والأوصياء والمربيين يتعلق بحماية الأطفال عبر الانترنت في 5 جويلية 2020.

4) القانون 15/04 المؤرخ في 2004/11/10، يعدل ويتمم الأمر 155/66، المؤرخ في 1966/6/08 المتضمن قانون العقوبات، ج.ر، الجزائر، العدد 71، سنة 2004.

5) قانون 09-04 المؤرخ في 5 أوت 2009، تتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، عدد 47 الصادرة بـ 16 أوت 2009.

6) القانون 18-05 المؤرخ في 2018/5/10، المتعلق بالتجارة إ، ج.ر، الجزائر، العدد 28، سنة 2018.

7) قانون 18-07 المؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات، عدد 34، الصادر في 2018./07/10

8) قانون رقم 15-03، المؤرخ في 01 فيفري 2015 المتعلق بعصرنة العدالة، ج.ر، عدد 06، الصادرة بـ 10 فيفري 2015.

9) المادة 10 و 11 و 12 من قانون 09-04.

10) المادة 14 من قانون الإجراءات الجزائية المعدل والمتمم بموجب الأمر رقم 02/15، ج.ر،ج.د.ش، العدد 49.

11) المادة 15، من قانون الإجراءات الجزائية المعدل والمتمم بموجب أمر 02./15

12) المادة 2 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ج.ر، عدد 47، 16 أوت 2009.

13) المادة 01/228 من قانون الإجراءات الجزائية.

14) المادة 5، الفقرة 2 و3 من قانون 09-04.

15) المادة 6 من قانون 09-04.

16) المادة 64، والمواد من 44 إلى 47 من قانون 06-22 المؤرخ في 20 ديسمبر يعدل ويتمم الأمر رقم 66- 155، العدد 84، الصادرة في 24-12-2006.

17) المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري.

18) مؤتمر فيينا في الفترة من 17/10 نيسان 2000.

**ثانيا : المراجع :**

*** الكتب :**

1) الغافري حسين بن سعيد، السياسة الجنائية في مواجهة جرائم الانترنت، القاهرة، دار النهضة العربية، 2009.

2) محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، 2018.

3) محمد لموسخ، تنازع الاختصاص بالجرائم المعلوماتية دفتر السياسة والقانون والجزائر، دار المنظومة، الجزائر، عدد2، 2009.

4) محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، ط1، مركز الدراسة العربية، مصر، 2016.

5) المقصودي محمد بن أحمد بن علي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا، الخليج العربي، دار المنظومة، 2015.

6) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ط 1، مطابع الشرطة، القاهرة، 2009.

7) ممدوح عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006.

8) نمور محمد سعيد، أصول الإجراءات الجزائية، دار الثقافة للنشر والتوزيع، الأردن، 2005.

9) نهلا عبد القادر المؤمني، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، ط2، دار الثقافة، 2010.

10) إبراهيم ممدوح، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، سنة 2009.

11) أحمد حمود وآخرون، الأدلة الالكترونية من الناحيتين القانونية والتقنية، هيئة مكافحة الفساد، جامعة بيزيت، فلسطين، 2015.

12) عائشة بن قارة، حجة الدليل الإلكتروني في مجال الإثبات الجنائي، د ط، دار الجامعة الجديدة، الإسكندرية، 2010.

13) أحمد خليفة الملط، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2006.

14) أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، 2015.

15) عصام أحمد البهجي، حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية، دار الجامعة الجديدة، الإسكندرية، سنة 2005.

16) بن فريحة رشيد، ميهوب يوسف، التحري الجنائي في مسرح الجريمة الالكترونية، جامعة عبد الحميد بن باديس، الجزائر، 2015.

17) حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، مصر، 2017.

18) خالد داودي، الجريمة المعلوماتية، ط1، دار الإعصار العلمي، الجزائر، سنة 2018.

19) رامى متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة، مصر، 2011.

20) رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، المكتب الجامعي الحديث، الإسكندرية، 2018.

21) زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى، عين مليلة (الجزائر)، 2011.

22) طه إبراهيم قسم السيد أحمد، الجريمة المعلوماتية في القانون السوداني، ط 1، السودان، سنة 2015.

23) عبد العالي خراشي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الإسكندرية، 2006.

24) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، مصر، دار الكتب القانونية، المجلة الكبرى، ط1.

25) عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية، دار الخلدونية، الجزائر، 2017.

26) على عدنان الفيال، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة )، المكتب الجامعي الحديث، مصر، 2011.

27) علي أحمد عبد، حق الخصوصية في القانون الجنائي (دراسة مقارنة)، المؤسسة الحديثة للكتاب، ط1، طرابلس، 2006.

28) فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون للنشر والتوزيع، ط 1، مصر، 2010.

29) فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016.

- **مذكرات والرسائل الجامعية:**

1) – إبراهيمي سهام، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2007/2004.

2)– براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة مولود معمري، .2012

3)– سفيان سوير، الجرائم المعلوماتية، مذكرة شهادة الماجستير في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011/2010.

4)– أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021./2020

5)– محمد صلاح محمد عبد المنعم، الجزائر الالكترونية وتحدياتها، أطروحة دكتوراه، جامعة المنصورة، كلية الحقوق، سنة .2017

6)- بدودة عزيزة، علالي سعاد، التحقيق الجنائي في الجرائم المعلوماتية، مذكرة ماجستير، كلية الحقوق، جامعة غرداية، 2018/2017.

7)- طاهر محمود أبو قاسم، الجرائم المعلوماتية، صعوبات وسائل التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، .2019

8)- بوعرعارة إبراهيم زياد، خصوصية الجرائم المعلوماتية، مذكرة لنيل شهادة ماستر، تخصص جنائي، جامعة غرداية، 2022./2021

9)- نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، أطروحة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، .2017

10)- بوبقرة خيرة، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة عبد الحميد بن باديس، مستغانم، 2020./2019

11)- يعقوبي زهرة، المعاينة والخبرة في الإثبات الجنائي، رسالة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2022/2021.

12)- هلالة آمنة، الإثبات الجنائي بالدليل الإلكتروني، مذكرة ماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة، 2015/2014.

13)- بن لاعنية عقيلة، حجية أدلة الإثبات الجنائية الحديثة، رسالة ماجستير، كلية العلوم الجنائية، الجزائر، 2012./2011

14)- مرابطين علاء الدين ومحمادي مراد، خصوصية الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة البشير الإبراهيمي، برج بوعريريج، 2023./2022

15)- نبيلة هبة هرول، الجوانب الإجرائية لجرائم الانترنت في مرحلة قمع الاستدلالات، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية.

16)- بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021.

17)- دلال مولاي ملياني، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018/2017.

18)- عثمان جبر محمد عاصي، ضمانات المشتكي عليه في التحقيق الجزائي الابتدائي، رسالة ماجستير، كلية الدراسات الفقهية، جامعة آل البيت، الأردن، 1998.

- **المقالات :**

1) بن مالك أحمد، خصوصية الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 8، العدد 1، سنة 2021.

2) إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، العدد 10.

3) أيمن عبد الله فكري، الاستجواب الجنائي الالكتروني، مجلة البحوث الفقهية والقانونية، العدد 43، غزة، 2023.

4) وهيبة رابح، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد 4، 2014.

5) بوضياف إسماهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، العدد 11، 2018.

6) عادل بدريدي، دور الشهادة الإلكترونية، مجلة النبراس للدراسات القانونية، المجلد 1، العدد 1، 2016.

7) محمد نظمي صعبانة، مدى حجية الشهادة عند الوسائل الإلكترونية في قانون البيانات الفلسطيني، مجلة جامعة الأزهر، المجد 19، العدد 5، غزة.

8) بلجراف سمير، سلطة القاضي في قبول وتقدير الأدلة الرقمية، مجلة الدراسات القانونية المقارنة، مجلد 7، العدد 61، الجزائر، 2021.

9) عيدة بلعاد، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة الآفاق العلمية، المجلد 11، العدد 11، 2019.

10) مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المجلد6، العدد 3، 2023.

11) عزدين عمراني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد 4، سنة 2018.

12) بوجاوي صليحة، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص، المجلد 7، العدد 1، الجزائر، 2021.

13) عشاش حمزة، خضري حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، المجلد 06، العدد 02، الجزائر، 2020.

14) محمد عمر مصطفى، النتيجة وعناصر الجريمة، مجلة العلوم القانونية والاقتصادية، العدد 02، 1965.

15) فتحي بن جديد، حماية الحق في الخصوصية أثناء التعاقد عبر الانترنت، مجلة القانون، العدد 3، 2012.

16) خدوجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الالكترونية، مجلة الأستاذ الباحث للدراسة القانونية والسياسية، المجلد 1، العدد 08، 2017.

17) صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل، المجلد 24، العدد 2، الجزائر، 2018.

18) محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، المجلد1، العدد 1، 2009.

*** المنشورات:**

1) طاهر محمود أبو قاسم، الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، 2019.

2) فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2003.

*** المواقع:**

- www, new, bbc, co, uk / hi/arabic/news/newsied/1153000/1153/24-stm.

(1- https://www.startimes.com/?t:7417291.

(2- https://www.asjp.cerist.dz/en/downArticle/272/5/2/20452/

(3- https://el3arabi.com/%D48%A7%D9%84%D9%82.

# فهرس المحتويات

## فهرس المحتويات:

**ملخص :**

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة التي انتشرت بشكل كبير في الوقت الحالي بسبب الاستغلال السيئ للثورة التكنولوجية مما أدى إلى إظهار اهتمام متزايد لمكافحة الجرائم المعلوماتية من طرف الحكومات خاصة والعالم عامة وسد ثغرات الأنظمة المعلوماتية وتوفير الحماية اللازمة لها.

وتبنت الجزائر آليات جديدة للتحقيق من خلال تعديل قانون العقوبات بموجب القانون رقم 06-22 والقانون 09-04، أما عن أهم خصوصية لهذه الجريمة فيكمن في الطابع الإجرائي الذي احتل المرتبة الأولى في بعض الصعوبات والتي تكون في مشاكل الاختصاص القضائي وكذلك العوائق التي تواجه السلطات والأجهزة الأمنية في مباشرة البحث والتحري والتحقيق إضافة إلى ذلك خاصية الإثبات وصعوبة قبول الدليل الرقمي.

***Summary :***

***Cybercrime is considered one of the new crimes that has spread widely at the present time due to the bad exploitation of the technological revolution, which has led to a growing interest in combating cybercrimes on the part of governments in particular and the world in general and filling the gaps in information systems and providing them with the necessary protection.***

***Algeria adopted new investigation mechanisms by amending the Penal Code under Law No. 06-22 and Law No. 09-04. As for the most important specificity of this crime, it lies in the procedural nature, which ranked first in some of the difficulties, which are in problems of judicial jurisdiction, as well as the obstacles facing the authorities and agencies. Security in conducting research, investigation and investigation, in addition to the property of proof and the difficulty of accepting digital evidence.***