الجمهورية الجزائرية الديمقراطية الشعبية
الطارف–
وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد –
كلية الحقوق والعلوم السياسيـــة
قســـم الحقـــوق

مذكـــرة بعنـــوان:

# الجريمة المعلوماتية في التشريع الجزائري

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي تخصص: قانون جنائي وعلوم جنائية

إعداد الطالبتان:
- بوطويل نسيمة
- سوالمي سندس

تحت إشراف الأستاذ (ة):
خضار فايزة

لجنـــة المناقشـــة

| الاسم واللقـــب | الرتبـــة | الهيئة المستخدمـــة | الصفـــة |
|---|---|---|---|
| د/ بليدي دلال | أستاذة محاضرة أ | جامعة الشاذلي بن جديد | رئيسا |
| د/ خضار فايزة | أستاذة محاضرة ب | جامعة الشاذلي بن جديد | مشرفا ومقررا |
| د/ عماري حورية | أستاذة محاضرة ب | جامعة الشاذلي بن جديد | ممتحنا |

السنـــة الجامعيـــة: 2024–2025


بسم الله الرحمن الرحيم

# شكر وتقدير

أولا الحمد والشكر لله تعالى الذي ألهمنا وأعاننا ووفقنا على إتمام بحثنا هذا

والذي آمل أن نكون قد حققنا الغاية المرجوة منه

نتقدم بالشكر الجزيل في هذا المقام أولا إلى الدكتورة القديرة والأستاذة المحترمة

" خضار فايزة "

على قبولها مهمة الإشراف على مذكرة تخرجنا هذه

وهي التي لم تبخل علينا بنصائحها القيمة النابعة من تجربتها الطويلة في ميدان البحث العلمي

ومتابعتها المتواصلة لأطوار إنجاز هذا البحث

وصبرها الطويل علينا فلكي منا أستاذتنا الفاضلة أكى عبارات الشكر والتقدير.

كما لا يفوتونا أن نتقدم بالشكر

إلى كل أعضاء اللجنة المحترمة الذين وبالإضافة إلى انشغالاتهم

المتعلقة بأداء مهام تبليغ الرسالة العلمية

إلا أنهم أبو إلا أن يشاركوا في مناقشة هذا العمل

يدفعهم إلى ذلك هدف نبيل وهو تطوير مجالات المعرفة العلمية.

# إهداء

الحمد لله حُبًا وشكرًا وامتنانًا على البدء والختام...ها أنا أتوّج اللحظات الأخيرة من طريقٍ لم يكن سهلًا طريقٍ حمل في باطنه العثرات والتعب والاختبار طريقٍ مشيتُه بثبات حينًا، وبكيتُ فيه بصمتٍ حينًا آخر لكني كنتُ أوقن دومًا أن الله لا يُخيّب من أودع أمله فيه فالحمد لله على الصبر حين ضاق الطريق والحمد لله على القوة حين خذلتني طاقتي والحمد لله على الوصول بعد طول انتظار أهدي هذا العمل:

إلى أنيسة العمر وحبيبة الروح وأعظم نعم الله علي إلى التي ضمت اسمي بدعواتها في ليلها ونهارها وأضاءت بالحب دربي وأنارت باللطف والود طريقي وكانت لي سحابا ماطرا بالحب والعطاء الى من كانت ملجأي ويدي اليمين في هذه الرحلة "**جدتي الغالية**"

"إلى توأم روحي وبهجة أيامي،نبع الحنان، إلى من كانت لي أما وأبا في آن واحد،شكرا على صبرك على دفئك وعلى كل لحظة من عمرك منحتها لي دون انتظار مقابل "**أمي الحبيبة**"

إلى من لا ينفصل اسمه عن اسمي،الى الذي غاب جسده وبقيت روحه معنا ندعو له كما علمنا، ونمشي بما أوصانا.رحمه الله، وجعل مثواه في جنات النعيم **أبي الغالي" رحمة الله عليك"**

صاحب الحكمة والمواقف الأصيلة كل نظراتك وفخرك بي كانت وقودًا في طريقي، فشكرًا لك على كل شيء قدمته لي "**جدي العزيز**"

إلى الذين وقفوا كالجدار خلفي شكرًا لصلابتكم لدعمكم الصامت حينًا والمعلن حينًا آخر كنتم اليد التي رفعتني حين شعرت أنني لا أستطيع الوقوف وحدي كنتم السند الذي لا يطلب والحب الذي لا يتغير إلى من غمروني بحنانهم ووقفوا إلى جانبي في كل مراحل الحياة وكانت وقفاتكم تشبه الجبال في ثباتها بارك الله في وقفاتكم ومواقفكم التي لا تقدر بثمن

"**إلى اخوالي وخالاتي الغاليين على قلبي**"

إلي ضلعي الثابت وآمان أيامي إلى من شددت عضدي بهم فكانوا ينابيع أرتوي منها الي خيرة أيامي وصفوتها إلى قرة عيني إلى من شاركني الحزن والفرح إلى سندي الجميل في هذه الحياة " **إخوتي وأخواتي**"

وإلى كتاكيت العائلة ضحكاتكم تنعش القلب ووجودكم يبهج الأرواح أنتم فخر هذه العائلة وأملها الجميل

**أبناء اخوالي وخالاتي وأبناء إخوتي وأخواتي "كبارا وصغار"**

لزميلتي وصديقتي في إنجاز هذا البحث لكِ كل التقدير على الجهد المشترك، والدعم المتبادل كنّا كتفًا لكتف في هذه الرحلة فشكرًا لصدقك واجتهادك وروحك النقية

إلى كل شخص كان عونا وسندا (سواء من قريب أو بعيد) لوصولي إلى نهاية هذا المشوار إلى كل من أفاضني بمشاعره ونصائحه المخلصة إل كل أصدقائي وزملائي إلى رفقاء الدرب الذين عرفتهم في المواقف الصعبة أهديكم هذا الإنجاز وثمرة نجاحي الذي لطالما تمنيته أهدي هذا العمل لنفسي بعد سنوات من الجهد والسهر والتحديات ها انا اليوم أكملت وأتممت أول ثمرات نجاحي بفضل الله سبحانه وتعالى أولا ثم عائلتي لقد آمنت بقدراتي رغم التعب رغم ثقل الطريق رغم كل الصعاب التي واجهتها والتي لم أنسَى أن ما عند الله أجمل وأنّ الخير قادم لا محالة. وآخر دعوانا أن الحمد لله رب العالمين.

"**هذا التخرج ليس نهاية، بل بداية لطريق جديد**"

**بوطويل نسيمة**

# إهداء

من قال أنا لها "نالها" وأنا لها أن أبت رغما عنها أتيت بها.

نلتها وعانقت اليوم مجدا عظيما، فعلتها بعد أن كانت مستحيلة

كانت دروبا اسية وطرقا خسرت بها الكثير و لكني "وصلت"

الحمد لله حبا و شكراً و امتنانا

الحمد لله الذي بفضله أدركت أسمى الغايات أنظر لنفسي ولنجاحي كالذي ينظر إلى معجزته

إلى الحلم الذي طال انتظاره، تحقق بفضل الله وأصبح واقعا افتخر به.

إلى العزيز الذي حملت اسمه فخرا، يرد اسمي عاليا في عنان السماء حاملة شرف لقبك و بكل اعتزاز انا لهذا

الرجل إلى من كلله الله بالهيبة والوقار إلى من غرس في روحي مكارم الأخلاق

داعمي الأول في مسيرتي و سندي **"والدي الغالي"**

إلى من كانت الداعمة الأولى والأبدية ملاكي الطاهر من كان وجودها يمدني بالسعي دون ملل

إلى من ظلت دعواتها تضم اسمي دائما، القلب الحنون، معلمتي الأولى"امي ومحبوبتي وملهمتي"

ها أنا اليوم أهديك علما وشهادة تخليت عنها في سبيل رعايتي و تعليمي

ممتنة لأن الله اصطفاك من البشر أما لي.

أهديكم هذا الإنجاز الذي لولاكم لم يكن اهديكم مراحلي وانجازاتي كلها فالفضل والثناء للمولى ثم لكفاحكم

لأجلي وعطائكم الذي يضمد تعبي.

إلى خيرة أيامي و صفوتها إلى من مدت لي أياديهم وقت ضعفي وآمنوا بقدراتي إلى ضلعي الثابت وآمان أيامي

"اخوتي (و) جدتي"

إلى من تحلت بالإخاء و تميزت بالوفاء والعطاء رفيقة دربي و توأمي و مصدر سعادتي "أختي آية"

إلى الذين يبهجهم نجاحي ولكل من كان عونا وسندا لي في هذا الطريق لأصدقاء ورفقاء السنين وأصحاب

الشدائد والأزمات.

إلى شريكة الدرب والكفاح ما كنا لنصل لولا تشاركنا العمل والإرادة لك نصف هذا النجاح ونصف هذا الامتنان

رفيقة النجاح **نسيمة**

**سوالمي سندس**

# قائمة

# المختصرات

**قائمة المختصرات:**

| الكلمة | الاختصار |
|---|---|
| الجريدة الرسمية للجمهورية الجزائرية | ج.ر.ج.ج |
| الطبعة | ط |
| دون طبعة | د.ط |
| الصفحة | ص |
| من الصفحة.. إلى الصفحة.. | ص ص |
| قانون العقوبات | ق.ع |
| قانون الإجراءات الجزائية | ق.إ.ج |

# مقدمة

**مقدمة:**

لقد شهد الإنسان على مر العصور تطورا هائلا في مختلف جوانب الحياة، من الاقتصاد والعلوم إلى التنظيم مما جعل الحياة أكثر سهولة و مرونة، حيث الفضل في هذا التطور يشكل كبير يعود إلى التكنولوجيا الحديثة، لاسيما في مجال تقنية المعلومات، حيث أثبتت الحواسيب و شبكة الانترنت فعاليتها ودقتها وسرعتها في كافة المجالات خاصة مع تطور تطبيقات الذكاء الاصطناعي.

لكن في المقابل، لا يمكننا إغفال حقيقة أن الجريمة ظاهرة متأصلة في المجتمعات البشرية، وقد استغلت دائما هذا التطور لتعزيز قدراتها نشاطها، فالتاريخ ملئ بأمثلة سفك الدماء والجشع التي رافقت التقدم البشري، و رغم ذلك لا يزال الانسان يسعى جاهدا لبناء مستقبل، وتحاول التشريعات جاهدة وضع قيود لضمان الأمن وحفظ الحقوق الفردية والمجتمعية وبناء الثقة .

مع تغلغل تقنية المعلومات في حياتنا وتزايد استخدامها بدأت تظهر آثارها السلبية في شكل نوع جديد من الجرائم، التي لم يتفق الفقه الجنائي على تسمية موحدة لها نظرا لحداثتها، تتميز هذه الجرائم بخصائص فريدة تميزها عن الجرائم التقليدية سواء من حيث كيفية اكتشافها، نطاق وقوعها، عدد ضحاياها، طرق تنفيذها، أو استراتيجيات مكافحتها .

لقد أدى التطور التكنولوجي إلى ظهور فئة جديدة من المجرمين يختلفون عن المجرمين التقليديين، فالمجرم المعلوماتي غالبا ما يكون شخصا عاديا يعيش حياة طبيعية وقد يكون مثقفا ومهذبا لكنه في نفس الوقت يعيش حياة موازية مليئة بالأنشطة الإجرامية الخبيثة، فالمعلوماتية بما توفره من سهولة في الاتصال والوصول إلى المعلومات، مهمة التحكم في هذه الجرائم مما يشكل تحديا كبيرا للتشريعات في وضع استراتيجيات فعالة لمكافحتها، وقد دفع هذا الأمر معظم التشريعات إلى السعي لفهم هذه الجرائم وسن قوانين تتناسب مع طبيعتها.

**أهمية الدراسة:**

إن أهمية البحث في موضوع «الجريمة المعلوماتية في التشريع الجزائري» تبرز من حيث كونه من المواضيع الحديثة التي تحظى باهتمام كبير على المستويين الدولي و الوطني، مما يجعل التصدي لها ضرورة ملحة، فقد أفرز التطور التكنولوجي الهائل خاصة في مجال تكنولوجيا المعلومات والاتصالات بيئة خصبة لظهور أنواع و أنماط جديدة من الجرائم تتميز بالتعقيد والتنوع.

و تتجلي كذلك أهمية هذا البحث أيضاً في ارتباطه الوثيق بالأمن القومي والسيادة الرقمية، باعتبار أن الجريمة المعلوماتية تمثل تهديدا حقيقيا يمس مؤسسات الدولة وأفراد المجتمع على حد سواء.

الأمر الذي دفع المشرع الجزائري إلى سن قوانين و تشريعات تهدف إلى الحد والوقاية منها، كما تسعى الدراسة إلى تقييم مدى فعالية هذه النصوص القانونية ومدى تكيفها مع التحولات الرقمية المتسارعة.

**أهداف الدراسة:**

إن البحث في أي موضوع جاد ومهم لا محالة يراد من وراءه تحقيق هدف أو بالأحرى مجموعة من الأهداف، لذلك فإن بحثنا في الجريمة المعلوماتية في التشريع الجزائري، يرجى من وراءه تحقيق الأهداف الآتية:

- ❖ التعرف على المفهوم القانوني للجريمة المعلوماتية.
- ❖ التعرف على موقف المشرع الجزائري من الجريمة المعلوماتية في إطار قانون العقوبات وخارجه.
- ❖ التعرف على الهيئات المختصة لمكافحة الجريمة المعلوماتية.
- ❖ التعرف على أساليب التحري عن الجريمة المعلوماتية.

**أسباب اختيار الموضوع:**

لقد شجعت العديد من المستجدات القانونية والأحداث الراهنة على عملية البحث في هذا الموضوع، دون أن ننسى الأسباب الشخصية التي ساهمت إلى حد كبير في اختيار هذه الدراسة دون سواها من المواضيع، وفيما يلي عرض لهذه الأسباب:

❖ **الأسباب الذاتية:**

إن البحث في أي موضوع لا بد أن ينطلق من إرادة ذاتية ورغبة شخصية في خوض غماره والاستمتاع بالبحث في جزئياته وتفاصيله، ولعل السبب الأبرز يكمن في ميولنا الشخصي لمثل هذا النوع من المواضيع، إضافة إلى أن الموضوعات التي تثير الاهتمام للبحث فيها هي تلك التي لا تحظى بالدراسة بالرغم من أهميتها، ومن هذا المنطلق كانت الرغبة جامحة للخوض فيه على الرغم من الصعوبات التي تحيط به.

ويمكن إضافة سبب آخر يتمثل في الرغبة الشخصية في متابعة الاهتمام بالمواضيع المرتبطة بالتكنولوجيا خاصة مع تطور تطبيقات الذكاء الاصطناعي.

❖ **الأسباب الموضوعية:**

إن البحث في موضوع الجريمة المعلوماتية في التشريع الجزائري يرجع إلى الأسباب الموضوعية التالية:

- يعد موضوع الجريمة المعلوماتية من المواضيع القانونية المستحدثة التي فرضت نفسها بقوة في الساحة التشريعية نتيجة التطور في تكنولوجيات الإعلام والاتصال، مما تترتب عليه مجموعة من التغييرات في طبيعة النشاط الإجرامي ووسائله، هذا ما دفع بالقانونيين والباحثين إلى تقديم اقتراحات تقضي بضرورة إعادة النظر في المنظومة التشريعية التقليدية.

**إشكالية الدراسة:**

ينطلق الإشكال الرئيسي من الدراسة من التقدم الهائل الذي أضحى واضحا في المجال التكنولوجي، والريادة عدد مستخدمي التكنولوجيا والأجهزة الحديثة من أشخاص طبيعيين أو هيئات، كل ذلك ساهم في ظهور أنواع جديدة من الإجرام المرتبط بالتكنولوجيات منها الجرائم المعلوماتية، ونظرا لتزايد نسب ارتكاب هذه الجريمة في الآونة الأخيرة، الأمر الذي دفعنا لدراسة هذا الموضوع وتتمحور الإشكالية في: **ما مدى فعالية المنظومة القانونية التي سنها المشرع الجزائري في مكافحة الجريمة المعلوماتية؟**

ويتفرع من هذه الإشكالية الرئيسية التساؤلات الفرعية الآتي ذكرها:

- ما المقصود بالجريمة المعلوماتية؟
- فيما تتمثل أبرز الآليات المؤسساتية المختصة في الكشف عن الجريمة المعلوماتية؟
- فيما تتمثل أهم أساليب التحري عن الجريمة المعلوماتية؟.

**الدراسات السابقة:**

- رسالة ماجستير: " الحماية الجنائية للمعطيات في المجال المعلوماتي" جامعة غرداية،كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021-2022 ، تناولت فيها الباحثة الجرائم الخاصة بأنظمة المعالجة للمعطيات الواردة في قانون العقوبات، هذه الدراسة كانت اللبنة الأولى للدراسة مع تحيينها بآخر تعديلات قانون العقوبات.
- رسالة ماجستير: "مكافحة جرائم تكنولوجيات الإعلام والاتصال على ضوء قانون 09-04" بجامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، أحمد مسعود مريم سنة 2012-2013 تناول فيها الباحث الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وآليات مكافحتها التي جاء بها القانون 09-04، هذه الدراسة اقتصرت على القانون رقم 09-04 في حين توسعت دراستنا أكثر و شملت قوانين أخرى.
- أطروحة الدكتوراه:" آليات البحث والتحقيق في الجرائم المعلوماتية "، جامعة باتنة 1، كلية الحقوق والعلوم السياسية، قسم الحقوق، ربيعي حسين، سنة 2015-2016 ، حيث تناول الباحث طرق الكشف عن الجريمة المعلوماتية، و التي اعتمدت في جزء من المذكرة مع التفصيل أكثر فيما يخص موضوع الجريمة المعلوماتية.
- شنبر خضرة: "الآليات القانونية لمكافحة الجريمة الإلكترونية"، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة أحمد دراية، أدرار، 2020-2021، هذه الدراسة كانت شاملة مع الحرص من خلال هذه المذكرة على آخر تعديلات قانون العقوبات.

**صعوبات الدراسة:**

الصعوبات التي واجهتنا في إعداده والمتمثلة في:

- تأخرنا في تحضير المذكرة مما نجم عند صعوبة في تحضيرها و كتابتها.
- طبيعة الموضوع في حد ذاته وعدم معالجته بآخر التعديلات القانونية.
- الجريمة المعلوماتية متشعبة في عدة مجالات منها القانوني التقني (مجال الحواسيب و الأنترنت)...

**منهج الدراسة :**

❖ **المنهج الوصفي :**

لقد كان استعمال هذا المنهج ضروريا لتوضيح عدة مفاهيم وتحديد معانيها ومدلولاتها للوقوف على مقاصدها و أهميتها كجزء فاعل في موضوع الدراسة .

❖ **المنهج التحليلي :**

لقد كان للمنهج التحليلي دور بارز في هذه الدراسة من خلال تحليل النصوص القانونية المتعلقة بالجريمة المعلوماتية، لاسيما القوانين العقابية و القوانين المتممة لها، ومقارنتها أحيانا بالتجارب الدولية، مما يسمح بتقييم فعالية هذه النصوص وقدرتها على التصدي للجرائم المعلوماتية.

**التقسيم العام لخطة البحث:**

قسم موضوع الدراسة وفقا لخطة ثنائية تفصيلها كما يلي:

- **الفصل الأول: تأطير المشرع للجريمة المعلوماتية**
- **المبحث الأول: الجرائم المعلوماتية في إطار قانون العقوبات**
- **المبحث الثاني: الجرائم المعلوماتية خارج إطار قانون العقوبات**
- **الفصل الثاني: آليات وإجراءات التحري في الجريمة المعلوماتية**
- **المبحث الأول: الوحدات المختصة في البحث عن الجريمة المعلوماتية**
- **المبحث الثاني: الإجراءات القانونية للكشف عن الجريمة المعلوماتية**

# الفصل الأول:

# تأطير المشرع للجريمة المعلوماتية

مع الانتشار الواسع لاستخدام تكنولوجيا المعلومات والاتصال في مختلف مجالات الحياة، برزت أنواع جديدة من الجرائم لم تكن مألوفة في المنظومة القانونية التقليدية، وهو ما استدعى تدخل المشرع الجزائري للتصدي لها من خلال تكييف النصوص القانونية أو سنّ نصوص جديدة. وقد تنوع هذا التدخل بين النصوص العامة في قانون العقوبات، ونصوص خاصة تعالج بعض الأفعال الإجرامية ذات الطابع المعلوماتي بشكل أكثر دقة.

وبناءً على ذلك، جاء هذا الفصل لتسليط الضوء على كيفية تأطير المشرع الجزائري للجريمة المعلوماتية، حيث نتناول في المبحث الأول الجرائم المعلوماتية التي نظمها ضمن قانون العقوبات، مثل جرائم الدخول أو البقاء غير المشروع وجرائم الحذف أو التغيير، ثم ننتقل في المبحث الثاني إلى الجرائم المعلوماتية التي عالجها المشرع خارج إطار قانون العقوبات، من خلال ثلاث مطالب: الجرائم المتعلقة بحقوق الملكية الفكرية، وتلك المرتبطة بحماية المعطيات الشخصية، إضافة إلى الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

## المبحث الأول: الجرائم المعلوماتية في إطار قانون العقوبات

أمام تزايد التهديدات المرتبطة باستخدام الأنظمة المعلوماتية، سعى المشرع الجزائري إلى إدراج نصوص قانونية ضمن قانون العقوبات تهدف إلى تجريم الأفعال غير المشروعة المرتكبة في الفضاء المعلوماتي، وذلك من أجل حماية سلامة النظم المعلوماتية والمعطيات الرقمية .ويُعد هذا التوجه بمثابة اعتراف صريح من المشرع بخطورة هذه الأفعال وضرورة التصدي لها ضمن الإطار الجنائي التقليدي.

وفي هذا السياق، يتناول هذا المبحث الجرائم المعلوماتية كما وردت في قانون العقوبات الجزائري، حيث سنعالج في المطلب الأول جرائم الدخول أو البقاء غير المشروع في نظام معلوماتي كصورة بسيطة، إلى جانب الحذف أو التغيير غير المشروع للمعطيات كصورة مشددة، لما تمثله من مساس مباشر بسرية وسلامة البيانات .أما المطلب الثاني، فنتطرق فيه إلى الجرائم التي تمس سلامة المعطيات أو الأنظمة المعلوماتية من خلال تخريب المعطيات في الفرع الأول، وإدخال المعطيات دون وجه حق في الفرع الثاني، باعتبارها من أخطر صور الجريمة المعلوماتية وأكثرها تهديدًا لأمن المعلومات.

### المطلب الأول: جرائم الدخول أو البقاء أو الحذف أو التعديل في منظومة المعالجة

أصبحت الجريمة المعلوماتية في الوقت الراهن من بين أخطر الجرائم المستحدثة التي فرضها التطور التكنولوجي الهائل في مجال استخدام الحواسيب وشبكات الإنترنت، حيث لم تَعُد ترتبط بمكان أو زمان محدّدين، بل أصبحت عابرة للحدود يصعب في كثير من الأحيان تتبّعها أو اكتشافها في الوقت المناسب .ومن بين أبرز صور هذه الجريمة، نجد أفعال الدخول أو البقاء غير المشروع في أنظمة أو شبكات معلوماتية، والتي تشكل انتهاكًا صريحًا لسرية وأمن هذه النظم.

وقد أولى المشرع الجزائري اهتمامًا خاصًا بهذا النوع من الأفعال، من خلال تجريم كل من يقوم بولوج أو الاستمرار في التواجد داخل نظام معلوماتي دون الحصول على الإذن المسبق من صاحبه، نظرًا لما يحمله هذا السلوك من تهديد مباشر للمصالح العامة والخاصة .وتتخذ هذه الجريمة صورتين : صورة بسيطة تتمثل في مجرد الدخول أو البقاء دون وجه حق، وصورة مشددة عندما تقترن الجريمة بأفعال خطيرة أخرى، كالحذف أو التغيير في المعطيات الإلكترونية.

وعليه، سيتم التطرق في هذا المطلب إلى جريمة الدخول والبقاء غير المشروع في نظام معلوماتي، من خلال التمييز بين الصورة البسيطة والصورة المشددة، وذلك في ضوء النصوص القانونية التي جاء بها التشريع الجزائري في مجال مكافحة الجرائم الإلكترونية.

**الفرع الأول: الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات**

تتمثل الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات في شكل الدخول (أولا) أو البقاء (ثانيا) غير المرخص بهما.

**أولا: جريمة الدخول:**

نص المشرع لجزائري على هذه الجريمة في المادة 394 مكرر من ق.ع.ج على أنه: " يعاقب بالحبس من ستة(06) أشهر إلى سنتين (02) أو بغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك"[1]ومن هن نستخلص من نص المادة أن المشرع الجزائري جرم فعل الدخول في كل أو جزء إلى المنظومة المعلوماتية بطريقة غير شرعية.[2]

تعد هذه الجريمة قائمة بمجرد دخول شخص ما عن قصد إلى نظام معلوماتي محمي سواء كانت لهدف معين أو لمجرد الاستطلاع. لم يحدد المشرع الجزائري وسيلة الدخول إلى نظام المعالجة الآلية للمعطيات (سواء كانت تقنية أو فنية).

[1] – المادة 394 مكرر من القانون رقم 24-06 المؤرخ في 19 شوال عام 1445 هـ الموافق لـ 28 أفريل 2024، يعدل ويتمم الأمر رقم 66-165 المؤرخ في 18 صفر عام 1386 هـ الموافق لـ 08 يونيو سنة 1966، المتضمن قانون العقوبات، ج.ر.ج.ج، العدد 30 المؤرخة في 21 شوال عام 1445 هـ الموافق لـ 30 أفريل سنة 2024.

[2] – زيدان زبيخة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص 49.

والهدف من الدخول لا يشترط أن يكون محدد بنتيجة معينة، بل مجرد الدخول غير المصرح يعد جريمة[1]، وعليه فالجريمة تتحقق بمجرد أن يكون الجاني عالما بدخوله إلى نظام معلوماتي لا يهمه ولا يخصه ومنه تقوم الجريمة حتى إذا لم يترتب على ذلك أي أضرار بالمعلومات.[2]

كما يفهم من نص المادة أن المشرع الجزائري لا يعاقب على الجريمة التامة فقط، وإنما يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية.

الجريمة لا تستوجب الدخول الكامل للنظام، بل يكفي الدخول إلى عنصر واحد أو منطقة ضيقة منه بشرط أن يكون هذا لعنصر جزءا من البرنامج الكلي للنظام.[3]

فجريمة الدخول هي جريمة نشاط أي جريمة خطر وليس جريمة ضرر لأنه لا يلزم لوقوعها تحقق ضرر من نوع معين.[4]

وتقع الجريمة من أي إنسان أيا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع الاستفادة من النظام أم لا، إنما فقط ألا يكون من أولئك الذين لهم حق الدخول إلى هذا لنظام.[5]

وعليه نص المادة 394 مكرر تضمنت شرط وحيد وهو أن يكون الدخول إلى منظومة المعالجة الآلية للمعطيات عن طريق الغش، أي دخول من دون وجه حق أو من دون ترخيص مسبق، أي لا يكون الدخول صدفة و لا عن طريق الخطأ.[6]

---

[1] – أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة للطباعة النشر والتوزيع، الجزائر، 2007، ص ص 107 110.

[2] – زيدان زبيخة، المرجع السابق، ص 49.

[3] – عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، تخصص إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح، ورقلة، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم علوم التسيير، 2019، ص 25.

[4] – شيماء عبد الغني محمد عطاالله، الحماية الجنائية للتعاملات الإلكترونية، د.ط، دار الجامعة الجديدة، الإسكندرية، 2007، ص 97.

[5] – عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتية، ط1، دار لفكر الجامعي، الإسكندرية، 2008، ص 82.

[6] – عمار حشمان، المرجع السابق، ص 26.

يشمل الدخول كافة الأساليب الاحتيالية المستخدمة لاختراق منظومة، سواء كانت محمية أو غير محمية، ويشمل أيضا استخدام شخص غير مخول للمفاتيح أو الوسائل المخصصة للدخول إليها.[1]

ويعرف الدخول غر المصرح به بأنه توجيه هجمات إلى بيانات أو خدمات الكمبيوتر بشكل غبر مشروع، مما قد يهدد سرية المعلومات أو سلامتها أو إمكانية الوصول إليه، وعليه هذا السلوك الإجرامي يستهدف المعلومات المخزنة بداخل النظام بهدف السيطرة عليها دون إذن صريح رسمي مما يعطل سلامة النظام أو يقلل من كفاءته.[2]

ولقد أصبح الدخول غير المشروع إلى الأنظمة الإلكترونية أولى المراحل في سلسلة لجرائم المعلوماتية[3]، حيث غالبا ما يتم التسلل إلى شبكات إلكترونية وحسب بيانات تخص حسابات خاصة

---

[1] – عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، جامعة أحمد دراية – أدرار–كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016-2017م، ص 28.

[2] – خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية،د.ط، الدار الجامعية، الإسكندرية، 2008، ص 84.

[3] – حيث ساهمت الهيئات والمؤسسات المهتمة بدراسة الجريمة المعلوماتية بوضع تعريف لها، ويعرف خبراء منظمة التعاون الاقتصادي والتنمية الجرائم المعلوماتية بأنها:"كل شلوك غير مشروع أو غير أخلاقي، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها".

– أما مؤتمر الأمم لمتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد تبنى التعريف الآتي للجريمة المعلوماتية أنها : " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

لمزيد من التفاصيل: أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، ط 1، مكتبة القانون والاقتصاد ، الرياض، 1435هـ/2014م.

التعريف التشريعي للجريمة الإلكترونية: في البداية، تجدر الإشارة إلى أن المشرع الجزائري لم يُعر اهتمامًا كافيًا لمجال الجريمة الإلكترونية في وقت سابق، حيث لم تكن هناك نصوص قانونية واضحة تنظم هذا النوع من الجرائم .غير أن هذا الفراغ القانوني لم يدم طويلًا، فقد سارع المشرع إلى تداركه من خلال إدراج نصوص قانونية تهدف إلى مواجهة هذه الظاهرة المتنامية.

وقد تجسد ذلك في القانون رقم 04-15 ، الذي جاء لتعديل قانون العقوبات الجزائري، حيث خصص قسماً جديداً تحت عنوان" القسم السابع مكرر"، تناول فيه الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات .كما تلاه لاحقاً صدور القانون رقم09-04 ، الذي وضع إطاراً قانونياً خاصاً للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومن المهم التنويه إلى أن مصطلح" نظام المعالجة الآلية للمعطيات "يُعد مصطلحاً تقنياً بامتياز، ما يجعل فهمه أمراً معقداً بالنسبة لغير المتخصصين في المجال التقني، كما أنه مفهوم متطور باستمرار نتيجة للتطور السريع في تقنيات الحوسبة.

لهذا السبب، فضل المشرع الجزائري – كما فعلت العديد من التشريعات الأخرى – عدم الخوض في تعريف دقيق لهذا المصطلح، وترك مهمة توضيحه لكل من الفقه والقضاء.

ولتفاصيل أكثر: عبد الرؤوف بوديسة بجاد، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري ،مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في الحقوق، تخصص : قانون الإعلام الآلي والانترنيت، جامعة محمد البشير الإبراهيمي– برج بوعريريج ،كلية الحقوق والعلوم السياسية، 2021/2022 ،ص ص10،11

بأفراد أو مؤسسات ليتم استغلالها لاحقا في لحصول على خدمات أو حتى لابتزاز أصحابها بفضح أسرارهم المالية.[1]

ومنه جريمة الدخول غير المشروع هي جريمة وقتية عل عكس جريمة البقاء في المنظومة المعلوماتية التي تعد من الجرائم المستمرة والتي سوف نتطرق إليها في العنوان الموالي.

**ثانيا: جريمة البقاء:**

حيث نصت عليها المادة 394 مكرر من ق.ع.ج تعد هذه الجريمة من الأنشطة الجرمية الأكثر انتشارا[2] يقصد بالبقاء غير المصرح به استمرار التواجد داخل نظام معلوماتي دون الحصول على إذن من مالكه مع العلم المسبق بعدم قانونية هذا البقاء، وقد اعتبر المشرع الجزائري الدخول إلى لنظام دون تصريح وكذلك الاستمرار أو البقاء فيه بدون إذن يشكلان جريمتين متساويتين من حيث الخطورة والمعاملة القانونية.[3]

يمكن القول أن البقاء غير المشروع داخل نظام معلوماتي قد يشكل جريمة مستقلة عن جريمة الدخول، إذ يمكن أن يكون الدخول في ذاته مشروعا بينما يتحول البقاء بعد ذلك إلى فعل معاقب عليه إذا تم بدون إذن وفي بعض الحالات، قد يجتمع الدخول غير المشروع مع البقاء غير لمشروع، كما لو أن الجاني لا يملك أي حق في الولوج إلى لنظام فيقوم بالدخول دون إذن، ثم يواصل التواجد داخل النظام دون وجه حق، مما يحقق تلازما ماديا بين الجريمتين.[4]

تعد جريمة البقاء غير المشروع داخل نظام معلوماتي امتدادا أو استمرارية لجريمة الدخول غير المشروع إليه، أو قد تشكل تعديا على الحق الممنوح بالدخول من حيث تجاوز المدة الزمنية المحددة لذلك ويعد الركن المادي في هذه الجريمة بمثابة فعل لا حق ومكمل للدخول غير المشروع، ويتمثل في الحالات

---

[1] – شيماء عبد الغنى محمد عطا الله، المرجع السابق، ص 119.

[2]– بن زرت آسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر، القانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2019، ص 14.

[3] – عمار حشمان، المرجع السابق، ص 26.

[4] – فريال العاقل، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، جامعة أكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014-2015، ص 33.

التي يكون فيها الدخول إلى النظام مشروعا في بدايته، لكن يتبعه بقاء غير مبرر وغير صريح، ويظهر ذلك من خلال حرمان الشخص من الحق في الاستمرار داخل النظام، وبالتالي فإن استمراره يشكل خرقا لهذا الحق وقد يقع هذا الفعل إما عن طريق المصادفة أو نتيجة الخطأ، كأن يجد الفرد نفسه داخل النظام ويقرر البقاء دون إنهاء الاتصال به وتعد هذه الجريمة من الجرائم الشكلية التي لا يشتر فيها تحقق نتيجة معينة، كما أنها تصنف ضمن الجرائم المستمرة طالما استمر الفاعل في تواجد داخل النظام بشكل غير قانوني، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية.[1]

هذا البقاء يعد خروجا عن الإذن الممنوح له، ويمكن أن يكون بداية لتحول هذا لتواجد إلى نشاط إجرامي.ففي بعض الحالات، يبقى الشخص في النظام رغم أن مهمته قد انتهت، مما يشكل تهديدا أمنيا للنظام وغالبا ما لا يكون هذا البقاء مبررا، ويعد غير مشروع قانونا وهنا تظهر خطورة هذه التصرفات، لأنها قد تتيح للمخترق أو الموظف غير المصرح له استخدام النظام لأغراض شخصية أو ضارة، مثل الحصول على بيانات أو تعطيل العمل، وقد عبر المشرع عن ذلك بوضوح حيث وصف البقاء غير المشروع في النظام بأنه تصرف يخالف القانون ويستوجب التدخل.[2]

يعد فعل البقاء في نظام المعالجة الآلية للمعطيات كحال الدخول، ويمكن القول أن البقاء غير المشروع قد يأخذ شكلين مختلفين:

- **الشكل 01**: يتمثل في حالة يكون فيها الدخول إلى لنظام مشروعا سواء تم ذلك عن طريق الخطأ أو بالصدفة، إلا أن الجانب وبعد أن يدرك أن وجود داخل النظام لم يعد مبررا، لا يغادره بل يستمر في استغلاله فيتحقق بذلك عنصر البقاء غير المشروع ويعاقب عليه.
- **أما الشكل 02**: فيكون حيث يرتبط فعل البقاء بفعل الدخول غير المشروع فيدخل الشخص إلى لنظام بدون إذن أو ترخيص، ثم يستمر في البقاء داخله وهذه الحالة أشد من الأولى، لأنها تنطوي على ارتكاب فعلين غير مشروعين معا: الدخول والبقاء.

[1] – عائشة نايري، المرجع السابق، ص ص 28،29.

[2] – شيماء عبد الغنى محمد عطا الله، المرجع السابق، ص 121.

الإشكال الذي يطرحه هذا التداخل بين الفعلين، هو كيف يمكن تحديد الزمن الفاصل بين نهاية جريمة الدخول وبداية جريمة البقاء؟ أي متى نعتبر أن الدخول قد تم ومتى يبدأ البقاء غير المشروع؟.

وقد تعددت الآراء الفقهية في هذا الشأن، فالبعض يرى أن جريمة البقاء تبدأ من لحظة الدخول نفسه، أي بمجرد أن يبدأ المتدخل في التنقل داخل النظام، فإن جريمة الدخول تكون قد اكتملت وتبدأ جريمة البقا، في حين يرى رأي آخر أن جريمة البقاء لا تتحقق إلا من اللحظة التي يدرك فيها الفاعل أن وجوده في النظام غير قانوني ورغم ذلك لا ينسحب منه.

وكما كانت وجهات النظر المختلفة، فإن المشرع الجزائري من خلال المادة 394 مكرر ق.ع.ج(من القانون 24-06)[1]. تناول كلا الفعلين: الدخول أولا ثم البقاء، وكأنه يميز بينهما من حيث الطبيعة الزمنية فالدخول يفهم على أنه جريمة وقتية نظرا لقصر مدتها في حين أن البقاء يصنف كجريمة مستمرة تمتد في الزمن مقارنة بالفعل الأول.[2]

ومنه نستخلص من نص المادة 394 مكرر ق.ع.ج أن هذه الجريمة (فعل الدخول أو البقاء غير المرخص بهما) قبل تعديل ق.ع.ج (04-15)[3]كانت أقل صرامة حيث أن العقوبة هنا كانت نوعا ما خفيفة على المجرم مقارنة بالتعديل الجديد الذي جاء به ق.ع.ج، حيث كان قبل التعديل من يقوم بالدخول أو البقاء عن طريق الغش في كل جزء من المنظومة الآلية للمعطيات، أو حتى يحاول ذلك يعاقب بالحبس من ثلاثة (03) أشهر إلى سنة (01) وبغرامة تتراوح بين 50.000 دج و 100.000 دج ، أما بعد التعديل ارتفعت بشكل كبير لتصبح الحبس من ستة (06) إلى سنتين (02) وبغرامة من 60.000 دج إلى 200.000 دج ومنه نلاحظ أن العقوبة تضاعفت وارتفعت بشكل ملحوظ ففي السابق ربما لم تكن هذه الجرائم شائعة بنفس القدر التي هي عليه الآن، لكن مع الاعتماد المتزايد على الرقمنة في جميع مناحي الحياة أصبح أي اختراق للأنظمة المعلوماتية يمكن أن يتسبب في أضرار بالغة

[1] – القانون 24 – 06، مصدر سابق

[2] – عمار حشمان، المرجع السابق، ص ص 27، 28.

[3] – القانون رقم 04- 15 المؤرخ في 10 نوفمبر 200، يعدل ويتمم الأمر رقم 66-166 المؤرخ في 08 يونيو 1966، المتضمن أحكام المساس بأنظمة المعالجة الآلية للمعطيات، ج.ر.ج.ج، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

على الأفراد والمؤسسات، وهذا التعديل الذي طرأ على ق.ع.ج يشمل الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات.

**الفرع الثاني: الصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات**

يشدد المشرع الجزائري العقوبة على جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات إذا نجم على ذلك نتائج معينة وهي حذف أو تغيير بيانات النظام، حيث نص على هذه الصورة المشددة للجريمة في مادة 394 مكرر ف 2 من ق.ع.ج، وعليه سوف نطترق إلى هذه الصورة فيما يلي الحذف (أولا) والتغيير أو التعديل(ثانيا).

**أولا: الحذف:**

نصت عليها المادة 394 مكرر في الفقرة 2 من ق.ع.ج على أنه " تضاعف العقوبة أذا ترتب على ذلك حذف أو تغيير المعطيات".

ويقصد بذلك حذف البيانات المخزنة على وسيط مادي داخل نظام المعالجة الآلية أو تدمير هذا الوسيط نفسه، أو حتى نقل جزء من تلك البيانات من منطقة الذاكرة المخصصة لها، مما يؤدي إلى الإخلال بسلامة النظام ووظائفه.[1]

ويقصد بإزالة جزء من المعطيات المسجلة في الحاسب الآلي أو إضافة جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، ويمكن للمسؤولين عن حفظ البيانات أن يخفوا المعلومات المكلفين بحفظها داخل جهاز الحاسب الآلي وذلك عن طريق إتلاف المعلومات أو محوها. كما يرى البعض أن محو البيانات يمكن أن يتحقق عن طريق التلاعب.[2]

[1]- أمال جابت، الجريمة المعلوماتية في التشريع الجزائري بين قانوني 09-04 و 04-15، العدد 25، المجلد 7، مجلة هيرودة للعلوم الإنسانية والاجتماعية، مؤسسة هيرودوت للبحث العلمي والتكوين، الجزائر، ، 2023، ص 58.

[2]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 93.

يقصد بالحذف عملية إزالة أو محو جزء أو كل البيانات المخزنة على وسائط معينة داخل النظام المعلوماتي، وقد يتم هذا المحو بشكل معتمد لهدف تدمير تلك البيانات أو إزالة أثرها أو بهدف نقلها وتخزينها في أماكن أخرى مثل الذاكرة الخاصة.[1]

شدد المشرع الجزائري العقوبة في هذه الجريمة مقارنة بالعقوبات السابقة،ومنه فإن حذف بيانات إلكترونية معينة يعني إسقاطها من موقعها داخل النظام المستهدف، حتى وإن كان ذلك بشكل مؤقت ما يجعل هذا الحذف ظرفيا وقابلا للاسترجاع عبر برامج متخصصة رغم أن هذه البرامج تعد معقدة بطبيعتها، ولكن حذف البرامج يهدف إلى القضاء عليها بشكل نهائي وكامل ولهذا السبب اعتبر المشرع الجزائري أن حذف البرامج أو محوها بالكامل يعد أكثر خطورة مما جعله يفرض أشد عقوبة على هذا الفعل مقارنة بالجرائم الأخرى.[2]

**ثانيا: التعديل (التغيير):**

نصت عليها المادة 394 مكرر في الفقرة 2 من ق.ع.ج "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة".

ونقصد به هو القيام بتعديل أو تغيير البيانات الموجودة داخل نظام المعالجة واستبدالها بيانات أخرى، ويكفي لتحقيق الجريمة وقوع أي صورة من صور التغيير دون الحاجة إلى توافرها مجتمعة.[3]

السبب الأساسي لتعديل بعض البرامج يكون في الغالب بهدف الاحتيال المالي أو اختلاس الأموال وغالبا ما تنتشر هذه التعديلات في مجال الحسابات ومثال على ذلك: أحد المبرمجين في أحد البنوك الامريكية قام بالتلاعب في برنامج الحسابات حيث أضاف دولارا واحدا على كل حساب يتجاوز رصيده عشرات دولارات، ثم قام بتحويل هذه الزيادات إلى حسابه الشخصي، أطلق على البرنامج المعدل اسم "ZAWICK" وتمكن من جني مئات الدولارات شهريا بهذه الطريقة، حيث

[1]- أمال قارة، المرجع السابق، ص 122.

[2]- علي إبراهيم بن دراج، محاضرات في الجرائم المعلوماتية، مطبوعة بيداغوجية مقدمة لسنة الثانية ماستر،تخصص قانون جنائي والعلوم الجنائية، المركز الجامعي، أفلو، معهد الحقوق والعلوم السياسية، قسم الحقوق، 2020-2021، ص 48.

[3]- أمال جابت، المرجع السابق، ص 58.

تم اكتشاف هذه الفعل الإجرامي بالصدفة أثناء محاولة البنك تقديم مكافأة لأول آخر عميل تابع للمؤسسات بمناسبة تأسيس شركة جديدة، مما أدى إلى كشف وجود حساب وهمي لا وجود له في الأساس.[1]

يقصد بالتعديل أي تغيير يجري على البيانات الموجودة داخل النظام، سواء بإبدالها بمعلومات اخرى أو بالتلاعب بها من خلال إدخال بيانات زائفة أو غير صحيحة باستخدام برامج خاصة صممت لهذا الغرض وغالبا ما يكون الهدف من هذا التعديل هو التأثير على نتائج النظام أو توجيهها بطريقة معينة. توجد العديد من الفيروسات تساهم في تعطيل النظام أو تعديل وظائفه مثل فيروس "حصان طروادة"، الذي يعد من أخطر الفيروسات كونه يستطيع اختراق الأنظمة وجمع المعلومات دون علم المستخدم، ومن هذه الفيروسات كذلك نجد "فيروس الدودة" الذي يتميز بقدرته على الانتشار بسرعة وتعطيل الأجهزة بشكل كامل.[2]

ومنه نلاحظ عند تحليل المادة 394 مكرر ف 2 من ق.ع.ج أن الصورة المشددة لنظام المعالجة الآلية للمعطيات طرأ عليها تعديلات .قبل تعديل 24-06 كانت العقوبة مضاعفة إذا ترتب على الدخول أو البقاء حذف أو تغيير معطيات المنظومة تضاعف العقوبة، وعليه فإن العقوبة الأصلية قبل لتعديل كانت (من 03 أشهر إلى سنة) ستصبح من (ستة أشهر(06) إلى سنتين) على سبيل المثال، أما بعد التعديل 24-06 فأن مبدأ مضاعفة العقوبة لا يزال قائما ولكن نظرا لزيادة العقوبة الأصلية فإن المضاعفة هنا ستؤدي إلى عقوبة أشبه بكثير مما كانت عليه في النص القديم.

فهذا التعديل يمثل رسالة واضحة وحازمة من المشرع بأن هذه الجرائم لم تعد تعتبر بسيطة وأن العقوبات الجديدة تهدف إلى الردع العام والخاص، بما يضمن حماية أفضل للبيانات والأنظمة المعلوماتية داخل وخارج الدولة.

[1]- عاصف أسماء، الجرائم الرقمية وطرق إثباتها، مذكرة نهاية الدراسة لنيل شهادة الماستر، تخصص قانون قضائي، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم قانون خاص، 2024، ص 48.

[2]- عبد الفتاح بيومي حجازي، المرجع السابق، ص ص 95،96.

## المطلب الثاني: تخريب وإدخال المعطيات

في ظل تطور الجرائم المعلوماتية وتنوع أساليب ارتكابها، أصبحت المعطيات الرقمية عرضة لاعتداءات متزايدة تهدف إلى التأثير على سلامتها أو التحكم فيها دون وجه حق .وتُعدّ المعطيات من بين أهم العناصر التي تقوم عليها الأنظمة المعلوماتية، مما يجعل المساس بها جريمة قائمة بذاتها تستوجب حماية قانونية فعّالة.

وقد أدرج المشرّع الجزائري ضمن نصوص قانون العقوبات، خاصة بعد التعديل بموجب القانون رقم09-04 ، مجموعة من الأفعال التي تُشكّل اعتداءً مباشرًا على المعطيات، سواء من خلال تخريبها وإتلافها أو عن طريق إدخال بيانات بطرق غير مشروعة داخل النظام .وتكمن خطورة هذه الجرائم في ما تسببه من أضرار تقنية وقانونية، فضلًا عن إمكانية استخدامها كوسيلة لارتكاب جرائم أخرى أكثر تعقيدًا.

وبناءً عليه، سيتناول هذا المطلب الجرائم المتعلقة بالمساس بالمعطيات، من خلال التطرق في الفرع الأول إلى جريمة تخريب المعطيات الإلكترونية، وفي الفرع الثاني إلى جريمة إدخال المعطيات غير المشروعة، وذلك في ضوء ما قرره المشرع الجزائري ضمن الإطار العام لقانون العقوبات.

### الفرع الأول: تخريب المعطيات

يشكل تخريب المعطيات أحد المظاهر الجرائم الإلكترونية التي تمس سلامة البيانات والمعلومات لرقمية، وقد تصدى له قانون العقوبات بنصوص خاصة، ويأتي ذلك في إطار حماية البنية التحتية المعلوماتية وضمان استقرار الأنظمة.

عالج المشرع الجزائري هذا النوع من الجرائم في المادة 394 مكرر الفقرة 2 من ق.ع.ج ويقصد بالإتلاف التسبب في جعل الشيء غير قابل للاستعمال أو القضاء على صلاحيته أو تعطيله عن أداء وظيفته سواء كان ذلك بشكل كلي أو جزئي.

وهو ما يقصد به تدمير نظام المعلومات[1] ونعني به تدمير البيانات بحيث تصبح للاستخدام ولا يقتصر هذا النوع على البرامج أو البيانات فحسب، بل يشمل أيضا الأجهزة والمكونات المادية للحاسوب(العتاد الصلب)وكذلك الأجهزة المتصلة به، مثل وحدات التخزين أو الشاشات وغيرها، ومن الجدير بالذكر أن هذا النوع من الإتلاف لا يشترط أن يكون الهدف منه الحصول على المال، بل يكفي أن يكون هناك ضرر مادي يلحق بالمعلومات أو الأنظمة. إن جوهر التخريب يتمثل في إتلاف الشيء أي تدمير المعطيات أو المعلومات وجعلها غير صالحة للعمل والعبرة في ذلك ليس بحجم الضرر وإنما بتأثير الفعل على وظيفة المال المعلوماتي، سواء أكان برنامجا أو جهاز أو بيانات.

ترتكب جرائم إتلاف البرامج والمعلومات عادة باستخدام ما يعرف بـ"القنابل المنطقية" أو عن طريق برامج "الدودة" و"الفيروسات" هذه الأخيرة هي برنامج خبيثة يتم إعدادها بواسطة أشخاص ذوي معرفة متقدمة بالبرمجة، يتميز هذا البرنامج بقدرته عل الانتقال إلى أجهزة الحاسب الآلي والتكاثر والانتشار فيها ويكون غير مرئي بالطرق لعادية، مما يتطلب أساليب علمية للكشف عنه.

تتسبب الفيروسات المنتشرة في الأجهزة المتصلة بالشبكات العامة والخاصة في تدمير البرامج والمعلومات المخزنة داخل الجهاز، يؤدي ذلك إلى تعطيله عن العمل وتضليل مستخدميه وضياع البيانات، وتحويل الجهاز إلى آلة صماء لا فائدة منها.[2]

ومنه نستنتج أن المادة 394 مكرر ف 3 المتعلقة بتخريب نظام اشتغال المنظومة فهي تستدعي موضوع أكثر خطورة قبل التعديل، أي في النص القديم كانت عقوبتها تتراوح بين ستة (06)أشهر إلى سنتين (02) وغرامة 50.000 دج غلى 150.000 دج، رغم أن هذه العقوبة مشددة إلا أنها قد لا تكون كافية لردع الجرائم التي قد تسبب أضرار جسيمة[3] ثم جاء تعديل 24-06 ليغير من العقوبة ويضاعفها أكثر ما كانت عليه لتصبح من سنة (01) إلى ثلاث(03) سنوات والغرامة من 100.000

[1]- أمال حابت، مرجع سابق، ص 57.

[2]- هبة الدزيري، جريمة الدخول الغير مشروع لنظام المعالجة الآلية للمعطيات، مذكرة نهاية الدراسة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2019-2020، ص 34.

[3]- القانون رقم 15- 04، مصدر سابق.

إلى 300.000 دج هذا الارتفاع يعكس إدراكا لأهمية حماية البنية التحتية الرقمية من التخريب الكامل.[1]

**الفرع الثاني: إدخال المعطيات**

يشكل إدخال المعطيات دون إذن قانوني صورة من صور الجرائم المعلوماتية التي تناولها القانون العقوبات، ويأتي ذلك لضمان حماية نظم المعلومات من التلاعب أو الإضرار بمحتواها.

يقصد بفعل الإدخال هنا قيام شخص ما بإدخال بيانات أو معلومات إلى النظام المعلوماتي دون أن يكون لديه الحق في ذلك غالبا ما يتم هذا الفعل من فبل موظف لديه صلاحيات في قسم الحاسب الآلي ويكون مطلعا على نظام التشغيل والبرمجيات ويستخدم معرفته تلك لزرع بيانات أو إجراء تغيرات على النظام بهدف إحداث ضرر معين، ومثال ذلك إدخال بيانات مغلوطة أو مزيفة عن الموظفين، كأن يتم تسجيل موظفين وهميين على أنهم يعملون في المؤسسة، وهم في الحقيقة غير موجودين وذلك بهدف سرقة الأموال المخصصة لرواتبهم.[2]

الإدخال هو عملية إضافة معلومات جديدة إلى النظام سواء كانت البيانات هذه موجودة سابقا أو لا ويتم هذا الفعل بنية الإخلال بسلامة البيانات أو التأثير على عمل النظام.[3]

الإدخال هو إضافة بيانات جديدة غير صحيحة إلى البيانات الموجودة في النظام، والتي تم معالجتها مسبقا بشكل آلي.[4]

عند مراجعة المادة 394 مكرر 1(04-15)[5] قبل وبعد تعديلها (24-06)، يبرز تغيير جوهري واحد وهو المتعلق بالمدة الحبسية، بينما ظلت الغرامة المالية ثابتة، فإن لتعديل يعكس موقفا أكثر صرامة من المشرع تجاه الجرائم المتعلقة بالتلاعب بالبيانات في أنظمة المعالجة.

---

[1]- القانون رقم 24-06، مصدر سابق.

[2]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 92.

[3]- أمال قارة، المرجع السابق، ص 121.

[4]- أمال جابت، مرجع سابق، ص 58.

[5] - القانون 04-15، مصدر سابق.

العقوبة الحبسية قبل التعديل (القانون 04-15) كانت تتراوح بين ستة (06) أشهر إلى ثلاث (03) سنوات بينما بعد التعديل أصبحت العقوبة من سنة (01) إلى ثلاث (03) سنوات فإن التغيير الذي طرأ على هذه المادة يحمل في طياته دلالات قانونية مهمة:

- ❖ زيادة الردع العام والخاص.
- ❖ رفع الحد الأدنى للعقوبة من ستة (06) أشهر إلى سنة كاملة يعني أن المشرع أصبح ينظر إلى جرائم إدخال معلومات بطريق الغش أو مزورة في نظام المعالجة الآلية للمعطيات بجدية أكبر مما يرسل رسالة واضحة بأن مثل هذه الأفعال لا يستهان بها.
- ❖ من الجدير بالذكر أن الغرامة المالية ظلت كما هي في كلا النصين، هذا يشير أن المشرع اعتبر هذا النطاق من الغرامات كاف لتحقيق الأهداف الردعية وأن التغيير الرئيسي كان ضروريا على مستوى العقوبة السالبة للحرية لتعكس خطورة الجريمة بشكل أفضل.
- ❖ يمكن القول أن التعديل الذي طرأ على المادة 394 مكرر 1 يمثل قفزة نوعية نحو سياسة جنائية أكثر صرامة في مواجهة مثل هذه الجرائم المتعلقة بالتلاعب بالمعطيات وأكثر ردعا.

قد يؤدي إدخال معلومات إلى نظام الحاسب الآلي بطرق غير مشروعة إلى التلاعب بذاكرة النظام، كما قد يترتب عليه تغيير أو إتلاف البيانات نفسها، مثل حذفها أو تدميرها بالكامل، وذلك كما يحدث عند إدخال برامج خبيثة تقوم بتعديل أو محو المعلومات المخزنة في النظام.

يعد إدخال البرامج الخبيثة أو البيانات المزيفة إلى نظام الحاسب الآلي أحد الأفعال التي تشكل جريمة إتلاف معلوماتي، حيث يمكن أن يؤدي ذلك إلى إضافة معلومات جديدة تؤثر سلبا على البيانات الأصلية سواء بتعديلها أو حذفها لاحقا.

ويعتبر التلاعب في مرحلة إدخال البيانات، وهي أولى مراحي تشغيل نظام المعالجة الآلية، من أسهل الطرق لتنفيذ هذا لنوع من الجرائم، إذ تحول البيانات في هذه إلى صيغة قابلة للقراءة والمعالجة من قبل النظام، مما يتيح فرصة إدخال بيانات غير صحيحة أو مزورة بسهولة ونظرا لأن الحاسب يخزن كل ما يقدم له دون تمييز بين الصحيح والخاطئ فهذا يسهل ارتكاب الاحتيال المعلوماتي.

ومن الأمثلة الواقعية على هذا النوع من التلاعب: قيام شخص بإدخال أسماء وهمية في سجلات الرواتب، ما يؤدي إلى صرف أجور شهرية لأشخاص غير موجودين، أو التعديل المعتمد في نسب الفوائد الخاصة ببعض لعملاء أو حتى تسجيل فواتير مزيفة باسم موردين وهميين بالإضافة إلى إدخال بيانات شخصية مزورة لأغراض غير مشروعة.[1]

## المبحث الثاني: الجرائم المعلوماتية خارج إطار قانون العقوبات

في ظل التطور التكنولوجي السريع وانتشار استخدام أنظمة الحاسوب وشبكات الاتصال، برزت ظاهرة الجرائم المعلوماتية التي تتخذ أشكالا متعددة تمس أنظمة المعالجة الآلية للمعطيات، وفي هذا السياق يتناول المبحث الثاني الجرائم المعلوماتية التي تقع خارج نطاق قانون العقوبات، حيث ستناول هذا الموضوع إطار حماية حقوق الملكية الفكرية (المطلب الأول) والمعطيات الشخصية (المطلب الثاني) والانتقال إلى الجريمة المعلوماتية المتعلقة بتكنولوجيات الإعلام والاتصال (المطلب الثالث).

### المطلب الأول: الجرائم المعلوماتية في إطار حماية الملكية الفكرية

وقع الجدل الفقهي في البداية حول اعتبار المعلوماتية حقا للمؤلف، فظهرت القوانين الخاصة بحماية حقوق المؤلف مع التطور التكنولوجي وانتشار المعلومات الرقمية، حيث كانت البداية في الولايات المتحدة الأمريكية بإنشاء مكتب حقوق المؤلف(Copyright Office) لتنظيم هذا المجال.

وفي فرنسا تم تعديل القانون رقم 86/66 المؤرخ في 03 يوليو 1986[2].

أما في الجزائر فلم يتم التطرق في البداية لهذا ألموضوع إلا أنه تم إصداره عدة أوامر لاحقا، من بينها: الامر رقم 14/73 المؤرخ في 03 أفريل 1973 والمتعلق بحقوق المؤلف والحقوق المجاورة ، والأمر

[1] – الطيبي البركة، الجماية الجنائية لنظام المعالجة الآلية للمعطيات– دراسة مقارنة–، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة دكتوراه الطور الثالث، تخصص قانون جنائي، جامعة أحمد دراية –أدرار–، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020– 2024، ص ص 190، 191.

[2] – الأمر 03-07، مؤرخ في 19 جمادى الأولى عام 1424، الموافق لـ 19 يوليو 2003، المتعلق ببراءات الاختراع، الجريدة الرسمية المؤرخة في 2003/07/19، العدد 44، ص 434.

رقم 05/03 الصادر في 19 يوليو 2003 [1] والذي جاء لتحديث وتعديل القانون السابق.وقد وضعت هذه القوانين لحماية المؤلفين والحد من الجرائم الإلكترونية المتعلقة البرمجيات والمصنفات الرقمية.

**الفرع الأول: جرائم تقليد المصنفات المعلوماتية**

لضمان حماية قانونية فعالة للمصنفات المعلوماتية، يجب أن يشمل القانون حق المؤلف والحقوق المجاورة، كما هو الحال بالنسبة للمصنفات الأدبية والإعلامية، وهذا يتماشى مع الاتفاقيات الدولية التي تؤكد على حماية الملكية الفكرية مثل اتفاقية التجارة العالمية وبما أن برامج الحاسوب تدرج ضمن هذه المصنفات المحمية، فإن أي استخدام غير مشروع لها يعد انتهاكا لحقوق المؤلف المعلوماتية، كما تكمن أهميته في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

وتجدر الإشارة إلى أن المشرع الجزائري كان مدركا لصعوبة تحديد المصطلحات القانونية الدقيقة لهذا النوع من الجرائم مما تطلب منه دقة كبيرة في صياغة لنصوص واختيار عنوان المادة: " القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"، حتى يكون النص مرنا قابلا للتكيف مع التطورات التقنية المتسارعة[2].

**أولا: أصناف جريمة التقليد:**

نستنتج من نص المادة 151 من الأمر رقم 05/03 وجود جرائم تعتبر من جنح التقليد ويمكن تصنيفها إلى ثلاث:[3]

❖ **الصنف الأول: الجنح التي تمس بالحق المعنوي للمؤلف.**

- لكشف غير لمشروع عن مصنف أدبي أو أداء في المادة 22 الأمر 05/03.

[1] - الأمر رقم 03-05، مؤرخ في 19 جمادى الأولى عام 1424، الموافق لـ 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية المؤرخة في 2003/07/19، العدد 44، ص03.

[2] - أحمد عمراني، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في التشريع الجزائري والمقارن، ع 16، مجلة الحضارة الإسلامية، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، جمادى الثانية 1433 هـ/ ماي 2012 م، ص 11-12.

[3] - الأمر 03-05، مصدر سابق.

– المساس بسلامة المصنف أو الأداء الفني في المادة 25 الأمر 05/03.

❖ **الصنف الثاني: الجنح المتعلقة بالحق المالي للمؤلف.**

– استنتاج مصنف بأي أسلوب من الأساليب في شكل نسخ مقلدة، هذا الصنف من جرائم التقليد هو الأكثر شيوعا في المجال المعلوماتي أي عملية استنتاج البرامج (النسخ غير الشرعي)[1].

– إبلاغ المصنف أو الأداء الفني للجمهور عن طريق التمثيل أو الأداء العلني أو البث السمعي أو السمعي البصري أو بواسطة التوزيع أو أية وسيلة أخرى لبث الإشارات الحاملة للأصوات أو أي نظام للمعالجة الآلية.

❖ **الصنف الثالث: الجنح المشابهة لجنحة التقليد.**

والمتمثلة في خمسة جنح متشابهة للتقليد، والتي يطلق عليها جنح البيع بالمفرق:

– استيراد النسخ المقلدة وتصديرها، لا يقتصر على واقعة النقل المادي للبرامج وإنما صلاحية النقل المعنوي لها سواء بالاستيراد أو التصدير عن طريق شبكات الحاسوب التي تربط العديد من الدول التي يطلق عليها شبكات الانترنت.

– بيع نسخ مزورة من المصنف(البرنامج).

– تأجير المصنف(البرنامج) مقلد أو عرضه للتداول.

– الجنحتين المتعلقتين بالمساعدة و المشاركة في المساس بحقوق المؤلف والرفض عمدا دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف المادة 154/115 الأمر 05/03.

**ثانيا: أركان جريمة التقليد:**

نخلص من هذه الأصناف الثلاث أن جريمة تقليد البرامج تستلزم لقيامها توافر العناصر التالية:

**1. الركن المادي:**

[1] – أمال قارة، المرجع السابق، ص 20.

❖ محل النشاط الإجرامي في جريمة التقليد بصفة عامة هو المصنف المحمي، وقد سبق وأن بين أن المشرع الجزائري قد اعترف لبرامج الحاسوب بصفة المصنف المحمي طبقا للمادة 04 من الأمر 03-05.

❖ النشاط الإجرامي يتمثل في الاعتداء على حق من حقوق المؤلف التالية دون موافقته على النحو التالي:

- **الاعتداء على الحق في الكشف عن المصنف:** لمؤلف برنامج الحاسوب حق اختيار الوقت والطريقة التي يراها مناسبة ليتم بها إذاعة أو نشر برنامجه، وعليه يتمثل الاعتداء عندما ينشر أو يذاع هذا البرنامج في وقت عبر الوقت الذي يراه ملائما أو بطريقة غير الطريقة التي يراها ملائمة له[1].
- **الاعتداء على الحق في سلامة المصنف:** يحمي المشرع جنائيا حق المؤلف في تعديل وتحويل أو تغيير أو حذف أو إضافة ترد على البرنامج من شخص آخر دون إذن من المؤلف، ومن يرتكب أحد الأفعال السابقة يتوافر في حقه النشاط الإجرامي لجريمة التقليد.

من يشتري برنامجا لاستغلاله في نشاط معين، فيصوره لاستغلاله في نشاط آخر بدون إذن المؤلف، أما التحويرات الطفيفة اللازمة للاستعمال العادي والمشروع للبرنامج مع تصحيح الأخطاء الواردة به[2] لا تشكل جنحة التقليد.

- الاعتداء على حق النسخ: كل اعتداء على حق المؤلف في استغلال ونسخ عدد من النسخ أكثر من العدد المتفق عليه، ويستوي أن يكون النسخ قد وقع كليا- النسخ الحر في الكامل copie serville، أو جزئيا - النسخ الحر في الجزئي copie pqrtielle أو بطريق الاقتباس plagiat أو التشويه denaturqtion عن طريق حذف أجزاء من البرنامج.

[1] – أمال قارة، المرجع السابق، ص 24.

[2] – علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، طبعة أولى، الدار الجامعية، بيروت، 1999، ص 24.

وتتوافر الجريمة أيضا سواء تم نسخ البرنامج باسم مؤلفه الحقيقي أم شخص آخر يخلق في الذهن لبسا حول مؤلفه الحقيقي أم باسم خيالي. والعبرة في تقدير وجود التقليد بأوجه الشبه لا بأوجه الاختلاف، أي بنقاط التشابه بين البرنامج الأصلي والبرنامج المقلد وليس نقاط الاختلاف بينهما، ويدخل تقدير ذلك في نقاط السلطة التقديرية لمحكمة ألموضوع وطبقا للمادة 53[1] من الأمر 05/03 فإنه يمكن قيام المالك الشرعي لبرنامج الحاسوب باستنساخ نسخة منه إذا كان النسخ ضروريا لاستعمال البرنامج للغرض الذي أكتسب من أجله ووفقا للشروط استعماله

كما أنه يمكن استنساخ نسخة أخرى لغرض التوثيق أو الحفظ (نسخة احتياطية) كإجراء أمني خشية الضياع أو التلف، والقانون يحد من نسخ البرامج ولا يسمح بأكثر من نسخة واحدة (المادة 54)، كما أنه ينبغي تدمير كل نسخة مستنسخة من برنامج عند انقضاء مشروعية حيازتها.وفقا للمادة 46 من الأمر 03/05[2] يحق لأي مكتبة أو مركز لحفظ الأرشيف نسخ عمل منشور، سواء كان على شكل مقال أو أي نوع آخر من المصنفات، باستثناء البرمجيات وذلك بشرط أن يتم النسخ بناءا على طلب شخص طبيعي، وتتوفر فيه الشروط التالية:

- ❖ أن تستخدم النسخة لأغراض دراسية، بحث جامعي، أو الإطلاع الشخصي فقط، دون أي استخدام آخر.
- ❖ أن تكون عملية الاستنساخ فعلا معزولا لا يتكرر وقوعه إلا في المناسبات متميزة لا علاقة لها فيما بينها.
- ❖ ألا يكون الديوان الوطني لحقوق المؤلف قد منح ترخيصا جماعيا يسمح بإيجاز مثل تلك النسخ.

[1] – نصت المادة 53 من الامر 05/03 على أنه:" ينبغي أن تقتصر الاستعمالات عل استنساخ نسخة واحدة من برنامج الحاسوب أو اقتباسه على الأوجه المنصوص عليها في المادة 52، يجب تدمير كل نسخة مستنسخة من برنامج الحاسوب أو مقتبسة منه عند اقتضاء مشروعية الحيازة".

[2] – فتيحة عمارة، الحماية الجنائية للمعلومات الإلكترونية في إطار قانون الملكية الفكرية، العدد 31، مجلة الحياة، الجزائر، 2014، ص 32.

كما ينص الامر 03/05 في مادته 150 على أنه أي شخص يقوم بإتاحة مصنف للجمهور دون إذن من المؤلف يعد مركبا لاعتداء على حقوق المؤلف، ويشمل ذلك جميع أشكال العرض للجمهور سواء عبر الصوت أو الصورة أو كليهما، أو بأي وسيلة كانت، بما في ذلك الإشارات أو الصور أو الأصوات الرقمية، أو ضمن أنظمة معالجة المعلومات، هذا انوع من الأفعال يعتبر انتهاكا لحقوق المؤلف ، بغض النظر عن نية الفاعل، ولا يشترط أن يكون الاعتداء ماديا فقط، بل يكفي توفر أحد أركانه، مثل غياب إذن المؤلف أو من ينوب عنه قانونا، وإذا كان المصنف ناتجا عن عمل جماعي أو مشترك، فإن الحصول على الإذن يتطلب موافقة جميع الشركاء أو ترخيص جماعي من الشخص المعنوي الذي يمثلهم[1].

**2. الركن المعنوي:**

القصد الجنائي في جريمة التقليد مفترض، فتوافر إحدى صور النشاط الإجرامي السابقة يعد قرينة على توافر القصد الجنائي، وهذا يعني أن حسن النية لا يفترض، وعلى الجاني إثباته، وللقول بتوافر حسن النية من عدمه من اختصاص محكمة الموضوع.

**ثالثا: الجنح المشبهة بالتقليد:**

**1. الركن المادي:**

صور التعامل المجرمة في البرامج المقلدة سواء قلدت داخل أرض الوطن أو خارجها:

- ❖ استيراد وتصدير نسخ مقلدة.
- ❖ بيع وتأجير نسخ مقلدة.
- ❖ عرض نسخ مقلدة للتداول.
- ❖ المساعدة والمشاركة في المساس بحق المؤلف والرفض العمدي لدفع المكافأة المستحقة.

[1] – أمال قارة، المرجع السابق، ص 87.

### 2. الركن المعنوي:

القصد الجنائي مفترض، أما بالنسبة للاستيراد والتصدير فإلى جانب القصد الجنائي العام يجب توافر قصد الاستغلال التجاري، وعلى الجاني إثبات حسن نيته، أما بالنسبة للحالتين الأخيرتين ضرورة توافر القصد الجنائي.

### الفرع الثالث: الإجراءات الخاصة بجرائم التقليد:

يولي المشرع الجزائري أهمية كبيرة لحماية حقوق الابتكار والإبداع، سواء في مرحلة الإنتاج الأول أو عند التوزيع[1]، وقد جاءت القوانين الوطنية لتواكب هذا التوجه من خلال سن نصوص قانونية واضحة تهدف إلى التصدي لظاهرة التقليد التي تمس الحقوق الفكرية، خاصة تلك المتعلقة بالمصنفات الادبية والفنية، سواء كانت أصلية أم مترجمة. ومن بين الوسائل التي وفرها القانون للتصدي لجرائم التقليد، ما نصت عليه المادة 160 من الأمر 05/03 والتي تمنح لمالك الحقوق المعنوية والمادية للمصنف حق تقديم شكوى إلى الجهات القضائية المختصة، ضد كل من يعتدي على حقوقه الفكري، شريطة أن يكون الفعل محل الشكوى منصوصا عليه ومعاقبا بموجب أحكام هذا الأمر [2].

وتجدر الإشارة إلى أن المشرع الجزائري لم يكتفي بالطرق التقليدية في إثبات واقعة التقليد، بل أتاح لمالك المصنف الأصلي وسيلة إجرائية هامة تتمثل في ما يعرف بالحجز على التقليد، وهي إجراء يستخدم كوسيلة لإثبات أن هناك تعديا على المصنف، وينفذ غالبا بموافقة الجهة القضائية المختصة قبل اللجوء إلى رفع الدعوى القضائية.

[1] – فتيحة عمارة، المرجع السابق، ص 242.

[2] – أمال قارة، المرجع السابق، ص88.

**أولا: الإجراء الحجز على التقليد:**

هذا الإجراء يمكن صاحب الحق من حجز نسخ المصنفات المقلدة أو الوثائق والمعدات التي استخدمت في عملية التقليد، وذلك بناءا على إذن قضائي مسبق كخطة استباقية لحماية المصنف من التداول غير المشروع، وقد حدد الامر 05/03 الجهات المخولة قانونا للقيام بهذا الإجراء وهي:[1]

- ❖ أعوان الضبط القضائي: أي أعوان الشرطة القضائية الذين يتمتعون بالصلاحيات القانونية للقيام بمهام الضبط والمتابعة في مثل هذه القضايا.
- ❖ الأعوان المؤهلون التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة: وهم موظفون مختصون، يخول لهم القانون بموجب المادة 146 من الامر 05/03 القيام بعمليات الحجز على النسخ المقلدة، سواء تعلق الأمر بالمصنفات الادبية أو التسجيلات الصوتية أو المرئية أو أي دعامة من دعامات التعبير الفني.

**ثانيا: الجزاءات المقررة لجرائم التقليد:**

نصت المادة 05/03[2]على مجموعة من العقوبات التي تهدف إلى الردع والحماية القانونية لحقوق المؤلف، ومن بين هذه العقوبات:

الحبس من 06 أشهر إلى 03 سنوات وغرامة مالية تتراوح بين 500.000 دج إلى 1.000.000 دج في حال كانت عملية لنشر أو التقليد دولية، فإن العقوبة تشمل كذلك مصادرة النسخ والإيرادات الناتجة عن الاستغلال الغير مشروع.

ويحق للقاضي أن يأمر بإتلاف النسخ المقلدة ومصادرة جميع الوسائط التي تم استخدامها في عملية التقليد، كما له صلاحية غلق المؤسسة المتورطة اذا ثبت تورطها المتكرر في نفس العمل.

---

[1] – .توفيق مجاهد، طاهر عباسة ، جريمة الإرهاب الإلكتروني على ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، المجلد 09، العدد 3، مجلة العلوم القانونية والسياسية، ديسمبر 2018، ص ص76، 100.

[2] – نصت المادة 153 من الأمر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة على ما يلي:" يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادة 151 و 152 أعلاه بالحبس من ستة( 06) أشهر إلى ثلاث (03) سنوات، وبغرامة مالية من خمسمائة ألف دينار 5.000.000دج إلى مليون دينار 1.000.000 دج سواء كان النشر قد حصل في الجزائر، أو في الخارج ، للمزيد انظر المادة 153 من الامر 05/03.

**ثالثا: الجزاءات القانونية المقررة:**

تضمنت الأحكام التشريعية المتعلقة بالاعتداءات على حقوق الملكية الادبية والفنية جملة من المواد القانونية الواردة في الأمر 05/03، وتحديدا المواد من 153 إلى 159، بالإضافة إلى المواد 390 إلى 394 من قانون العقوبات، غير ان احكام هذه المواد ألغيت بمقتضى المادة 165 الأمر 10/97 المعدل والمتمم بالأمر 05/03 ويتضح من خلال هذه النصوص أن المشرع الجزائري شدد في العقوبات المتصلة بالاعتداء على حقوق المؤلف وذلك على النحو التالي:

يعاقب الجاني بعقوبة سالبة للحرية تتراوح ما بين ستة (06) أشهر إلى ثلاث(03) سنوات حبسا، بالإضافة إلى غرامة مالية تتراوح بين 500.000 دج إلى 1.000.000 دج[1]، سواء ارتكبت الجريمة داخل الجزائر أو خارجها، طالما أن أثارها تمتد إلى الإقليم الوطني

يمنح القاضي سلطة فرض عقوبات تكميلية، من أبرزها مصادرة المبالغ المالية الناتجة عن الاستغلال غير المشروع للمصنف، سواء عبر الإيرادات أو أرباح التوزيع، وكذا مصادرة النسخ والوسائط التي استعملت في الجريمة، وكل ما تم استعماله أو إنتاجه خصيصا للقيام بالنشاط غير المشروع.

يمكن للقاضي، بناءا على طلب المتضرر الحكم بمصادرة قيمة الأرباح الناتجة عن النشر غير المشروع لصالح الطرف المدني في حال عدم إمكانية تحديدها بدقة.

كما يحق له الحكم بغلق المؤسسة أو الشركة التي استخدم اسمها أو كيانها لتسهيل ارتكاب الجريمة، إذا ثبت أنها كانت أداة لتحقيق الجريمة وقد منح الامر 05/03 للقضاء سلطة واسعة لتقرير هذه العقوبات، سواء الأصلية أو التكميلية، بما يتماشى مع حماية المصنفات الفكرية وحماية حقوق المؤلفين من الاستغلال غير المشروع.

رغم هذه الإجراءات، يسجل على النصوص القانونية الجزائرية أنها لا تولي اهتماما كافيا لبعض أنواع المصنفات الحديثة، مثل تطبيقات الإعلام الآلي، والتي لم يذكرها القانون 97/10[2]أو الأمر 05/03 صراحة، وهو ما يثير إشكاليات ي التطبيق.

[1] – الأمر 05/03، المصدر السابق.

[2] – القانون رقم 97-10، المؤرخ في 06 مارس 1997، المتعلق بالأرشيف، ج.ر.ج.ج، العدد 15، الصادرة بتاريخ 1 مارس 1997.

**المطلب الثاني: الجرائم المعلوماتية في إطار معالجة المعطيات الشخصية:**

تشير المعطيات الشخصية إلى كل المعلومات التي تخص فردا معينا، سواء تعلق بالأمر باسمه الكامل، أو مكان إقامته، أو وظيفته، أو جنسيته، أو حالته الاجتماعية أو الصحية، أو غيرها من التفاصيل لت ترتبط بحياته الخاصة وتميزه عن غيره من الأشخاص، ونظرا لكون هذه البيانات تتعلق بالحياة الخاصة للفرد، فهي بطبيعتها تحمل طابعا سريا وشخصيا، مما يستدعي احترام خصوصيتها وبالتالي لا يجوز لأي شخص غير المعني بالأمر أن يطلع على هذه المعطيات او يتصرف بها داخل أي منظومة معلوماتية دون موافقة صريحة من صاحبها، فالمعلومات الشخصية تعد ملكا لصاحبها، ويحظر التعدي عليها أو استعمالها دون إذن قانوني أو تفويض مسبق، ومن خلال هذا سوف نتطرق إلى مفهوم المعطيات الشخصية (الفرع الأول) وإلى مفهوم موضوع المعالجة(الفرع الثاني).

**الفرع الاول: مفهوم المعطيات الشخصية:**

عرف المشرع الجزائري البيانات أو المعطيات ذات طابع شخصي في المادة 03 فقرة أولى من قانون 07/18[1] التي تنص على: "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعريف بصفة مباشرة أو غير مباشرة لاسيما بالرجوع غلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

فالتعريف محسوم بنص قانوني في جل التشريعات المتعلقة بحماية المعطيات إذ لا يخلو أي قانون لحماية المعطيات الشخصية من تعريف لهذا المفهوم وقد يكون السبب وراء هذا التوجه الطابع الفني لمصطلح المعطيات ذات طابع الشخصي ما يجعل هذا التعريف وظيفي يرتبط بمقتضيات وأهداف القانون.

**أولا: أنواع المعطيات الشخصية:**

**1. المعطيات الشخصية الحساسة:**

[1] – قانون 18-07 المؤرخ في 10 يوليو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد، 34، الصادرة في 10 يوليو 2018.

عرفها المشرع الجزائري في المادة 03 فقرة 1 و 6 المعطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية[1].

ونلاحظ من خلال هذا التعريف أن المعطيات الحساسة تمثل البيانات الشخصية الخاصة بالأفراد، لذلك أولى لها المشرع الجزائري عناية منفردة من خلال النصوص العقابية لكل من قام بمعالجتها بخلاف احكام القانون[2].

**2. المعطيات الشخصية غير الحساسة:**

عرف المشرع الجزائري من خلال المادة 03 في الفقرة 01 المعطيات غير الحساسة كل معلومات التي تمكننا من تحديد الشخص والتعرف عليه بالرجوع إلى مظاهر شخصية والمتعلقة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية والاقتصادية أو ثقافية أو الاجتماعية[3].

**ثانيا: حقوق الشخص المعني:**

أوجب المشرع في المواد 34 و 36 على المسؤول عن المعالجة تمكين الشخص المعني من ممارسة مجموعة من الحقوق فيما يخص معطياته الشخصية على الشكل التالي:

**1. حق الولوج:**

منح القانون 18-07 للشخص المعني هذا الحق وذلك من خلال التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، وأغراض المعالجة وفئات المعطيات التي تنصب عليها

[1] – المادة 03 فقرة 6/1 من القانون 07/18، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجته المعطيات ذات الطابع لشخصي، مصدر سابق.

[2] – فاطيمة الزهرة عواد، الحماية الجزائية للبيانات الشخصية المعالجة آليا، مذكرة لنيل شهادة الماستر، قسم الحقوق، ،كلية الحقوق والعلوم السياسية، جامعة سعيدة، 2020/2019، ص 13.

[3] – المادة 3 فقرة 1 من القانون 07/18، مصدر سابق.

والمرسل إليهم، وإفادته وفق شكل مفهوم المعطيات الخاصة به التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات.

**2. الحق في الإعلام:**

تنص المادة 32 من القانون 07/18 على منح الشخص المعني حقا في الإعلام في حال لم يكن على علم مسبق بجمع بياناته ويتعين على المسؤول عن معالجة البيانات أو من ينوب عنه، أن يزود الشخص المعني بمعلومات واضحة وصريحة، على أن تكون موجهة إليه شخصيا، وليس لأي طرف آخر، ويجب أن يتم ذلك في إطار جمع بيانات ذات طابع شخصي.

ويتضمن هذا الحق عددا من العناصر الأساسية التي يجب إعلام الشخص بها وهي:

- ❖ هوية الجهة المسؤولة عن المعالجة أو هوية من يمثلها.
- ❖ الغرض أو الأغراض التي تتم من اجلها معالجة البيانات.

**3. الحق في التصحيح:**

كما منع القانون للشخص المعني هذا الحق بصفو مجانية من قبل المسؤول عن المعالجة سواء تعلق الأمر:

- ❖ تحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة للقانون.
- ❖ وكلك لو تعلق الأمر تبليغ الغير الذي أوصلت إليه لمعطيات الشخصية بكل أو مسح أو إغلاق للمعطيات ذات الطابع الشخصي[1].

**4. الحق في الاعتراض:**

نصت عليه المادة 36 من القانون، والتي تتيح للفرد الاعتراض على معالجة بياناته سواء تم جمعها من طرف الغير أم تم الحصول عليها مباشرة منه، ويمنح هذا الحق يشكل شخصي لا يمكن التنازل عنه أو ممارسته من قبل الغير بالنيابة إلا في حالات استثنائية يحددها القانون، كما أن هذا الاعتراض لا

[1] – علي إبراهيم بن دراج، مرجع سابق، ص 72، 73.

يشترط أن يكون مبينا على أسباب خاصة أو محددة، بل يكفي أن يرى الشخص أن في المعالجة مساسا بحقه في الخصوصية أو تعارضا مع مصلحته المشروعة[1].

ويعد هذا الحق من الضمانات الأساسية لحماية الحياة الخاصة، ويعتبر وسيلة قانونية تحول للفرد الدفاع عن بياناته الشخصية، غير أن هذا الحق ليس مطلقا إذ لا يجوز الاعتراض على المعالجة إذا كانت المعطيات تجمع لأغراض إعلامية وفقا للمادة 32 من نفس القانون، ويشترط في هذه الحالة أن يكون المسؤول عن المعالجة قد اخطر الشخص المعني بالحصول على البيانات مسبقا إذا كانت متاحة ومتوفرة[2].

**الفرع الثاني: تعريف المعالجة:**

يعرف المشرع الجزائري معالجة المعطيات الشخصية بأنها كل عملية أو مجموعة من العمليات التي تجرى عل بيانات ذات طابع شخصي، سواء عبر وسائل آلية أو يدوية، ومهما كانت الطريقة أو الوسيلة. وتشمل هذه العمليات مثلا جمع البيانات، تسجيلها، تنظيمها، حفظها، تعديلها، استخراجها، الإطلاع عليها، استعمالها، إرسالها أو نشرها بأية طريقة كانت، إضافة إلى ربطها أو دمجها أو حجبها أو محوه، كما تمتد هذه المعالجة لتشمل الإغلاق، المسح أو الإعلان، بل وكل نشاط يقوم به شخص طبيعي تجاه بيانات يمكن أن تحدث تغييرا في طبيعتها أو هويتها.

**أولا: أنواع المعالجة:**

يشترط في معالجة لمعطيات الشخصية نوعين يدوية وآلية كما يلي:

**أ. المعالجة اليدوية:**

تعني المعالجة اليدوية تلك الإجراءات التي تتم لتنظيم البيانات الشخصية وتخزينها ضمن ملفات ورقية أو سجلات تقليدية، دون الاعتماد على الوسائل التقنية الحديثة أو الطرق المؤتمنة، وغالبا ما تتم

[1] – خديجة بن موسى، الحماية الجنائية للمعطيات في المجال المعلوماتي، مذكرة لنيل شهادة الماستر أكاديمي حقوق، قانون جنائي، حقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 1442 هـ/1444 هـ، 2022/2021، ص 20.

[2] – عز الدين طباش، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الاكاديمية للبحث القانوني، العدد 2، 2018، ص37.

هذه العمليات بشكل يدوي بحت، حيث لا يستخدم أي جهاز إلكتروني أو برمجي لتنفيذها وقد عرفها المشرع الجزائري في المادة 03 فقرة 03 بأنها كل عملية أو مجموعة عمليات منجزة بطريقة يدوية.[1]

وتكمن أهمية هذا لنوع من المعالجة في أنه لا يتطلب بالضرورة تدخل أنظمة إلكترونية، لكنه يعد معالجة فعلية متى ما أنجزت البيانات بشكل منظم ومنهجي، حتى وإن لم تعالج عبر وسائل آلية.

**ب. المعالجة الآلية:**

بالرجوع إلى نص المادة 03 فقرة 05 من القانون 18-07[2] نجد أنها حددت المقصود بالمعالجة الآلية للبيانات بأن هذه الأخيرة تشمل كل عملية أو مجموعة من العمليات التي تتم بطريقة مؤتمتة، والتي تتعلق بجمع أو تسجيل البيانات أو تنظيمها أو تعديلها أو حفظها أو استرجاعها أو حتى ربها ونقلها أو حجبها أو إتلافه، شريطة أن تكون هذه المعطيات ذات طابع شخصي، وبالتالي يقصد بها كل أسلوب تقني يستعمل للحصول على معلومات شخصية أو التعامل معها بصورة مؤتمتة.

**ثانيا: شروط المعالجة**

ذكرها المشرع الجزائري في المواد 7 و 8 من القانون 18-07[3]شروط معالجة المعطيات الشخصية والمتمثلة في موافقة الشخص المعني وإجرائي التصريح والترخيص.

**1. موافقة الشخص المعني:**

تنص المادة 07 من القانون 18-07 على إلزامية ووجوب الحصول على الموافقة الواضحة والصريحة للشخص المعني كشرط أساسي لمعالجة معطياته الشخصية، وإن كان فاقد أو ناقص للأهلية فهذا لا يمنعه من إغفال هذا الشرط بل يستوجب الامر مراعاة القواعد القانونية العامة، فالموافقة يجب

[1] – المادة 03 فقرة 05 من القانون 18-07، مصدر سابق.

[2] – المادة 03 فقرة 05 من القانون 18-07، المصدر نفسه.

[3] – المادة 07 و 08 من القانون 18-07، المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، مصدر سابق.

أن تعطى بشكل حر ومسبق دون أي إكراه أو ضغط، كما يجب أن تكون محددة بزمن معين ولا يمكن أن تكون مشروطة.

وتعد الموافقة تعبيرا عن إرادة الشخص المعني سواء تم التعبير عنها كتابة أو بأي وسيلة أخرى، شرط أن تظهر بشكل لا لبس فيه موافقة الشخص المعني عن معالجة بياناته الشخصية، ولتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة مع مراعاة مصلحة المعني وحقوقه وحرياته، فنجد أن المشرع للحفاظ على حقوقه وحرية الشخص أورد هذه الحالات على سبيل الحصر لا على سبيل المثال لتصبح أي حالة خارج ما ذكرته هذه المادة هو انتهاك وتعدي على المعطيات الشخصية التي أصبحت محمية بموجب هذا القانون.[1]

### 2. إجراء التصريح:

ذكره المشرع الجزائري في المواد من 13 إلى المادة 16 من القانون 18-07، ويقصد به تقديم طلب يتضمن إخطار السلطة الوطنية الالتزام بإنجاز عملية المعالجة للمعطيات الشخصية في إطار أحكام قانون 18-07 إذ يسلم المسؤول عن المعالجة بموجب هذا التصريح وصل إيداع غما مباشرة أو يرسل إليه بالبريد الإلكتروني فورا أو في أجل لا يتعدى 48 ساعة[2].

وقد ميز القانون نوعين من التصريح:

#### أ. التصريح العادي:

الذي يجب أن تتوفر فيه كل البيانات التي تم ذكرها في المادة 14، وهي 09 بيانات تتضمن اسم وعنوان المسؤول عن المعالجة أو ممثلة، طبيعة المعالجة والغرض منها، وصف فئة أو فئات الأشخاص المعنيين والمعطيات أو فئات المعطيات ذات الطابع الشخصي المتعلقة بهم، المرسل أو فئات المرسلين

[1] – المادة 7 من القانون 18-07، المصدر السابق.

[2] – محمد العيداني ويوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07، مجلة معالم الدراسات القانونية والسياسية، العدد 05، ص 122.

الذين يمكن أن تفصح لهم المعطيات، المدة الزمنية المقدرة لحفظ المعطيات، الوسائل التي تضمن لمن المعطيات ما إذا كانت المعطيات ستنقل إلى دولة أجنبية، وصف عام للعمليات التي ستجرى على المعطيات.

هذه المعلومات ضرورية لضمان الشفافية وحماية حقوق الأفراد في ما يتعلق بمعالجة بياناتهم الشخصية.

**ب. التصريح البسيط:**

وهو ما نصت عليه المادة 15 الحالات التي لا تشكل خطر يهدد حقوق وحريات الأفراد، خاصة إذا لم تتضمن المعالجة بيانات حساسة، كما هو منصوص عليه في المادة 14 من نفس القانون. وعليه لا يتطلب هذا النوع من التصريح الشروط المقررة والمذكورة في التصريح العادي.

كما أوجبت المادة 14 من نفس القانون في فقرتها الأخيرة وبشكل صريح في حالة التنازل عن ملف المعطيات أن يتم المتنازل له إجراءات التصريح، في حين أوجبت فقط إخطار السلطة الونية في حالة تغيير المعلومات المذكورة في المادة 04 أو أي حذف يطال المعالجة.[1]

**3. إجراء الترخيص:**

إن الترخيص هو إجراء مباشر بعد إجراء التصريح وهو قرار صادر عن السلطة الوطنية والتي تعمل على دراسة التصريح للتحقق من خلو المعالجة من أي تهديدات تمس كرامة الأفراد أو حياتهم الخاصة أو الحريات الأساسية، وهذا ما نصت عليه المادة 17 الفقرة 01 القانون، كما يلزم القانون السلطة بالرد على طلبات التصريح خلال مدة لا تتجاوز (10) أيام من تاريخ إيداع الطلب وفقا لما ورد في المادة 17 الفقرة 02 والمادة 18 فقرة 07 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، كما تجدر الإشارة إلى أن المشرع الجزائري أكد في نص المادة 18 فقرة 1 و 2 من نفس القانون على حماية المعطيات الحساسة ومنع معالجتها غلا للضرورة.

[1] – عز الدين طباش، مرجع سابق، ص ص 38- 40.

هذا وأشارت المادة 44 من قانون حماية المعطيات الشخصية إلى لزوم الرخيص في حالة نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية، ويمنح هذا الترخيص بناءا على تقدير السلطة الوطنية المختصة التي تقوم بتقييم مدى توفر مستويات كافية من الأمن والحماية في تلك الدولة، وكذلك فإن السلطة الوطنية أن تمنح الترخيص بنقل المعطيات إلى دولة أجنبية استثناءا إذا كانت المعالجة تتطابق مع أحكام القانون[1].

**ثالثا: التزامات المسؤول أثناء المعالجة:**

هذه الالتزامات نص عليها المشرع الجزائري في المواد 38 إلى 45 على النحو التالي:

**أ. سرية وسلامة المعالجة:**

أوجب المشرع الجزائري على المسؤول عن المعالجة في المادة 38 ضرورة حماية المعطيات الشخصية من خلال وضع مجموعة من التدابير التقنية والتنظيمية تفاديا لأي ضرر قد يصيبها خاصة عندما تستوجب هذه المعالجة إرسال معطيات عبر شبكة معينة[2].

وتنقسم هذه التدابير إلى نوعين[3]:

❖ **التدابير التنظيمية:**

تعنى بتنظيم آليات الوصول إلى المعطيات، ومراقبة من يسمح لهم بذلك، مع اتخاذ التدابير اللازمة لحماية المعطيات من أي خرق أو استخدام غير مشروع، كما تشمل إعداد خطط لتأمين المعطيات ضد أي خطر محتمل.

[1] – أمينة ميساد، آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون(18-07)، مجلة الباحث في العلوم القانونية والسياسية، العدد 05، جامعة محمد الشريف مساعدية، سوق أهراس، 2021، ص 10.

[2] – المادة 43 من القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مصدر سابق.

[3] – صبرينة جدي، الإطار القانوني لمعالجة المعطيات ذات الطابع الشخصي في التشريع الجزائري على ضوء قانون رقم 18-07، المجلة الشاملة للحقوق، مجلد 2، عدد 3، جامعة باجي مختار عنابة- الجزائر، سبتمبر 2022، ص 13.

❖ **التدابير التقنية:** ترتكز على اعتماد وسائل تكنولوجية مثل برامج مكافحة الفيروسات، ونظم كشق التسلل، وغيرها من الحلول التقنية الكفيلة بضمان أمن وسلامة المعلومات.

**ب. التزام المسؤول عن المعالجة فيما يخص المعالجة المرتبطة بخدمات التصديق الكتروني والمتعلقة بمجال الاتصالات الإلكترونية:**

نصت على هذا الالتزام المادتين 42 و 43[1]، حيث ألزمت المادة 42 على المسؤول عن المعالجة بعدم استعمال المعلومات التي يتم جمعها لأي غرض خارج إطار تسليم وحفظ الشهادات الإلكترونية الخاصة بالتوقيع الرقمي، وذلك تجنبا لأي استخدام مخالف لهذا الغرض.

كما أن المادة 43 شددت على ضرورة إخطار كل من السلطة الوطنية المختصة والشخص المعني، في حال حصول أي خرق أو مساس ببياناته الشخصية أثناء معالجتها ضمن شبكات الاتصالات الإلكترونية المفتوحة للعامة.

**ج. الالتزام الخاص بنقل المعطيات نحو الخارج:**

نصت عليه المادة 44، حيث جاء في مضمون هذه المادة أنه لا يجوز للمسؤول عن المعالجة القيام بنقل المعطيات الشخصية نحو دولة اجنبية إلا بعد الحصول على ترخيص من السلطة الوطنية بعدما تقدر المستوى الكافي التي تتضمنه هذه الدولة من حماية لحقوق وحريات الأفراد، غير أنه يمكن أن تتم عملية النقل إلى دولة أجنبية لا يتوفر فيها هذا الشرط وفق ما أوردته المادة 45 من القانون 18-07 [2].

**المطلب الثالث: الجرائم المعلوماتية المتصلة بتكنولوجيات الإعلام والاتصال:**

لم يولى المشرع الجزائري قبل عام 2004 اهتماما كافيا بالجرائم المعلوماتية، حيث لم يتطرق المشرع صراحة لهذا النوع من الجرائم، لكن مع صدور القانون رقم 15-04[3] الذي عدل قانون العقوبات،

[1] – المادتين 42 و 43 من القانون 18-07، مصدر سابق.

[2] – المادتين 44 و 45 من القانون 18-07، المصدر نفسه.

[3] – قانون رقم 04-15، مصدر سابق.

ثم إدراج أحكام خاصة في القسم السابق مكرر تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات. كما جاء القانون 09-04 ليحدد القواعد العامة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها.

بناءا على ذلك سوف نترق إلى أسباب إصدار قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (الفرع الأول، ثم نتحدث عن أبرز ما عالجه قانون 09-04 (الفرع الثاني).

**الفرع الأول: أسباب إصدار قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:**

لقد جاء القانون رقم 15- 04 لملء الفراغ القانوني الذي عرفه التشريع الجزائري في مجال مكافحة الجرائم المعلوماتية، وقد أدرك المشرع الجزائري هذا الفراغ، مما دفعه إلى استصدار نصوص وتشريعات قانونية لسد هذا الخلل القانوني.

وفي هذا السياق صدر القانون 15- 04 متضمنا أحكام تنظم آلية المعالجة الآلية للمعطيات، ثم تتبعه صدور قانون آخر هو القانون 06- 23[1] والذي اهتم بتجريم أفعال الاعتداء على أنظمة المعالجة الآلية للمعطيات، غير أن القانون 09- 04[2] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جاء ليعزز نفس هذه القواعد من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما ألزم المشرع مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات والمراسلات ووضعها تحت تصرفها، مع مراعاة سرية هذه المعاملات، والالتزام بحفظ المعطيات التي تساعد في الكشف عن الجرائم ومرتكبيها، وكذلك التدخل

[1] – قانون رقم 06-23 مؤرخ في 20 ديسمبر 2006، يتعلق بتنظيم أنظمة المعالجة الآلية للمعطيات ذات الطابع الشخصي، ج.ر.ج.ج، العدد 7، صادرة بتاريخ 20 ديسمبر 2006.

[2] – قانون رقم 09-04 مؤرخ في 5 أغسطس 2009، يتضمن قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، ج.ر.ج.ج، ع 47، الصادرة بتاريخ 16 أغسطس 2009.

الفوري لسحب المحتويات التي يطلعون عليها بمجرد العلم بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.[1]

## الفرع الثاني:الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل القانون رقم 09-04

عرفت المادة الثانية من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جرائم انتهاك الحياة الخاصة في البيئة الرقمية بأنها كما يلي: " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أن يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[2].

ولقد حصر المشرع في المادة الرابعة من نفس القانون أربع حالات سمح فيها للسلطات باللجوء إلى مراقبة الاتصالات الإلكترونية تتمثل في ما يلي:

- الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- عند توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- مقتضيات التحري والتحقيقات القضائية عندما يصعب الوصول إلى نتيجة تهم. يعتبر فعلا من أفعال التقليد، مما يستدعي فرض عقوبات قانونية.

ينص الأمر 05/03 في القانون الجزائري على أن تقليد المصنفات أو ارتكاب جرائم مشابهة لها يعد مخالفة يعاقب عليها، ويتم اعتبار المصنف مقلدا في الحالات التالية:

- تقليد المصنف أو الأداء الفني بطريقة تحاكي الاصل.
- نسخ أو تصوير المصنف أو تكراره.
- بيع نسخ مقلدة أو مزورة من المصنف أو أدائه.

[1] – سناء شيخ ومحمد زكرياء، مكافحة الجرائم الإلكترونية في القانون الجزائري، مجلة وميض الفكر للبحوث، العدد 05، سبتمبر 2020، ص7-8.

[2] – المادة 02 من القانون رقم 09-04، مصدر سابق.

- تأجير المصنف المقلد أو توزيعه.

**خلاصة الفصل الأول:**

شهد العالم في العقود الأخيرة ثورة رقمية غيرت من طبيعة المعاملات اليومية، وفتحت المجال أمام ظهور جرائم مستحدثة تُرتكب في بيئة افتراضية تتسم بالسرعة والتعقيد. وفي هذا السياق، أدرك المشرع الجزائري ضرورة مواكبة هذا التطور بوضع إطار قانوني ينظم ويجرّم الأفعال الإجرامية المرتكبة بواسطة تكنولوجيا المعلومات، وهو ما يُعرف اصطلاحًا بـ" الجريمة المعلوماتية ".

وقد تجلى هذا الوعي القانوني بشكل واضح من خلال إدراج أحكام جديدة ضمن قانون العقوبات بموجب القانون 04 -15 المؤرخ في 5 أوت 2009، حيث تم تخصيص قسم خاص بالجريمة المعلوماتية تحت عنوان " الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ". تناول هذا القسم مجموعة من الجرائم المستحدثة مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، والاعتراض غير المشروع للمعطيات، وتزوير البيانات الإلكترونية، واستعمالها بدون وجه حق، إلى جانب المساس بسلامة وسير النظام المعلوماتي.

ويعكس هذا التوجه التشريعي إدراكًا من السلطات الجزائرية لخطورة هذه الجرائم، التي لا تقتصر آثارها على الأفراد فقط، بل تمتد إلى المؤسسات الاقتصادية، بل وحتى الأمن الوطني. لذلك، حاول المشرع أن يقدم تعريفات قانونية دقيقة لبعض المصطلحات التقنية لضمان فعالية تطبيق النصوص على أرض الواقع، مع الحرص على إضفاء الطابع الزجري للعقوبات بغرض الردع العام والخاص.

غير أن التأطير القانوني، على الرغم من أهميته، لا يزال يطرح عدة إشكالات من حيث التطبيق العملي، خاصة أمام التطور السريع للجرائم الإلكترونية وتعدد أشكالها، ما يفرض على المشرع تبني رؤية مرنة ومتجددة، وربط التشريع الوطني بالجهود الدولية في هذا المجال، عبر الانخراط في الاتفاقيات متعددة الأطراف ذات الصلة.

في المجمل، يُمكن القول إن المشرع الجزائري خطا خطوة مهمة نحو تأطير الجريمة المعلوماتية، إلا أن هذا التأطير لا يزال بحاجة إلى تدعيم مستمر، سواء على مستوى الصياغة القانونية، أو من خلال توفير الآليات المؤسسية والتقنية التي تواكب طبيعة هذه الجرائم العابرة للحدود.

# الفصل الثاني: أساليب وآليات التحري عن الجريمة المعلوماتية

تعد الجريمة المعلوماتية من الجرائم المعقدة التي تتطلب معرفة تقنية متقدمة، حيث غالبا ما يرتكبها أشخاص يمتلكون مهارات عالية في مجال البرمجيات، وفهم دقيق لآليات تشغيل الحاسوب والأنظمة الرقمية. هذه الطبيعة الخاصة للجريمة تجعل من الصعب على الجاني ترك أي أثر يدل على هويته، مما يعيق عملية اكتشافها أو الوصول إلى مرتكبيها بسهولة، ومع تصاعد هذا النوع من الجرائم أصبحت الحاجة ملحة لتطوير ادوات وتقنيات التحقيق، وتمكين الجهات المختصة من الإلمام الكافي بالجوانب التقنية المرتبطة بها حتى يتسنى لها رصد الجريمة المعلوماتية وجمع أدلة رقمية قابلة للاستغلال قضائيا.

ومن هنا، يأتي هذا الفصل لتسليط الضوء على آليات وإجراءات التحري في ميدان الجرائم المعلوماتية أي التطرق إلى الوحدات المختصة في البحث عن الجريمة المعلوماتية (**المبحث الأول**) والإجراءات القانونية التحري للكشف عن الجريمة المعلوماتية (**المبحث الثاني**).

## المبحث الأول: الوحدات المختصة في البحث عن الجرائم المعلوماتية

سنحاول من خلال هذا المبحث استعراض أبرز الهيئات والوحدات المختصة في مجال مكافحة الجرائم المعلوماتية وذلك بالنظر لطبيعة هذه الجرائم التي تتطلب خبرات دقيقة ومهارات تقنية عالية في مجال التكنولوجيات الرقمية، حيث تضم فرقا من المحققين ذوي تخصصات دقيقة يعملون على تتبع مسارات الجريمة الإلكترونية، ولعل أن أبرز هذه الهيئات والوحدات هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (**المطلب الأول**)، إضافة إلى تلك الأجهزة الأمنية (**المطلب الثاني**) سواء التابعة لسلك الأمن الوطني أو التابعة لقيادة الدرك الوطني.

## المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

ترجع فكرة تأسيس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام إلى سنة 2005، وتحديدا بتاريخ 05 أوت 2005، وهو نفس التاريخ الذي صدر فيه القانون رقم 09-04[1] الذي خصص جزء منه لوضع قواعد تهدف إلى التصدي لمثل هذه الجرائم، وقد جاء في نص المادة 13 من نفس القانون على أنه تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. كما تكلف هذه الهيئة بوضع التنظيمات اللازمة لضبط مهامها، وتحديد هيكلها الإداري، وكيفية تسييرها.

وقد بقي هذا النص القانوني معلقا إلى أن صدر المرسوم الرئاسي رقم 15-261[2] والذي تم نشره في العدد 53 من الجريدة الرسمية، وقد جاء هذا المرسوم ليفصل في تعريف الهيئة واختصاصها (الفرع الأول) ومهامها التي سوف نتحدث عنها (الفرع الثاني) وكيفية تشكيلها في (الفرع الثالث).

### الفرع الأول: التعريف بالهيئة واختصاصها

[1] – قانون رقم 09- 04 مؤرخ في 5 أوت 2005، مصدر سابق.

[2] – المرسوم الرئاسي 15-261 المؤرخ في 2015/10/08 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 53، المؤرخة في 24 ذي الحجة 1436 هـ، الموافق لـ 08 اكتوبر 2015.

خصص هذا الفرع للتعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام، و كذا عرض خصائصها، و هذا ما سيتم تفصيله من خلال ما يلي:

**أولا: التعريف بالهيئة:**

تدعي "الهيئة"[1] كما يصطلح عليها في صلب نصوص المرسوم الرئاسي رقم 15-261 حسب أحكام المواد من 01 إلى 04 منه بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة، تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون 09-04 وذلك تحت رقابة السلطة القضائية وطبقا لأحكام قانون الإجراءات الجزائية.

**ثانيا: اختصاص الهيئة:**

وضحت الفقرة الثانية 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام الأساسية التي تتولى بها الهيئة وهي على سبيل الحصر الهدف منها هو الوقاية من الجرائم المعلوماتية ومكافحتها من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية وأبرز مهام هذه الهيئة هي: [2]

1. اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
2. تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
3. مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

[1]- المادة 01 من المرسوم الرئاسي رقم 15-261، المصدر السابق، ص 16.

[2]- المادة 04 ، المصدر نفسه، ص 17.

4. ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات أخرى.
5. تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
6. السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
7. تطوير التعاون مع المؤسسات والهيئات الونية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
8. المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.
9. المساهمة في تحديد المعايير القانونية في مجال اختصاصها.

**الفرع الثاني:تشكيل الهيئة:**

تضم لهيئة لجنة مديرة ومديرة عامة ومديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية التنسيق التقني ومركز للعمليات التقنية وملحقات جهوية[1]، حيث يرأس اللجنة المديرة الوزير المكلف بالعدل وتتشكل من الوزير المكلف بالداخلية والوزير المكلف بالبريد وتكنولوجيات الاتصال وقائد الدرك الوطني والمدير العام للأمن الوطني وممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع الوني وقاضيات من المحكمة العليا يعينها المجلس الأعلى للقضاء.[2]

اكتفى المشرع الجزائري بالإشارة إلى أعضاء اللجنة المديرة ووحدات المراقبة فقط، ولم يفصل في عضوية باقي التشكيلة المذكورة في المادة 2 من المرسوم الرئاسي 15-261 واكتفى بالإحالة غلى قرار

[1]- المادة 6 من المرسوم الرئاسي 15-261، مصدر سابق، ص 17.

[2]- هشام بخوش، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل التشريع الجزائري، جامعة خنشلة، العدد 07، جانفي 2017، ص 14.

مشترك يصدر بين الوزير المكلف بالعدل والوزير المكلف بالدفاع والوزير المكلف بالداخلية (المادة 15 من المرسوم الرئاسي 15-261)، كما أن السمة الطاغية على التشكيلة هي الأمنية وهو ما يعكس الدور الأصيل للهيئة، وقد تشكلت من عضو واحد عن وزارة البريد والمواصلات السلكية واللاسلكية وكان من الصواب إقحام ممثل لسلطة ضبط البريد والمواصلات السلكية واللاسلكية لما تتمتع به من خبرة وتخصص في هذا المجال.[1]

### 1. المديرية العامة:

يترأس المديرية العامة مدير عام يعين بمرسوم رئاسي[2]من دون تحديد وضبط تشكيلتها، ويمكن للهيئة الاستعانة بالقضاة وأعوان الشرطة القضائية، وأفراد من الاجهزة العسكرية عند الحاجة لأغراض الاستعلام، وكذا أعوان من الجمارك وأمن الدولة، كما يجوز الاستعانة بكفاءات فنية وإدارية أو التعاقد مع خبراء للقيام بمهام[3] محددة.

❖ **تعيين الأعضاء:**

اعتمد المشرع طريقة تعيين تعتمد على مرسوم رئاسي، حيث يعين كل من ممثل رئاسة الجمهورية، ممثل وزارة الدفاع الوطني، المدير العام للأمن الوطني، ومدير المراقبة الوقائية واليقظة الإلكترونية، ومدير التنسيق التقني بموجب مرسوم رئاسي كذلك، وتحددها صلاحياتهم وطريقة عملهم وفقا لما تنص عليه السلطة التنفيذية.[4]

تخضع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أثناء القيام بمهامها لنوعين من الرقابة هما:

---

[1]- حميدة بوادي وفطيمة بن سالم، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مذكرة لنيل شهادة الماستر، تخصص إعلام آلي وانترنت، كلية الحقوق والعلوم السياسية، جامعة البشير الإبراهيمي، برج بوعريريج، 2022-2023، ص 21.

[2]- المادة 09 من المرسوم الرئاسي 15-261، مصدر سابق.

[3]- المواد 18 و 19 من المرسوم الرئاسي 15-261، مصدر نفسه.

[4] - حميدة بوادي وفطيمة بن سالم، المرجع السابق، ص22.

**أ. رقابة السلطة التنفيذية:**

تمارسها السلطة التنفيذية كما هو مبين في المادة 32 من المرسوم الرئاسي 15-261، حيث تخضع الهيئة لمراقبة إدارية من قبل السلطات التنفيذية.

**ب. الرقابة القضائية:**

وفقا للمادة 04 من المرسوم 15-261، تعتبر الهيئة خاضعة للسلطة القضائية بحكم أن القضاء هو المكون الأساسي للهيئة المنصوص عليها في نفس المرسوم.

❖ **مديرية المراقبة الوقائية واليقظة الإلكترونية:**

لم يتطرق الأمر الرئاسي رقم 15-261 إلى تشكيلة هذه المديرية، لكن بالرجوع إلى تحليل المادة 18[1] من نفس القانون نجد أن هذه المديرية تتشكل من مجموعة من ضباط وأعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطني وكذلك الدرك الوطني والمصالح العسكرية للاستعلام والأمن. يتم تعيين مديرها بموجب مرسوم رئاسي موقع من رئيس الجمهورية، كما يتم إنهاء مهامه بنفس الطريقة.

تعمل هذه المديرية على إنجاز المهام التالية منها القيام بتنفيذ عمليات المراقبة والوقاية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناءا على رخصة مكتوبة تمنح من السلطة القضائية وتتم تحت مراقبتها، كما تقوم بإرسال المعلومات المتحصل عليها من خلال القيام بالمراقبة إلى السلطات القضائية مصالح الشرطة القضائية ومن مهامها أيضا تنفيذ الطلبات الواردة من الجهات القضائية الاجنبية في إطار التعاون الدولي في مجال مكافحة هذه الجرائم.

كما تتولى أيضا مهمة جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما تعمل على المشاركة في حملات التوعية حول مخاطر تكنولوجيات الإعلام والاتصال وكيفية استعمالها، كما تعمل على تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناءا على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المعلوماتية.[2]

[1] – المادة 18 من المرسوم الرئاسي 15-261، مصدر سابق.

[2] – المواد 11- 13-14-18-21 من المرسوم الرئاسي 15-261، مصدر سابق.

❖ **مديرية التنسيق التقني:**

يتم تعيين مديرها وإنهاء مهامه بموجب مرسوم رئاسي يصدره رئيس الجمهورية، أما تشكيلتها لم ينص عليها المرسوم الرئاسي رقم 15-261 مما يترك المجال للقول بأن تشكيلتها تكون وفقا لقرارات مشتركة بين وزراء العدل والدفاع والداخلية على شاكلة مديرية المراقبة الوقائية واليقظة الإلكترونية، غير أنهما يختلفان من ناحية المهام التي تتولاها هذه المديرية.

فتتمثل مهامها في النقاط التالية:

- إنجاز الخبرات القضائية في مجال اختصاص الهيئة.
- تكوين قاعدة معطيات تحليلية للإجرام المتعلق بتكنولوجيات الإعلام والاتصال.
- إعداد الإحصائيات الوطنية المتصلة بالإجرام المعلوماتي.
- تسيير المنظومة المعلوماتية وإدارتها.

❖ **مركز العمليات التقنية:**

يتم تزويد مركز العمليات التقنية بكافة الاجهزة والمعدات اللازمة بجانب توظيف الطاقم البشري المؤهل والمستخدمين المختصين لمراقبة الاتصالات الإلكترونية ويتبع هذا المركز إداريا لمديرية المراقبة واليقظة الإلكترونية حيث يتم تشغيله من طرفها.

**المطلب الثاني: الأجهزة الأمنية:**

إضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يوجد هناك كذلك هيئات تابعة للجهاز الأمني، مكلة بالتدخل للمواجهة العملية على المستوى التطبيقي للجرائم المعلوماتية، وتنقسم الهيئات التابعة للجهاز الامني والمكلف بالجرائم ذات الصلة إلى قسمين الهيئات التابعة لسلك الامن الوطني (الفرع الأول)، والوحدات التابعة للقيادة العامة للدرك الوطني (الفرع الثاني).

**الفرع الأول: الهيئات التابعة لسلك الأمن الوطني:**

يضم جهاز الأمن الوطني وحدات متخصصة تهدف إلى تنفيذ سياسة أمنية فعالة، مستفيدة من كافة الإمكانيات البشرية والتقنية المتاحة لأجل التصدي لكل أنواع الجرائم وخاصة تلك الجرائم المستحدثة مثل الجريمة المعلوماتية والتي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال وجاء هذا لحماية المصلحة العامة وكذلك حماية المصالح الخاصة المرتبطة بالتهديدات الناجمة عن هذه الجرائم التقنية.

ويوجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحري في الجرائم المعلوماتية وهي:

**أولا: على المستوى المركزي:**[1]

عملت المديرية العامة للأمن الوطني على إعادة تنظيم هيكلتها من خلال استحداث وحدات متخصصة، تهدف إلى مكافحة هذا النوع من الجرائم بشكل دقيق، فأنشأت المديرية العامة للشرطة القضائية مصلحة مختصة في مكافحة الجريمة المعلوماتية سميت بنيابة مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالإضافة إلى نيابة مديرية الشرطة العلمية والتقنية، حيث تعمل من أجل توفير الدعم التقني في البحث والتحري والتحقيق بشأن هذا النوع من الجرائم، وتسمى هذه الوحدة بالمخبر المركزي للشرطة العلمية والتي يكون مقره بالجزائر العاصمة.

يعمل هذا المخبر المركزي على فحص وتحليل الأدلة الجنائية وتقديم الدعم الفني والتقني للمحققين، كما يعمل على جمع الأدلة بطريقة علمية يمكن اعتمادها قضائيا، وقد سخرت لهذه الوحدة تجهيزات متطورة وتقنيات حديثة لمواكبة تطور هذا النوع من الجرائم.

**ثانيا: على المستوى الجهوي:**

تمت إنشاء مخابر جهوية للشرطة العلمية بكل من ولايتي قسنطينة ووهران، بالإضافة إلى ثلاث 03 مخابر أخرى قيد الإنجاز على مستوى ورقلة- بشار-تمنراست ينتظر تسليمها قريبا لأجل تعميم

[1] – عمار حشمان، المرجع السابق، ص 37.

هذا النوع من النشاط على كافة جهات الوطن، وتوجد على مستوى كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية، حيث تتكفل هذه المصلحة بأعمال البحث والتحري بشأن الجريمة المعلوماتية وذلك تحت تسمية "دائرة الأدلة الرقمية والآثار التكنولوجية".[1] والتي لم تكن عند استحداثها سوى قسم، لكن مع تزايد انتشار الجرائم المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي:

1. قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.
2. قسم استغلال الادلة الناتجة عن الهواتف النقالة.
3. قسم تحليل الأصوات.

تضم الدائرة ثمانية 08 أعضاء محققين، بينهم أربع محققين، بالإضافة إلى أربعة 04 عناصر شرطة رسميين يحملون صفة ضباط شرطة قضائية، جميعهم حاصلون على شهادات جامعية في تخصص إعلام آلي، إضافة إلى إلمامهم بالجانب القانوني، مما يعزز من كفاءتهم في مجال عملهم، حيث يخضع هؤلاء الأعضاء بشكل دوري لدورات تكوينية متخصصة في الجرائم المعلوماتية، لأجل الإطلاع على أحدث الإجراءات القانونية والتقنية في مجال الجرائم المعلوماتية.[2]

تلعب الجهات المختصة دورا فعالا في الكشف والتحري عن الجريمة المعلوماتية من خلال استعمال وسائل وإجراءات مختلفة ومتعددة وتقوم في مرحلتين: مرحلة البحث والتحري ومرحلة تتمثل في التحقيق القضائي.

- **مرحلة البحث والتحري:**

غالبا ما يتولى أعضاء هذه الجهات مهمة تنفيذ الطلبات التي تقدم لهم من قبل ضباط الشرطة المتخصصين بمكافحة الجريمة المعلوماتية المنتشرين عبر مختلف مديريات الأمن الوطني، أو من قبل وكلاء

[1] – عمار حشمان، المرجع السابق، ص 37.

[2] – حسين ربيعي، آليات التحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في الحقوق، تخصص قانون العقوبات العلوم الجنائية، جامعة باتنة 1، السنة الجامعية 2015-2016، ص 18.

الجمهورية أو قضاة التحقيق، وذلك بغرض جمع الأدلة وإثبات الجريمة بدعم تقني، كما تتولى هذه المرحلة أيضا إصدار الأوامر بتفتيش المحلات وحجز الوسائط الرقمي المحتوية على الأدلة.

- **مرحلة التحقيق القضائي:**

يقتصر دور الدائرة على إعداد تقارير فنية بناءا على طلبات وكيل الجمهورية أو قاضي التحقيق، ولا يتعدى ذلك إلى دور الخبير، وتعهد إلى المحققين مهمة فحص وتحليل الأدلة الإلكترونية المحجوزة، بما يشمل استخراج البيانات الرقمية، مثل تحليل محتوى الأقراص الصلبة الخاصة بالحواسيب المستخدمة في ارتكاب الجريمة. كما يشمل ذلك أيضا مراجعة جميع وسائط التخزين الإلكترونية على اختلاف أنواعها وتعمل كذلك على تحليل المواقع الإلكترونية المخترقة أو المستعملة في تنفيذ الأفعال الإجرامية مع تحديد مواقعها الجغرافية ومواقع المستخدمين ويتم ذلك باستخدام أجهزة حديثة تقنية ومتطورة ودقيقة ووسائل مادية ذات جودة عالية.[1]

**ثالثا: على المستوى المحلي:**

في إطار تعزيز قدرات الشرطة القضائية في التصدي للجريمة المعلوماتية، بادرت المديرية العامة للأمن الوطني منذ سنة 2016 إلى إنشاء قرابة 48 فرقة متخصصة على المستوى المحلي، تهدف إلى تحسين الأداء في لتحقيقات المرتبة بهذه الجرائم المستحدثة.

**الفرع الثاني: الوحدات التابعة للقيادة العامة للدرك الوطني:**

يضع الدرك الوني لتنفيذ مهامه في مجال المحافظة على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية وهي كالتالي:

1. قيادة الدرك الوطني.
2. الوحدات الإقليمية.
3. الوحدات المشكلة.

[1] – حسين سعيداني، آليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص 181.

**4**. الوحدات المتخصصة وحدات الإسناد.

**5**. هياكل التكوين.

**6**. المعهد الوني للأدلة الجنائية وعلم الإجرام.

**7**. المصالح والمراكز العلمية والتقنية.

**8**. المصلحة المركزية للتحريات الجنائية.

**9**. المفرزة الخاصة للتدخل.[1]

تعمل مؤسسة الدارك الوطني جادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الانترنت، وهذا لتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحواسيب والعمل على مراقبة مختلف الشبكات وبالتالي فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، وذلك حسب الاختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث 03 مستويات مركزية جهوية محلية.[2]

**أولا: على المستوى المركزي**

يوجد على المستوى المركزي هيئات تتكفل بمكافحة الجريمة المعلوماتية يمكن إجمالها في:

**أ. المعهد الوطني للأدلة الجنائية وعلم الإجرام:**

أنشأ المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب مرسوم رئاسي 04-183[3]، يعد هذا المعهد مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزارة الدفاع الوطني المكلف بإجراء الفحوص العلمية في إطار التحريات الأولية، وإجراءات البحوث المتعلقة بالكشف عن الإجرام باللجوء إلى التكنولوجيا الحديثة والدقيقة[4]، ويتكون من مجموعة من المصالح: مصلحة البصمات ومصلحة

[1] – حسين ربيعي ، مرجع سابق، ص 41.

[2] – عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، ص 41.

[3] – مرسوم رئاسي 04-183 المؤرخ في 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، ج.ر.ج.ج، ع41، الصادرة بتاريخ 27 يونيو 2004.

[4] – التفصيل أكثر حول هذه النقطة، المادة الرابعة من المرسوم الرئاسي 04-183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني السالف الذكر.

الإعلام الآلي، حيث يتم على مستوى هذه المصلحة رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وتفكيك البرامج المعلوماتية.

ومن المهام التي يقوم بها المعهد الوطني للأدلة الجنائية وعلم الإجرام تتلخص في ما يلي:[1]

- إنجاز الخبرات والتحاليل بناء على طلبات القضاة المحققين والسلطات المؤهلة.
- الدعم التقني للوحدات أثناء التحقيقات المعقدة.
- تصميم بنوك معطيات وإنجازها وفقا للقانون.
- المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- الإسهام في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحث التطبيقي وأساليب التحريات التي تثبت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المشاركة في تنظيم دورات تحسين المستوى والتكوين ما بعد التخرج في تخصصات العلوم الجنائية.

**ب. مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:**

في سنة 2008 أنشأ هذا المركز، ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحري في الجرائم المعلوماتية[2]، فهو هيئة تقنية تعمل تحت وصاية مديرية الامن العمومي والاستغلال لقيادة الدرك الوطني ويحقق المهام التالية:

- ضمان المراقبة الدائمة والمستمرة على شبكة الانترنت.

[1] – الموقع الرسمي لقيادة الدرك الوطني:

. http:www.mdn.dw/site/dz, visité le 09/05/2025 à 20 :00.

[2] – عز الدين عز الدين– قيادة الدرك الوطني – الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، ص 29.

- القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.
- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال والبحث عن الأدلة في شبكة الانترنت.
- المشاركة في عمليات التحري والتسرب عبر شبكة الانترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.
- المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

**ج. مديرية الأمن العمومي والاستغلال:**

وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

**د. المصلحة المركزية للتحريات الجنائية:**

وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والاتصال.[1]

**ثانيا: على المستوى الجهوي:**

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية، وكذلك دعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة كالجرائم المعلوماتية.

[1] – سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، المجلد 07، ع 01، مجلة القانون العام الجزائري والمقارن، جوان 2021، ص 281.

يلعب الدرك الوطني دورا هاما في ميدان الشرطة القضائية نظرا لانتشار وحداته على مستوى كامل التراب الوطني، ونظرا للوسائل المادية الموضوعة تحت تصرفه وعدد أفراده الهائل والصلاحيات التي خولها لهم القانون، وهم في الواقع حسب الرتب والوظائف ضباط وأعوان الشرطة القضائية.

**ثالثا: على المستوى المحلي:**

يحوز الدرك الوطني على فصائل للأبحاث التي ينتمي إليها أفراد ذو خبرة واختصاص واسعين في ميدان الشرطة القضائية، هذه الفصائل مكلفة خصوصا بمكافحة هذا النوع من الجرائم كالجريمة المعلوماتية، وكذلك عن ريق القيام بتحقيقات تتطلب تحريات معقدة ، هذه الوحدات المختصة تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني.

## المبحث الثاني: الإجراءات القانونية للكشف عن الجريمة المعلوماتية

أمام تطور الجريمة المعلوماتية وتعقيد أساليب ارتكابها، وجد المشرّع الجزائري نفسه مطالبًا بمواءمة الإجراءات القانونية لتتلاءم مع طبيعة هذا النوع من الجرائم .فبالرغم من إمكانية اعتماد بعض إجراءات التحري الكلاسيكية المنصوص عليها في قانون الإجراءات الجزائية، إلا أن فعاليتها تبقى

محدودة في مواجهة الجرائم التي ترتكب في بيئة افتراضية .ولهذا الغرض، تم إدراج إجراءات مستحدثة تمكّن من تعقب الأدلة الرقمية وكشف مرتكبي الجرائم المعلوماتية.

وعليه، سنتناول في هذا المبحث الإجراءات القانونية المعتمدة في التشريع الجزائري للكشف عن الجريمة المعلوماتية، من خلال التطرق في المطلب الأول إلى الإجراءات الكلاسيكية، وفي المطلب الثاني إلى الإجراءات المستحدثة

## المطلب الأول: إجراءات التحري الكلاسيكية

رغم الطابع الحديث والمعقّد للجريمة المعلوماتية، لا يزال المشرّع الجزائري يعتمد على وسائل التحري الكلاسيكية، وعلى رأسها المعاينة والتفتيش، للكشف عنها وجمع الأدلة .وقد حاول تكييف هذه الإجراءات التقليدية مع طبيعة الجرائم المرتكبة في بيئة رقمية، خاصة بعد تعديل قانون الإجراءات الجزائية بموجب القانون .04-18 وسنقوم في هذا المطلب بدراسة هذه الإجراءات، من خلال التطرق في الفرع الأول إلى المعاينة، وفي الفرع الثاني إلى التفتيش، مع بيان كيفيات تطبيقهما في مجال الجريمة المعلوماتية وفقًا للتشريع الجزائري.

### الفرع الأول: المعاينة

تعد المعاينة من أولى الإجراءات التحري المعتمدة في التشريع الجزائري، وتهدف إلى إثبات حالة الأماكن أو الأشياء المرتبطة بالجريمة، وقس مجال الجرائم المعلوماتية، تأخذ المعاينة طابعا خاصا يراعي طبيعة الأدلة الرقمية وبيئة ارتكاب الفعل الإجرامي وهذا ما ستناوله في هذا الفرع.

#### أولا: تعريفها

هي إجراءات عملية انتقال الجهات المختصة بسرعة إلى موقع ارتكاب الجريمة مباشرة بعد وقوعها مباشرة لتفادي مرور وقت طويل قد يسمح للجاني بإخفاء أو تغيير الأدلة المادية التي يمكن أن تكشف

الحقيقة، وهذا من أجل توثيق حالة المكان والأشخاص الموجودين فيه، وجمع كل ما يمكن أن يساعد من في كشف ملابسات الجريمة والتعرف على الجاني.[1]

تنص المواد 42، 79 و 80 من ق.إ.ج على أن المعاينة يمكن أن تجرى من قبل قاضي التحقيق بعدم إعلام وكيل الجمهورية الذي يمكنه مرافقته خلال المعاينة وفي حال اقتضى الضرورة يمكن توسيع صلاحيات قاضي التحقيق لتشمل محاكم أخرى مجاورة، كما يجوز أيضا لضباط الشرطة القضائية القيام بالمعاينة، لكن يجب عليهم فور عملهم بالجريمة الانتقال بسرعة إلى مكان وقوعها دون تأخير، مع إبلاغ وكيل الجمهورية بذلك فورا.[2]

يعتبر مسرح الجريمة بمثابة شاهد صامت، فإذا أحسن المحقق التعامل معه وتحليل معطياته، يمكنه الوصول إلى معلومات حاسمة تساعد في كشف ملابسات الجريمة.[3]

**ثانيا: معاينة مصرح الجريمة**

ولمعاينة مسرح الجريمة يجب التفرقة بين حالتين:

**1. المسرح الافتراضي:**

معاينة مسرح الجريمة في الجرائم الإلكترونية تتم داخل بيئة الحاسوب وما يحتويه من بيانات رقمية تنتقل وتخزن في الذاكرة أو على الأقراص الصلبة، ويقصد بالمعاينة تتبع الآثار الإلكترونية التي يتركها المستخدم أثناء استخدامه للشبكة، مثل الرسائل التي أرسلها أو استقبلها، وسجل اتصالاته الالكترونية. كما تشمل عملية المعاينة التحقق من أنشطة المتهم على الانترنت، كالدخول إلى بريده الالكتروني أو

[1]- زهية معمش، نسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمن ميرة – بجاية- كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2012-2013، ص ص 6، 7.

[2]- المرجع نفسه، ص 9.

[3]- عبد الرؤوف بوديسة بجاد، آليات التحري عن الجريمة الإلكترونية في القانون الجزاري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر في مهني في الحقوق، تخصص قانون الإعلام الآلي والانترنت، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحقوق والعلوم السياسية، 2022/2021، ص 56.

حسابه على مواقع التواصل الاجتماعي، ومن خلال فحص جهاز الحاسوب الخاص به، يمكن الكشف عن المواقع التي زارها أو الملفات التي قام بتنزيلها.[1]

بإمكان المعاينة في الجرائم الإلكترونية أن تتم دون الحاجة للانتقال فعليا إلى موقع مادي، إذ يمكن تنفيذها داخل الفضاء الرقمي نفسه. وهناك عدة وسائل متاحة أمام المحقق للدخول إلى هذا العالم الافتراضي ومنها:

- استخدام جهاز الحاسوب الموجود في مكتبه داخل المحكمة للولوج إلى الأدلة الرقمية.
- التوجه إلى احد المقاهي الانترنت لتنفيذ المعاينة.
- الاستعانة بمزود خدمة الانترنت والذي يعد من أفضل الأماكن التي يمكن فيه إجراء هذا النوع من المعاينات نظرا لما يملكه من بيانات تقنية مهمة.[2]

### 2. المسرح التقليدي:

هو المكان الواقعي الذي حدثت فيه الجريمة ويكون خارج البيئة الرقمية إذ يتكون من العناصر المادية كالموقع الفعلي للجريمة. في هذا النوع من المسرح قد يترك الجاني آثار مادية مثل البصمات أو أغراضه الشخصية أو حتى أجهزة تخزين رقمية.[3]

### ثالثا: الضوابط الواجب مراعاتها عند معاينة مسرح الجريمة

وعليه يجب إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة المعلوماتية والمتمثلة في:

❖ من الضرورة جمع معلومات مسبقة عن موقع الجريمة مثل عدد الأجهزة التي يجب فحصها ونوع الشبكات الموجودة وذلك لتحديد الاحتياجات الفنية بدقة.

---

[1]- خضرة شنبر، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة أحمد دراية أدرار، 2021/2020، ص 65.

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

[3]- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار النشر، كلية الحقوق جامعة الإسكندرية، 2006، ص 85.

- ❖ يجب توفير خريطة مفصلة للموقع المستهدف، توضح المبنى أو الطابق المعني، مع تحديد أماكن الأجهزة، الخزائن والملفات، ويفضل الحصول على هذه المعلومات من مصادر أمنية موثوقة.
- ❖ ينبغي حصر الاجهزة التي يحتمل أن تكون لها علاقة بالجريمة الإلكترونية، لتحديد طريقة التعامل معها فنيا أثناء المعاينة.
- ❖ تأمين جميع الادوار والمعدات اللازمة للمعاينة، سواء كانت أجهزة تقنية أو برامج متخصصة.
- ❖ تجهيز فريق من المتخصصين يضم خبراء فنيين ورجال أمن وضبط، مع توضيح مهام كل فرد بشكل دقيق لتجنب تضارب الأدوار.
- ❖ وضع خطة واضحو ومفصلة للمعاينة تشمل الرسومات والبيانات الضرورية على أن تتم مراجعتها جيدا قبل التنفيذ لضمان الدقة والفعالية.
- ❖ التأكد من استمرار توفر التيار الكهربائي وال فترة المعاينة، لأن توقف الكهرباء يعيق فحص الأجهزة والبرامج والشبكات بشكل كامل وفعال.[1]

**الفرع الثاني: التفتيش**

يعد التفتيش من الوسائل الأساسية التي يقرها التشريع الجزائري للكشف عن الأدلة وإثبات الجرائم، وفي سياق الجريمة المعلوماتية يكتسي هذا الإجراء أهمية خاصة نظرا لارتباطه باختراق الأنظمة والأجهزة الرقمية التي قد تحتوي على بيانات حاسمة

**أولا: تعريف التفتيش**

هو أحد إجراءات التحقيق المهمة ويهدف إلى الوصول إلى الحقيقة من خلال البحث في الأماكن التي قد تخفى فيها الادلة. يعد هذا الإجراء من ابرز وسائل التحقيق لأنه غالبا ما يؤدي العثور على أدلة مادية تدعم توجيه الاتهام إلى شخص معين، ولا يحق تنفيذ التفتيش إلا للنيابة العامة أو قاضي التحقيق ويكون الهدف الأساسي منه هو جمع أدلة تثبت وقوع الجريمة وقد يشمل التفتيش أماكن مختلفة مثل مساكن المتهمين أو الأشخاص المرتبطين بالقضية، سواء كانوا متهمين أو غير متهمين.[2]

[1]- عائشة بن قارة مصطفى، المرجع السابق، ص 87.

[2]- أسماء عاصف، مرجع سابق، ص 15.

رغم أن المشرع الجزائري اعتبر التفتيش أحد إجراءات التحقيق المهمة وأحاطه بقيود قانونية صارمة، إلا أنه لم يقدم تعريفا دقيقا وواضحا له وقد أولى الدستور الجزائري أهمية كبيرة لحماية حرية وكرامة الأفراد، حيث نص في لمادة 41 منه: " فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلة القضائية المختصة " ومنه نستنتج من نص المادة أن التفتيش لا يجوز إلا وفقا للقانون ويجب أن يتم بأمر مكتوب صادر عن جهة قضائية مختصة، بما يضمن احترام حقوق الأشخاص وعدم انتهاكها.[1]

أما بالنسبة للجرائم المعلوماتية فأن التفتيش يتركز أساسا على الحاسوب، سواء في جوانبه المادية أو المعنوية. فالأولى أي المكونات المادية تشمل وحدات الأجهزة التي تعمل معا ضمن نظام متكامل في حين تشمل المكونات المعنوية البرامج والأنظمة والبيانات الإلكترونية. ولا يعد تفتيش الأجهزة المادية امرا معقدا فإن الصعوبة تظهر عند استهداف المكونات المعنوية إذ يتطلب ذلك في الكثير من الأحيان تجاوز حواجز مثل كلمات لمرور أو فك الشفرات المستخدمة لحماية البيانات.

**ثانيا: شروط وضوابط التفتيش**

تنقسم شروط التفتيش إلى نوعين: شروط شكلية وأخرى موضوعية.

**1. الشروط الشكلية للتفتيش:**

**❖ أن يتم التفتيش على إذن مكتوب:**

ينبغي أن يتم تفتيش نظام الحاسوب الآلي بناء على إذن كتابي صادر عن وكيل لجمهورية أو قاضي التحقيق، كما نصت عليه المادة 44 من ق.إ.ج.ج، ويشترط قبل الشروع في عملية التفتيش، وجوب إظهار هذا الإذن القانوني من أجل الدخول إلى المكان المعني بشكل رسمي للتفتيش.إن تفتيش أنظمة الكمبيوتر يستلزم صدور مذكرة قضائية تجيز هذا الإجراء صراحة، حيث أن القيام بالتفتيش دون توفر تلك المذكرة يعد محل جدل كبير، خاصة في ظل القواعد القانونية التي تكفل حماية الحياة الخاصة وحقوق الأفراد. ويجب أن تكون المذكرة محددة وواضحة فيما يتعلق بالنظام المعلوماتي المراد تفتيشه.[2]

[1]- آسيا بن زرت، مرجع سابق، ص 22.

[2]- فريال العاقل، المرجع السابق، ص 71.

❖ **الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش الخاص بنظام الحاسوب الآلي:**

ألزم المشرع الجزائري في الفقرة الأولى من المادة 45 من ق.إ.ج.ج بأن يجري التفتيش بحضور صاحب المسكن المعني.

استثنى المشرع الجزائري بموجب المادة 45 من القانون رقم 22/06 الصادر بتاريخ 20 ديسمبر 2006، حضور بعض لأشخاص أثناء التفتيش وذلك في حال كان التفتيش مرتبطا بالجرائم التي تمس أنظمة المعالجة الآلية للمعطيات، ورغم هذا الاستثناء أوجب القانون الحفاظ على السر لمهني، بالإضافة إلى ضرورة جرد الأشياء وحجز الوثائق عند الاقتضاء.أما إذا كان التفتيش يخص مسكن شخص موقوف للنظر أو محبوس في مكان آخر، فقد ألزم المشرع وفقا للمادة 47 أن يتم ذلك بحضور شاهدين يتم تسخريهما أو بحضور شخص يمثل صاحب المسكن ويعن من قبله.[1]

❖ **إعداد محضر خاص بالتفتيش:**

يكلف الشخص القائم بالتفتيش باصطحاب كاتب يتولى تدوين محضر خاص بعملية التفتيش والضبط يوثق فيه كل ما يجري أثناء التفتيش بدقة وتفصيل، مع تسجيل كافة البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة وحرص.

❖ **إجراءات تنفيذ تفتيش نظام الحاسوب الآلي وميعاده:**

يتميز تفتيش أنظمة الحاسوب الآلي بخصوصية تفرضها طبيعة هذه الأنظمة، نظرا لما تتطلبه من دقة في التعامل مع الاجهزة والبرمجيات لذلك من الضروري تحديد نوع النظام المراد تفتيشه مسبقا، كما يجب أن يمتلك القائم بالتفتيش معرفة واسعة في مجال الإعلام الآلي تمكنه من فهم طبيعة النظام المستهدف. وفي حال الحاجة يمكن الاستعانة بخبراء متخصصين لتقديم الدعم الفني أثناء عميلة التفتيش.

وعند تنفيذ أمر التفتيش يتوجب على القائمين به اتخاذ الإجراءات التالية:

- تأمين موقع الجريمة من خلال فصل التيار الكهربائي عن الأجهزة ومزودات الانترنت وذلك لتعطيل أي محاولة من الجاني للتلاعب بالأدلة.

[1]– فريال العاقل، المرجع السابق، ص 70.

- إبعاد الشخص المشتبه به عن النظام إن كان متواجد بالقرب منه.
- التأكد من منع المتهم من الوصول عن بعد إلى النظام المعلوماتي.
- الدخول إلى موقع التفتيش بحذر لتجنب إتلاف أو تشويه الأدلة الرقمية.
- تجنب استخدام لوحة المفاتيح، لأن ذلك قد يتطلب لاحقا استعمال أدوات وبرامج خاصة قد تؤثر على الأدلة أي تضر بالبيانات.
- توثيق جميع الملاحظات وكلمات المرور ورموز التشفير وغيرها من البيانات الفنية التي قد تساهم في كشف الجريمة وإثباتها.

أما فيما يخص مدة التفتيش، فإن المشرع الجزائري لم يضع سقفا زمنيا محددا لهذا الإجراء ويترك الأمر إلى السلطة التقديرية، خصوصا أن الجرائم المعلوماتية غالبا ما تحدث خلال الليل، نظرا لانخفاض تكلفة الاتصال وسهولة الوصول إلى الأنظمة المستهدفة في تلك الفترات لقلة المستخدمين وهذا ما أشار إليه صراحة في نص الفقرة الثالثة من المادة 47 من ق.إ.ج.ج.[1]

### 2. الشروط الموضوعية:

وتشمل ما يلي:

- أن تكون هناك جريمة إلكترونية وقعت فعلا، أي استخدام غير قانوني لأجهزة الحاسوب بهدف تحقيق أغراض مخالفة للقانون.
- أن يكون هناك اشتباه في تورط شخص أو أكثر في ارتكاب هذه الجريمة أو المساعدة فيها.
- أن تتوفر مؤشرات قوية أو أدلة مبدئية تشير إلى وجود أجهزة أو أدوات إلكترونية قد تساهم في كشف ملابسات الجريمة.
- يجب أن يكون موضوع التفتيش هو جهاز الحاسوب بجميع مكوناته سواء كانت مادية كالأجهزة والمعدات أو معنوية كالبرمجيات والبيانات بالإضافة إلى شبكات الاتصال المرتبطة به.[2]

[1]- عمار حشمان، المرجع السابق، ص ص 51- 53.

[2] - خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 154.

**ثالثا: خضوع أنظمة الحاسب الآلي للتفتيش:**

**1. تفتيش المكونات المادية للحاسوب:**

بالنسبة لتفتيش مكونات الحاسوب المادية لا يوجد خلاف حول إمكانية خضوعها للتفتيش، لكن ذلك يعتمد أساسي على طبيعة المكان الموجود فيه الحاسوب فإذا كان المكان خاصا فلا يجوز تفتيش تلك المكونات إلا وفقا لنفس الضوابط و الإجراءات القانونية المعتمدة في حالات التفتيش التقليدية، أما إذا كان المكان عاما فلا يمكن التفتيش إلا وفقا لنفس الشروط والقيود التي تحكم تفتيش الأشخاص.

**2. تفتيش المكونات المعنوية للحاسوب:**

ثار جدل فقهي حول مدى إمكانية إخضاع المكونات المعنوية للحاسوب لإجراءات التفتيش، وانقسمت الآراء إلى اتجاهين رئيسيين الأول يرفض فكرة تفتيش هذه المكونات ويستند إلى ضرورة حمايتها بموجب قوانين الملكية الفكرية، وقد تبنت بعض الدول هذا التوجه وأكدت على ضرورة صون الكيانات المنطقية للحاسوب من أي انتهاك.

أما الاتجاه الثاني، فيرى أن المكونات المعنوية للحاسوب يمكن تفتيشها طالما أنها تشغل حيزا ماديا في الذاكرة ويمكن قياسها والتحكم فيها. فبرامج الحاسوب على الرغم من طابعها غير المادي يتم تخزينها في وحدات مادية قابلة للقياس مثل "البايت" و " الكيلوبايت" و "الميغابايت" وهو ما يجعلها تخضع من حيث المبدأ لإجراءات التفتيش، لكن الإشكالية تكمن في أغلب النصوص القانونية المنظمة للتفتيش وضعت قبل ظهور مفهوم الكيانات غير المادية وبالتالي فإن تطبيق هذه القواعد التقليدية على النظم المعلوماتية قد لا يكون مناسبا بل ويتعارض أحيانا مع المبادئ الأساسية للشرعية الإجرائية، لذلك فإن التعامل مع البيانات الرقمية يتطلب إطارا قانونيا خاصا يراعي طبيعتها الفريدة.[1]

[1] – عبد العزيز أحمد، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، جامعة الدكتور الطاهر مولاي سعيدة، كلية الحقوق والعلوم السياسة، قسم الحقوق، 2021-2022 م الموافق لـ 1442-1443 هـ، ص ص 87، 88.

من خلال المادة 5 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، يتضح لنا بوضوح.

**رابعا: مدى خضوع شبكات الحاسب الآلي للتفتيش:**

تعد شبكات الحاسب الآلي وسيلة أساسية لربط أجهزة الحاسوب ببعضها، سواء داخل نطاق محلي أو على مستوى عالمي. وبالرجوع إلى المادة 05 من القانون 09-04 فإن إمكانية إخضاع هذه الشبكات للتفتيش تنقسم إلى حالتين أساسين:

❖ **حالة 01: وجود جهاز متصل بجهاز المتهم داخل الدولة:**

إذا كان نظام المتهم متصلا بنظام معلوماتي آخر داخل البلاد وأثناء تفتيش النظام الأول تبين أن هناك مؤشرات توحي بأن البيانات المطلوبة موجودة على النظام الثاني، وكان بالإمكان الوصول إليها من خلال النظام الأول، فإنه يسمح بتمديد عملية التفتيش لتشمل النظام الآخر أو جزءا منه، بشرط إعلام السلطة القضائية المختصة مسبقا بذلك، وذلك وفقا لما نصت عليه الفقرة الثانية من المادة 05 من القانون 09-04.[1]

❖ **حالة 02: جهاز متصل بجهاز المتهم خارج الدولة:**

بالإمكان الوصول إلى منظومة أو جزء منها بما ذلك البيانات المخزنة فيها عن بعد، وفي حال كانت البيانات المستهدفة موجودة في منظومة معلوماتية تقع خارج التراب الوطني، فإن الحصول عليها يتم بالتنسيق مع الجهات الأجنبية المختصة، وفقا للاتفاقيات الدولية المعمول بها والاستناد إلى مبدأ المعاملة بالمثل. كما يمكن الاستعانة بأشخاص ذوي خبرة في تشغيل هذه المنظومات أو في الوسائل المعتمدة لحماية المعلومات التي تحتويها.[2]

حيث نصت المادة 05 من القانون 09- 04 على أنه : " إذا تبني مسبقا أن المعطيات المبحوث عنها والتي يمكن الوصول إليها انطلاقا من المنظومة الاولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم

[1] – نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، علوم جنائية، جامعة الحاج لخضر-باتنة، كلية الحقوق والعلوم السياسية، 2013، ص149.

[2] – عائشة نايري، المرجع السابق، ص 50.

الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل".[1]

موقف المشرع الجزائري، حيث أقر صراحة حق السلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في الدخول إلى الأنظمة المعلوماتية أو اجزاء منها بهدف التفتيش، سواء بشكل مباشر أو عن بعد، وذلك في إطار ما يسمح به قانون الإجراءات الجزائية (ق.إ.ج.ج) ويشمل هذا التفتيش المعطيات الرقمية المخزنة داخل هذه الأنظمة أو في وسائط التخزين المعلوماتية المرتبطة بها.[2]

## المطلب الثاني: الإجراءات المستحدثة للكشف عن الجريمة المعلوماتية

نظرا لخطورة الجرائم الإلكترونية وصعوبة التعرف على هوية مرتكبيها باستخدام طرق التحقيق التقليدية، استحدث المشرع الجزائري جملة من الآليات الخاصة ضمن التعديل الجديد لقانون الإجراءات الجزائية بموجب القانون 22- 06 ومن بين هذه الوسائل المستحدثة: تقنية التسرب(الاختراق الإلكتروني) واعتراض المراسلات وتسجيل الأصوات والتقاط الصور وهذا ما سنتناوله في هذا المطلب.

### الفرع الأول:أسلوب التسرب أو الاختراق الإلكتروني

تعد تقنية التسرب أسلوبا جديدا وحساسا للغاية في مجال عمل الضبطية القضائية، لما لها من تأثير بالغ على الأمن، تتطلب هذه التقنية جرأة ومهارة ودقة عالية في التطبيق وقد أقر المشرع الجزائري هذه التقنية ضمن تعديلات ق.إ.ج.ج لعام 2006 وفي هذا السياق سنتناول تعريف التسرب والشروط اللازمة لتطبيقه.

#### أولا: تعريف التسرب

[1] – المادة 5 من الامر رقم 09-04، مصدر سابق.

[2] – أسماء عاصف، المرجع السابق، ص 54.

نظم المشرع الجزائري إجراء "التسرب الإلكتروني" أو ما يعرف بالاختراق في إطار قانون الإجراءات الجزائية، وذلك من خلال المواد الممتدة من المادة 65 مكرر 11 إلى المادة 65 مكرر 18، وقد بينت هذه المواد مفهوم التسرب الإلكتروني وشروطه، وتتمثل هذه العملية في سياق الجريمة الإلكترونية، في تمكن ضابط أو عون من الشرطة القضائية من الدخول إلى القضاء الافتراضي، سواء باختراق مواقع إلكترونية معينة أو الانضمام إلى غرف الدردشة، مع التظاهر بأنه أحد المشاركين مستخدما اسما مستعارا وكأنه فاعل مثلهم.[1]

التسرب يعد من التقنيات من التقنيات الحديثة والخطيرة في مجال الضبطية القضائية، حيث يستلزم تنفيذها جرأة عالية، ودقة كبيرة، وكفاءة مهنية. وقد نظم المشرع هذه الجزائري هذه الآلية من خلال التعديل الذي طرأ على ق.إ.ج سنة 2006.

يعتبر التسرب من أساليب التحري والتحقيق الخاصة، حيث يمكن لضابط أو عون من الشرطة القضائية التسلل إلى داخل جماعة إجرامية، وذلك تحت إشراف ومتابعة ضابط شرطة قضائية مكلف بتنسيق العملية.وتتمثل الغاية من هذا الإجراء في مراقبة المشتبه فيهم وكشف أنشطتهم غير المشروعة، مع اعتماد المتسرب على إخفاء هويته الحقيقية وتقديم نفسه على أنه أحد المتشاركين في النشاط الإجرامي، سواء كفاعل مباشر أو كشريك.[2]

ويعتبر البعض أن هذا النوع من رسائل التحري الأكثر تعقيدا وخطورة، لأنه يتطلب من ضابط الشرطة ومساعديه القيام بتصرفات ومناورات توحي بأنهم شركاء حقيقيون في الجريمة إلى جانب باقي أفراد العصابة. لكن في الواقع هم لا يشاركون فعليا بل يخدعون المجرمين ويتظاهرون بأنهم جزء من المخطط الإجرامي بهدف التسلل إلى داخل التنظيم وكشف أسراره ومن خلال هذا الأسلوب يتمكنون

[1] – عبد القادر فلاح، نادية آيت عبد الله، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، العدد 2، المجلد 04، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، 2019، ص 1698.

[2] – عبد الرؤوف، بوديسة بجاد، المرجع السابق، ص 68.

من جمع الأدلة اللازمة وإبلاغ السلطات بها، مما يساهم في توقيف المجرمين ووضح حد لنشاطهم الإجرامي.[1]

حيث عرفه المشرع الجزائري من خلال المادة 65 مكرر 12 ف 2 بأنه:"قيام ضابط عون الشرطة القضائية تحت مسؤولية ضباط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"[2] ومنه نستنتج أن التسرب هو عملية يتولى فيها ضابط الشرطة القضائية التوغل إلى داخل الجماعات الإجرامية متظاهرا بأنه أحد أفرادها أو متعاطف معهم وذلك بهدف جمع الأدلة والإيقاع بهم.

يمكن تصور عملية التسرب في مجال الجريمة المعلوماتية من خلال قيام ضباط أو عون الشرطة القضائية بالتسلل إلى الفضاء الرقمي وذلك عبر اختراق مواقع محددة أو استغلال ثغرات إلكترونية فيها ، أو من خلال الانضمام إلى غرف الدردشة أو حلقات التواصل المباشر مع المشتبه فيهم، مظهرا نفسه كفاعل مشارك باستخدام أسماء وصفات وهمية ومستعارة، بهدف كشفهم والإيقاع بهم.[3]

**ثانيا: شروط التسرب**

[1] – وردة شرف الدين، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية، العدد 15، مجلة الفكر، جامعة محمد خيضر بسكرة، الجزائر، 15 جوان 2017، ص 545.

[2] – المادة 65 مكرر 12 فقرة 2 من قانون الإجراءات الجزائية.

[3] – إبراهيم زياد بوعرعارة، خصوصية الجريمة المعلوماتية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق، تخصص قانون جنائي، جامعة غرداية، كلية الحقوق والعلوم السياسية، قسم الحقوق 1442 هـ- 1443 هـ /2021-2022، ص 88.

بطبيعة الحال، فإن عملية التسرب تخضع لجملة من الشروط، وفي حال الإخلال بأي منها تعتبر العملية باطلة وقد تناولت المواد من 65 مكرر 11 إلى مواد 65 مكرر 15 هذه الإجراءات بشكل مفصل.[1]

- ❖ لا يتم اللجوء إلى هذا الإجراء غلا في جرائم محددة، من بينها تلك التي تمس أنظمة المعالجة الآلية للمعطيات.
- ❖ يجب أن رخصة (إذن) إجراء عملية التسرب إما من قبل وكيل الجمهورية (النيابة العامة) أو قاضي التحقيق، وذلك بعد إعلام وكيل الجمهورية.
- ❖ يجب أن يكون الإذن مكتوب ومعلل بشكل دقيق وإلا اعتبرت باطلة.
- ❖ يجب أن تتضمن الرخصة (الإذن) الأسباب القانونية التي تبرر العملية بالإضافة إلى هوية ضابط الشرطة القضائية المسؤول عنها وتحدد فيها مدة العملية، والتي لا يجوز أن تتجاوز أربعة (04) اشهر ويمكن تمديد هذه المدة بنفس الشروط القانونية والزمانية إذا اقتضى التحقيق أو البحث ذلك.
- ❖ كما يجوز للقاضي الذي منح الإذن أن يأمر في أي وقت بإيقاف العملية قبل نهاية المدة المحددة وتحفظ نسخة من هذه الرخصة في ملف الإجراءات بمجرد انتهاء عملية التسرب.[2]

عند انتهاء مدة رخصة التسرب أو في حال صدور قرار بوقف العملية، وإذا لم تمدد المدة، يمكن للعون المتسرب أن يواصل مهامه مؤقتا وبالقدر الضروري فقط وذلك لضمان إنهاء عملية المراقبة في ظروف آمنة تضمن سلامته، دون أن يتحمل مسؤولية جزائية، بشرط ألا تتجاوز هذه المدة أربعة (04) أشهر.

وفي هذه الحالات يتعين على العون إشعار القاضي الذي منح الرخصة في أقرب وقت ممكن، وإذا انقضت مدة الأربعة أشهر دون أن يتمكن العون من إنهاء مهمته في ظروف تضمن له الأمان،

[1] – إبراهيم زياد بوعرعارة، المرجع السابق، ص 88.

[2] – وردة شرف الدين، لمرجع السابق، ص 546.

يمكن للقاضي أن يمنحه تمديدا إضافيا لنفس المدة، أي أربعة (04) أشهر أخرى، إذا اقتضت الضرورة ذلك.

كما يمكن الاستماع لضابط الشرطة القضائية الذي أشرف على العملية بصفته شاهدا على مجريات التسرب دون إشراك غيره في هذا السياق.[1]

لا يجوز كشف الهوية الحقيقة لضباط أعوان الشرطة القضائية الذين شاركوا في عملية التسرب مستخدمين هويات مستعارة، وذلك في أي مرحلة من مراحل الإجراءات ويعاقب كل من يقوم بكشف هذه الهوية بالسجن من سنتين إلى خمس سنوات وبغرامة مالية تتراوح بين 50.000 دج إلى 200.000 دج.

وإذا أدى هذا الكشف إلى أعمال عنف أو ضرب أو جرح ضد أحد هؤلاء الضباط أو ضد أزواجهم أو أبنائهم أو أصولهم المباشرين، فإن العقوبة تشدد لتتراوح بين خمس (05) إلى عشر (10) سنوات وغرامة مالية من 200.000 دج إلى 500.000 دج

أما إذا تسبب الكشف في وفاة أحد المعنيين، فترتفع العقوبة لتصبح السجن من عشر(10) سنوات إلى عشرين (20) سنة وغرامة مالية من 500.000 دج إلى 1.000.000 دج وذلك دون الإخلال، عند الاقتضاء، بتطبيق الأحكام العامة الخاصة بالجرائم المنصوص عليها في الباب الثاني من الكتاب الثالث من ق .ع.[2]

**الفرع الثاني:اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور**

اعتمد المشرع الجزائري على وسائل حديثة للكشف عن الجرائم الإلكترونية، مثل اعتراض المراسلات وتسجيل الأصوات والتقاط الصور باعتبارها من أبرز الأساليب المستحدثة لمواجهة هذا النوع من الجرائم التي غالبا ما ترتكب في الخفاء، وقد جاء هذا التوجه انسجاما مع التطور التكنولوجي الهائل، لاسيما في ميدان الاتصالات الرقمية، مما أتاح ظهور تقنيات عملية فعالة ساهمت بشكل كبير

[1] – وردة شرف الدين، المرجع السابق، ص 547.

[2] – إجراءات التسرب: قانون رقم 06-22، المؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66- 155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ص ص 9، 10.

في تطوير أساليب التحري. وفي هذا الإطار سنتناول هذه الإجراءات بشكل مفصل باعتبار كل منها إجراء قائما بذاته.[1]

## أولا: اعتراض المراسلات السلكية واللاسلكية

### 1. تعريفها:

بالاعتماد على نص المادة 65 مكرر 5 من ق.إ.ج يتضح أن المشرع الجزائري يقصد بها كل العمليات المتعلقة باعتراض أو تسجيل أو نسخ المراسلات التي تجري عبر وسائل الاتصال السلكية أو اللاسلكية وتشمل هذه المراسلات البيانات القابلة للإنتاج، التوزيع، التخزين، الاستقبال أو العرض، غير أن المراسلات الإلكترونية تم استثناؤها من هذا الإطار نظرا لإمكانية حدوثها خارج نطاق الشبكات السلكية واللاسلكية، وقد خصص لها تنظيم قانوني مستقل بموجب القانون رقم 04-09 المتعلق ب بمراقبة الاتصالات الإلكترونية.

وهذا يشير بوضوح إلى أن المراسلات المعنية في هذا السياق تتعلق في المقام الأول بالاتصالات الهاتفية، سواء الثابتة أو النقالة. لكن ومع التحول الرقمي الواسع الذي يشمل مختلف وسائل الاتصال والإعلام، أصبح من الصعب التمييز بدقة بين الوسائل الرقمية وغيرها، مما دفع بالمشرع إلى توحيد التعامل مع مختلف أشكال الاتصالات تحت إطار قانوني واحد كما نصت عليه المادة 5 من المرسوم التنفيذي رقم 15- 161.[2]

بالرغم من أن المراسلات تتمتع بخصوصية حظيت بحماية قانونية من خلال نصوص تشريعية توفر لها قدرا كبيرا من الحماية الجزائية، إلا أن هذه الحماية ليست مطلقة، فقد اجاز المشرع في بعض الحالات، مثل حالات التلبس بالجريمة أو أثناء التحقيق الابتدائي في الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات، اعترض هذه المراسلات وكشف سيرتها إذا ادعت الضرورة لذلك ضمن نطاق التحقيق، يشكل هذا الإجراء مبررا قانونيا استثنائيا يتيح السماح به رغم كونه يعد انتهاكا واضحا لحرمة الحياة

[1] – بومدين كعبيش، أساليب التحري الخاصة في جرائم الفساد، العدد 07، مجلة القانون، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ديسمبر 2016، ص 304.

[2] – عبد الرؤوف بوديسة بجاد، المرجع السابق، ص 62.

الخاصة وسرية المراسلات، لذلك لا يسمح به إلا في حالات ضيقة واستثنائية عندما تقتضي الضرورة ذلك وبهدف تحقيق مصلحة جوهرية تتمثل في كشف لحقيقة وتوضيح ملابسات الجريمة والوصول إلى الجناة.[1]

تظهر عمليات اعتراض المراسلات بشكل واضح في مجال المراسلات الإلكترونية، وبشكل خاص في البريد الإلكتروني المرتبطة بخدمة قوائم التراسل(Mailinglist) وهي عبارة عن نظام يتيح إرسال رسالة واحدة إلى مجموعة من الأشخاص المسجلين ضمن القائمة، ويتميز البريد الإلكتروني باحتوائه على برامج متخصصة تستخدم في كتابة الرسائل، إرسالها، عرضها وتخزينها.[2]

## 2. الشروط والضمانات المقررة لاعتراض المراسلات:

تخضع عملية اعتراض المراسلات إلى مجموعة من الشروط والضمانات هي:

### ❖ ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ:

لا يجوز لضباط الشرطة القضائية الشروع في اعتراض المراسلات إلا بعد الحصول على إذن كتابي ومعلل من وكيل الجمهورية أو من قاضي التحقيق إذا كان هناك تحقيق قضائي مفتوح. وهذا ما تنص عليه المادة 65 مكرر 5 من ق.إ.ج، مما يؤكد أن السلطة القضائية وحدها هي المخولة بمنح هذا الإذن وهو ما يعد ضمانة أساسية لشرعية الإجراء.

### ❖ تحديد نوع المراسلة وفترة الاعتراض:

وفقا للمادة 65 مكرر 7، يجب أن يتضمن الإذن جميع التفاصيل التي تمكن من تحديد طبيعة الاتصالات أو المراسلات المراد اعتراضها، كما أن مدة الاعتراض لا يجب أن تتجاوز أربعة أشهر مع إمكانية تمديدها بناء على تقدير نفس الجهة القضائية التي أصدت الإذن، ووفقا لمتطلبات سير التحقيق.[3]

---

[1] – محمد أو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، دار لنهضة العربية، 2008، ص 192.

[2] – عبد الحليم بن بادة، إجراءات البحث والتحري عن الجريمة المعلوماتية، العدد 23، المجلد 2، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، 2015، ص 86.

[3] – عبد الرؤوف بوديسة بجاد، المرجع السابق، ص 63.

**ثانيا: تسجيل الأصوات:**

لقد أسم التطور العلمي في ظهور العديد من الوسائل الحديثة التي تساهم في كشف الجرائم وإظهار الحقيقة.من بين هذه الوسائل، برزت أجهزة التسجيل الصوتي التي تطورت بشكل كبير لتصبح سهلة الحمل والاستخدام وقادرة على التقاط الأحاديث التي تدور في الأماكن المغلفة دون علم الحاضرين، وكثيرا ما يتفوه المشتبه بهم بعبارات تدل على تورطهم في جريمة أو يخططون لجريمة مستقبلية ولأن الأقوال قد تكون دليلا قضائيا هاما، أجاز المشرع الجزائري استخدام هذا التطور العلمي، ووضع إجراءات خاصة لتسجيل ما يقال، سواء كان ذلك حديثا لشخص واحد أو بين شخصين أو أكثر، وفي الأماكن العامة أو الخاصة وذلك لخدمة العدالة، لقد ازدادت قدرة وكفاءة وتفوق أجهزة التسجيل الصوتي يوما بعد يوم، سواء من حيث جودة التسجيل أو صغر حجمها وسهولة استخدامها، وتعددت أنواعها لدرجة أصبح من الصعب متابعة أحدث تطوراتها.

**1. تعريفها:**

تسجيل الأصوات المقصود به تسجيل أحاديث المتهم وشركائه عن واقعة معينة من الوقائع المنصوص عليها في المادة (65 مكرر 5 من ق.إ.ج.ج) خلسة.[1]

المشرع الجزائري لم ينص في ق.إ.ج.ج. على تعريف التسجيل الصوتي مثل ما لم ينص على تعريف عملية اعتراض المراسلات، إنما أشار لها بنص المادة 65 مكرر في ف 2 "وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية ".[2]

فالمهم في العملية هو الكلام المتفوه به، الذي قد يشكل دليلا لإظهار الحقيقة، بغض النظر عن مكان التسجيل الذي قد يكون عاما كالشارع أو خاصا كالمسكن والأداة التي يتم بها.

[1] – ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، ط 1، دار المطبوعات الجامعية، جامعة القاهرة، 2009، ص 165.

[2] – حسنين المحمدي البوادي، الوسائل الحديثة في الإثبات الجزائري، د ط، الإسكندرية، 2005، ص 67.

وتعتمد عملية التسجيل الصوتي على وضع الرقابة على المكالمات الهاتفية ونقل الأحاديث وتسجيلها ويتم عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، كما يتم عن طريق التقاط الإشارات اللاسلكية، إلا أن هذه الترتيبات التقنية لا تكون إلا بإذن من وكيل الجمهورية أو قاضي التحقيق حسب الحالة وتحت مراقبته وإشرافه.

فالتسجيل الصوتي الذي يهمنا هو التسجيل الذي يجريه رجال الشرطة القضائية للاستعانة به في مجال الإثبات الجنائي وعليه فإن التسجيلات التي يقوم بها الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجنائية نظرا لأنها لم تصدر في شأن دعوى جنائية حركتها السلطات القضائية بقصد الحصول على الحقيقة، كما لا يوجد بعين الاعتبار تسجيل الأحاديث التي تتضمن اعتداء على حق من يتم تسجيل حديثه كما في حالة تسجيل الاحاديث التلفزيونية أو الإذاعية أو الصحفية متى تم ذلك بموافقة المعني.[1]

## 2. إجراءات التسجيل الصوتي:

التسجيل الصوتي ليصبح دليل إدانة يعتمد عليه القاضي يجب أن يكون واضحا على النحو التالي:

### أ. التأكد من أن الصوت يخص المتهم:

نظرا لسهولة التلاعب بالتسجيلات الصوتية عبر عمليات "المونتاج"، أي إدخال تغيرات، تعديلات أو نقل أجزاء الحديث من موضع إلى موضع آخر، فإن مسألة تحديد هوية صاحب الصوت تصبح بالغة الأهمية فقبول الدليل من عدمه يتوقف عليها.لهذا من الضروري أن يستعين قاضي التحقيق بخبير مختص في الأصوات ورأي الخبير يكون استشاريا، بما يتماشى مع القواعد العامة للإجراءات الجزائية، هذا الإجراء في بعض الأحيان يكون من الصعب فيه التمييز بين الأصوات المتشابهة أو عندما تختلط الأصوات المسجلة بالضوضاء المحيطة بمكان التسجيل.[2]

### ب. تفريغ وتخزين التسجيلات:

[1] – مختار خداوي، إجراء البحث والتحري الخاصة في التشريع الجزائري، مذكرة التخرج لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، جامعة د الطاهر مولاي سعيدة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2015- 2016، ص ص 33، 34.

[2] – ياسر الأمير فاروق، المرجع السابق، ص 155.

بالرغم من أن المشرع الجزائري لم ينص صراحة على وجوب وضع التسجيلات الصوتية أو مقاطع الفيديو في أحراز مختومة عند اعتراض المراسلات وتسجيل الأصوات أو التقاط الصور إلا أن الاستناد إلى مواد أخرى من ق.إ.ج.ج يوضح ضرورة ذلك فالمادة 18 من ق.إ.ج.ج يشير إلى وجوب موفاة وكيل الجمهورية بالأشياء المضبوطة والمادة 45 من نفس القانون تنص على ضرورة إغلاق الأشياء المضبوطة وختمها إن أمكن.

بما أن الأشرطة المسجلة تعد أدلة إثبات مادية أصلية، فإن الشرعية الإجرائية تقتضي حفظها بطريقة خاصة يتم ذلك بوضعها في أحراز مختومة لضمان عدم العبث بالمحادثات المسجلة سواء بالحذف أو الإضافة، كما يجب ضم هذه الأحراز إلى ملف الإجراءات القضائية، مرفقة بالمحاضر التي تصف محتواها أو تنسخه وذلك بهدف الكشف عن الحقيقة دون أي شبهة تلاعب.[1]

**ثالثا: التقاط الصور**

**1. تعريفها:**

بشكل عام يمنع منعا باتا التقاط صور لأي شخص أو تقليدها أو نشرها دون موافقته. يعد هذا انتهاكا لخصوصية الفرد وخرقا لحقوق الإنسان التي تحميها المواثيق الدولية والدساتير الوطنية على سبيل المثال، ينص الدستور الجزائري 39 على أنه "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون"[2] مع ذلك وضع المشرع الجزائري استنادا لهذا المبدأ بهدف مكافحة جرائم الفساد وحماية المصلحة العامة.

كما أجاز القضاء استخدام الصور كأداة لتحديد هوية المشتبه بهم. هذا يدل على أن القضاء الجنائي لم يستبعد استخدام هذه الوسيلة في الإثبات الجنائي، تصبح حجية الصورة الفوتوغرافية مقبولة قانونيا في حالات التلبس، حيث يقوم ضابط الشرطة القضائية بإثباتها خلال جميع مراحل البحث والتحري، يشمل ذلك على سبيل المثال تصوير أفراد العصابة، موقع الجريمة، وعمليات استلام وتسليم الأشياء أو الوسائل المستخدمة في الجرائم، وغيرها من الأدلة الجنائية.

[1] – مختار خداوي، المرجع السابق، ص ص 35،36.

[2] – أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية ، ط 1، دار الهومة، الجزائر، 2005، ص 231.

لم يعرف المشرع الجزائري "عملية التقاط الصور" بشكل صريح، بل اكتفى بالإشارة إليها بكلمة "الالتقاط"ومع ذلك عرفها البعض بأنها تمثيل شخص أو شيء باستخدام فنون مختلفة مثل النقش، النحت، التصوير الفوتوغرافي، أو الأفلام. ولم يقتصر دور الصورة على تجسيد الدور المادي للشخص بل امتد إلى ليشمل إظهار شخصيته وانفعالاته.[1]

نظرا لأن المجرمين لا يترددون في استخدام أحد الأساليب العلمية لارتكاب جرائمهم، أصبح من الضروري استغلال التطور العملي والتكنولوجي في مكافحة الجريمة. لقد تطورت تقنيات التصوير بشكل مستمر، مما أدى إلى إنتاج أجهزة تصوير أكثر كفاءة، وزيادة قدرة العدسات التلسكوبية وتحسين أجهزة تصوير الأفلام.

ومن بين الأجهزة المستخدمة في هذا الإجراء نجد: وسائل الرؤية والمشاهدة القادرة على التصوير من مسافات بعيدة، وأجهزة التصوير بالأشعة تحت الحمراء التي تتيح التصوير في الظلام الدامس، المرايا ذات الازدواج المرئي التي تسمح بالتصوير داخل الأماكن المغلقة من خلال زجاج شفاف من جهة، بينما ويبدو كالمرآة من جهة أخر، عدسات التصوير التي الدقيقة التي يسهل وضعها في زوايا الغرف، أ, داخل مفاتيح الإنارة، أو في أي أماكن يصعب اكتشافها.

## 2. شروط التقاط الصور:

لكي يكون التقاط الصور مشروعا ومتوافقا مع الإجراءات القانونية، يجب أن توفر شروط موضوعية وشكلية هذه الشروط لا تقتصر على التقاط الصور فحسب بل، بل تنطبق أيضا على اعتراض المراسلات وتسجيل الأصوات وهي كالتالي:[2]

### أ. الشروط الموضوعية:

[1] – رشيد شميشم، الحق في الصورة، العدد 03، العدد 01، مجلة العلوم الإنسانية والاجتماعية، جامعة المدية، 2008، ص 127.

[2] – مختار خداوي، المرجع السابق، ص 37.

- **السلطة المختصة بالإجراء:**

يشرف على هذه العمليات وكيل الجمهورية أو قاضي التحقيق، ورغم أنهم لا يقومون بالإجراء بأنفسهم، إلا أنه يتم تحت إشرافهم ومراقبتهم المباشرة.

- **وقت ومكان الإجراء:**

لم يضع المشرع الجزائري قيودا زمنية أو مكانية على هذه الإجراءات فهي مسموحة في أي وقت (ليلا أو نهارا) وفي أي مكان (عام أو خاص) باستثناء السفارات والقنصليات الأجنبية التي لا تخضع لهذه العمليات.

- **عدم مسؤولية القائمين والمشرفين على الإجراء:**

عادة ما تعتبر أفعال مثل الاعتداء على الحياة الخاصة بالتقاط الصور، تسجيل الأصوات، دخول المنازل دون إذن، تسلق الجدران ليلا وفتح الأقفال كلها جرائم، ومع ذلك لا تعتبر هذه الأفعال مجرمة إذا تمت في إطار إجراءات البحث والتحري الخاصة وبإذن من وكيل الجمهورية أو قاضي التحقيق.

- **ضرورة اللجوء إليها:**

يجب أن تكون هناك ضرورة ماسة تستدعي اللجوء إلى هذه الإجراءات بالإضافة إلى ذلك، يجب أن تكون الجريمة المرتكبة من ضمن الجرائم السبع المذكورة في المادة 6 مكرر 6 من ق.إ.ج.ج وأن تكون هناك دلائل قوية تربط المتهم بالجريمة.

**ب. الشروط الشكلية:**

- **الإذن المسبق من السلطة القضائية:**

تنص المادة 6 مكرر 6 من ق.إ.ج.ج على أنه في حال وقوع إحدى الجرائم المنصوص عليها في نفس المادة، يسمح لوكيل الجمهورية أو قاضي التحقيق بمنح إذن مسبق لالتقاط الصور، هذا يعني أن البدء بهذه العمليات يتطلب ترخيصا قضائيا مسبقا قبل الشروع فيها.

- **ضرورة أن يكون الإذن كتابي:**

يتطلب القانون أن يكون الإذن الصادر من وكيل الجمهورية أو قاضي التحقيق مكتوبا، يسلم هذا الإذن إلى ضابط الشرطة القضائية المسؤول الأول عن تنفيذ العمليات، ويمنحه الحق في الاستعانة بالخبراء عند الحاجة.

- **محاضر العمليات:**

يجب على ضابط الشرطة القضائية تحرير محضر لكل مرحلة من مراحل العمليات على حدى، وإرساله إلى قاضي التحقيق بشكل مفصل دون انتظار اكتمال عملية المرحلة الأخيرة، ويجب أن يتضمن كل محضر:

- تاريخ وساعة بداية ونهاية العملية.
- وصفا أو نسخة من المراسلات، الصور، والمحادثات.
- إذا كانت المكالمات أو المحادثات بلغة اجنبية، يجب أن ترفق ترجمة لها من قبل مترجم ينم تسخيره خصيصا لهذا الغرض.[1]

**خلاصة الفصل الثاني:**

تم في هذا الفصل التطرق إلى مختلف الأجهزة المكلفة بمكافحة الجريمة المعلوماتية، وعلى رأسها الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، بالإضافة إلى الأجهزة الأمنية ممثلة في الشرطة) الأمن الوطني (والدرك الوطني، وذلك على مختلف مستويات تدخلها سواء الوطنية أو الجهوية أو المحلية .وتكمن أهمية هذه الجهات في دورها المباشر في التصدي للجرائم الإلكترونية، من خلال التنسيق فيما بينها وتوظيف الوسائل المتاحة لضمان فعالية الاستجابة.

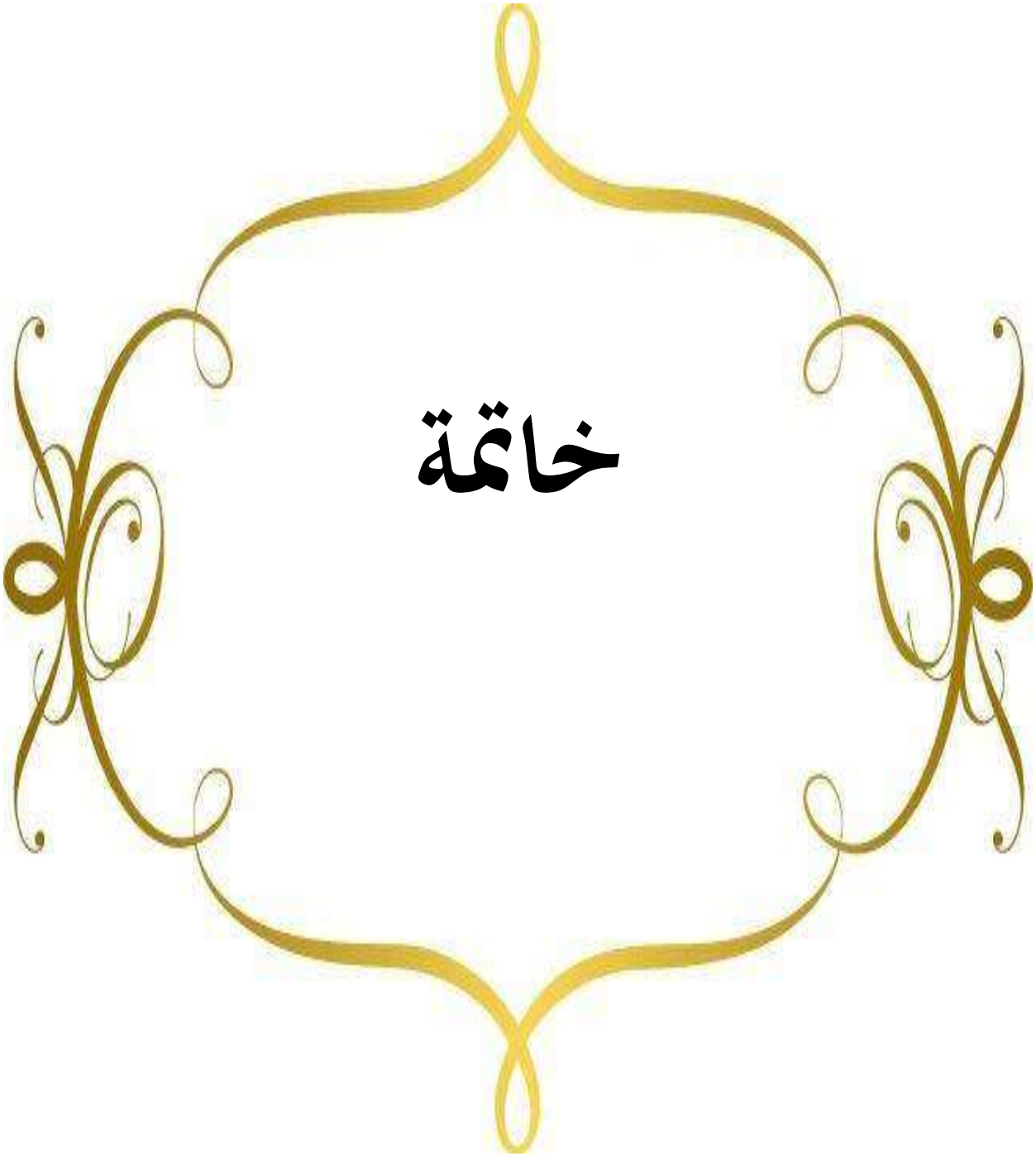
[1] – مختار خداوي، المرجع السابق، ص ص 38،39.

كما تناول الفصل الإجراءات القانونية الخاصة بالتحري، والتي تهدف إلى تمكين الجهات المختصة من الكشف عن مرتكبي الجرائم المعلوماتية وتوقيفهم ثم إحالتهم إلى النيابة العامة لاتخاذ الإجراءات القضائية المناسبة في حقهم.

وتجدر الإشارة إلى أن هذه الإجراءات تنقسم إلى نوعين:

- ❖ إجراءات تحري كلاسيكية، وهي تلك المعتمدة في الجرائم التقليدية، مثل استجواب الشهود، التفتيش، المراقبة الميدانية، وضبط الأدلة المادية.
- ❖ إجراءات تحري مستحدثة، فرضتها طبيعة الجريمة المعلوماتية، وتشمل تحليل الأدلة الرقمية، تتبع العناوين الإلكترونية (IP)، مراقبة الأنشطة عبر الإنترنت، واسترجاع البيانات المحذوفة، وذلك غالبًا باستخدام أدوات وتقنيات متطورة، وفي بعض الحالات بالتنسيق مع جهات دولية.

تُظهر هذه الإجراءات، سواء الكلاسيكية أو المستحدثة، أهمية التكيف مع طبيعة الجريمة المعلوماتية الحديثة لضمان فعالية التحقيق والوصول إلى الجناة.



# خاتمة

**خاتمة :**

نحن نعيش اليوم في عصر يشهد تطورًا تكنولوجيًا هائلًا، خاصة مع ما يسمى بالثورة المعلوماتية، حيث أصبحت حياتنا اليومية تعتمد بشكل كبير على هذه التكنولوجيا. ولكن، ورغم الفوائد الكبيرة، فإن هذا التقدم التكنولوجي أفرز تحديات جديدة، أبرزها ظهور ما يعرف بـ"الجريمة المعلوماتية"، الناتجة عن الاستخدام الخاطئ أو الإجرامي للتكنولوجيا والحاسوب.

تتميز هذه الجريمة بأنها لا ترتبط بمكان أو زمان معين، فهي عابرة للحدود، وتؤثر على الأفراد والمؤسسات في كل مكان، وقد تضر بالأمن والخصوصية. كما أن تعريفها القانوني ليس واضحًا تمامًا، بسبب تباين الآراء حول طبيعتها والوسائل التي تُرتكب بها، مما يخلق صعوبة في تحديد مفهوم موحد لها.

هناك من يرى أن الجريمة المعلوماتية مجرد وسيلة جديدة لارتكاب الجرائم التقليدية، بينما يرى آخرون أنها نوع جديد من الجرائم تمامًا. وما يزيد الأمر تعقيدًا هو أن طبيعتها الرقمية تجعل من السهل إخفاء آثارها، ويصعب ملاحقة مرتكبيها أو تحديدهم بدقة.

وتكمن خطورة هذه الجرائم في أنها لا تعتمد على العنف الظاهري كما في الجرائم التقليدية، بل تنفذ بطرق معقدة وذكية يصعب اكتشافها. وقد تكون أضرارها مادية أو معنوية، أو حتى الاثنين معًا.

من جانب آخر، تتطلب هذه الجرائم أساليب خاصة في مكافحتها، وهو ما دعى غالبية التشريعات إلى ضرورة تطوير القوانين الإجرائية لتتماشى مع البيئة الرقمية. مثال ذلك القانون 04/06 الذي أقر قواعد خاصة للتعامل مع الجرائم المعلوماتية.

لكن، هناك إشكاليات أخرى تتعلق بتحقيق التوازن بين احترام الخصوصية وفعالية التحقيق، إلى جانب صعوبة الوصول إلى أدلة رقمية دون انتهاك حقوق الأفراد. كما أن تحقيقات الجرائم المعلوماتية تتطلب كفاءات فنية متخصصة وأدوات تقنية دقيقة، قد لا تكون متوفرة دائمًا.

## النتائج

من خلال دراسة موضوع الجريمة المعلوماتية في ظل التشريع الجزائري، توصلنا إلى جملة من النتائج المهمة التي تُبرز مدى تعقيد هذا النوع من الجرائم وحدود الاستجابة التشريعية لها، وتتمثل أبرز هذه النتائج فيما يلي:

1. تصنيف الجريمة المعلوماتية كجريمة مستحدثة :تُعد الجريمة المعلوماتية من الجرائم المستحدثة التي لم تكن مألوفة في السابق، وقد فرضتها الثورة التكنولوجية وتطور وسائل الاتصال والمعلومات.
2. قصور التشريع الجزائري في مواكبة التطورات التقنية :رغم الجهود المبذولة من قبل الدولة، لا يزال هناك نقص واضح في الإطار القانوني المتعلق بمكافحة الجريمة المعلوماتية، حيث أن التشريعات المعمول بها تُعد تقليدية ولا تواكب السرعة الكبيرة في تطور الوسائل الإجرامية الإلكترونية.
3. صعوبة إثبات الجريمة المعلوماتية :يتسم هذا النوع من الجرائم بصعوبة الكشف عنه وضبط مرتكبيه، نظراً لاستخدامهم وسائل رقمية متطورة تُمكّنهم من إخفاء هويتهم وتتبع آثارهم، إضافة إلى غياب الأدلة التقليدية التي تعتمد عليها الأجهزة الأمنية والقضائية.
4. عدم كفاية التعديلات القانونية الحالية :التعديلات التي أُدخلت على قانون العقوبات، خاصة بموجب القانون04/09 ، غير كافية للحد من هذه الجرائم، إذ لم تضع منظومة قانونية شاملة، بل اكتفت بإضافة بعض النصوص الجزئية دون إطار شامل.
5. الطبيعة العابرة للحدود للجريمة المعلوماتية :هذه الجرائم لا تقتصر على إقليم الدولة بل تمتد إلى خارج حدودها، مما يزيد من تعقيد مكافحتها ويُبرز الحاجة إلى تعزيز التعاون الدولي والإقليمي لمواجهتها بفعالية.
6. نقص التخصص في مكافحة الجرائم المعلوماتية :تعاني الجهات الأمنية والقضائية من قلة الخبرات المتخصصة في مجال تكنولوجيا المعلومات، وهو ما يؤثر سلباً على فعالية ملاحقة مرتكبي الجرائم الإلكترونية والتحقيق فيها.

7. ضعف التوعية المجتمعية :هناك ضعف واضح في حملات التوعية التي تستهدف المواطنين من أجل تحذيرهم من خطورة الجريمة المعلوماتية وطرق الوقاية منها، وهو ما يساهم في ارتفاع نسبة الضحايا، لاسيما من الفئات الأكثر استخداماً للإنترنت.

**الاقتراحات:**

نقترح من وجهة نظرنا أنه على المشرع استحداث تعريف قانوني خاص لهذا النوع المستجد من الجرائم، نظرا لإزدياه وخطورته، الأمر الذي يستوجب إضفاء تعريف يبين نوعية الجريمة لعدم الوقوع في الخطأ خاصة من ناحية التكييف.

1. على المشرع أن يقوم بتطوير بنيته التشريعية تماشيا مع التطور السريع والملحوظ لهذه الجريمة.
2. إنشاء أقسام متخصصة بالجرائم المعلوماتية.
3. ضرورة تخصيص شرطة جنائية خاصة وخبراء من ذوي الكفاءة العالية في مجال الانترنت.
4. حبذا لو سار المشرع توفير الوسائل و الأجهزة المسخرة والمتنوعة لقمع الجريمة من جهة مغايرة.
5. إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية، خاصة فيما يتعلق بحقوق الملكية الفكرية و الحقوق المجاورة لم تعد قابلة للتطبيق في بيئة رقمية .
6. ضرورة خلق ثقافة اجتماعية جديدة تندد بجرائم الانترنت مع تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية على استخدام الأمثل لهذه التقنيات .
7. ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الإحتياطات الوقائية اللازمة.
8. تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة المعلوماتية والحد من آثارها .
9. من الضروري تفعيل دور أجهزة الوقاية من الجرائم المعلوماتية على أرض الواقع من الضروري تبني إجراء مراقبة الاتصالات الإلكترونية كإجراء للتحقيق القضائي.

مما سبق ذكره أن هذه الجريمة عابرة للحدود وصعبة الثبات، لذلك أقترح أن تكون دراسات في المستقبل، تتضمن نظرة المشرع الجزائري لهذه الجريمة المعلوماتية مقارنة بتشريعات الدول العربية أو بتشريعات الدول الغربية، ومدى الجهود الدولية المبذولة لمكافحة هذه الجريمة.

أرجوا أن أكون قد وقفت في معالجة هذا الموضوع، وإن لم أوفق فإنني اجتهدت ولكل مجتهد نصيب.

# قائمة المصادر

# والمراجع

## قائمة المصادر والمراجع

### I. المصادر

**أولا: القوانين:**


1. القانون رقم 97-10، المؤرخ في 06 مارس 1997، المتعلق بالأرشيف، ج.ر.ج.ج، العدد 15، الصادرة بتاريخ 1 مارس 1997.
2. القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الامر رقم 66-166 المؤرخ في 08 يونيو 1966، المتضمن أحكام المساس بأنظمة المعالجة الآلية للمعطيات، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.
3. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر 66- 155 المؤرخ في 8 يونيو سنة 1966، والمتضمن قانون الإجراءات الجزائية، المعدل و المتمم إلى غاية الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، ج ر ج ج العدد 65 المؤرخة في 26 غشت سنة 2021.
4. قانون رقم 06-23 مؤرخ في 20 ديسمبر 2006، يتعلق بتنظيم أنظمة المعالجة الآلية للمعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 7، الصادرة بتاريخ 20 ديسمبر 2006.
5. القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، يتضمن قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 أغسطس 2009.
6. القانون 18-07 المؤرخ في 10 يوليو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد، 34، الصادرة في 10 يوليو 2018.

7. القانون رقم 24- 06 المؤرخ في 19 شوال عام 1445 هـ الموافق لـ 28 أفريل سنة 2024 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386هـ الموافق لـ 8 يونيو سنة 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 30 المؤرخة في 21 شوال عام 1445 هـ الموافق لـ 30 أفريل سنة 2024.

**ثانيا: الأوامر**

1. الأمر رقم 03-05، المؤرخ في 19 جمادى الأولى عام 1424، الموافق لـ 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية، العدد 44، المؤرخة في 2003/07/19.
2. الأمر 03-07، مؤرخ في 19 جمادى الأولى عام 1424، الموافق لـ 19 يوليو 2003، المتعلق ببراءات الاختراع، الجريدة الرسمية للجمهورية الجزائرية، العدد 44، المؤرخة في 2003/07/19.

**ثالثا: المراسيم**

1. المرسوم الرئاسي 04- 183 المؤرخ في 26 يونيو 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، الجريدة الرسمية للجمهورية الجزائرية، العدد 41، الصادرة بتاريخ 27 يونيو 2004.
2. المرسوم الرئاسي 15-261 المؤرخ في 2015/10/08 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 53، المؤرخة في 24 ذي الحجة 1436 هـ، الموافق لـ 08 اكتوبر 2015.

## II.المراجع

**أولا: الكتب:**


1. الأمير فاروق ياسر، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، ط 1، دار المطبوعات الجامعية، جامعة القاهرة، 2009.
2. بن قارة مصطفى عائشة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة لجديدة، كلية الحقوق جامعة الإسكندرية، 2006.
3. بيومي حجازي عبد الفتاح، الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتية، ط1، دار لفكر الجامعي، الإسكندرية، 2008.
4. حياد الحلبي خالد، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2011.
5. ربيحة زيدان، الجريمة المعلوماتية في التشريع المدرسي والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة- الجزائر-2011.
6. عطاالله محمد عبد الغني شيماء، الحماية الجنائية للتعاملات الإلكترونية، د.ط، دار الجامعة الجديدة، الإسكندرية، 2007.
7. عقيدة محمد أو العلاء، مراقبة المحادثات التلفونية، دراسة مقارنة، دار لنهضة العربية، 2008.
8. قارة أمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة للطباعة النشر والتوزيع، الجزائر، 2007، ص ص 107 110.
9. قهوجي علي عبد القادر ، الحماية الجنائية لبرامج الحاسب الآلي، طبعة أولى، الدار الجامعية، بيروت، 1999.
10. ممدوح إبراهيم خالد، أمن الجريمة الإلكترونية،د.ط، الدار الجامعية، الإسكندرية، 2008.

11. ممدوح إبراهيم خالد، فن التحقيق الجنائي في الجرائم الإلكترونية، ط 1، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص ص 156، 157.

12. المولدي المهدي حسين، الوسائل الحديثة في الإثبات الجزائري، د ط، الإسكندرية، 2005.

**ثانيا: المقالات**

1. بخوش هشام، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل التشريع الجزائري، جامعة خنشلة، العدد 07، جانفي 2017.

2. بن بادة عبد الحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية، العدد 23، المجلد 2، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، 2015.

3. جابت أمال، الجريمة المعلوماتية في التشريع الجزائري بين قانوني 09-04 و 04-15، العدد 25، المجلد 7، مجلة هيرودة للعلوم الإنسانية والاجتماعية، مؤسسة هيرودوت للبحث العلمي والتكوين، الجزائر، ، 2023.

4. جدي صبرينة، الإطار القانوني لمعالجة المعطيات ذات الطابع الشخصي في التشريع الجزائري على ضوء قانون رقم 18-07، المجلة الشاملة للحقوق، مجلد 2، عدد 3، جامعة باجي مختار عنابة- الجزائر، سبتمبر 2022.

5. رابح سعاد، ضوابط مكافحة الجريمة المعلوماتية، المجلد 07، ع 01، مجلة القانون العام الجزائري والمقارن، جوان 2021، ص 281.

6. شرف الدين وردة، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية، العدد 15، مجلة الفكر، جامعة محمد خيضر بسكرة، الجزائر، 15 جوان 2017.

7. شيخ سناء ومحمد زكرياء، مكافحة الجرائم الإلكترونية في القانون الجزائري، مجلة وميض الفكر للبحوث، العدد 05، سبتمبر 2020.

**8.** طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل القانون 18-07 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، العدد 2، المجلة الأكاديمية للبحث القانون، 2018.

**9.** عمارة فتيحة، الحماية الجنائية للمعلومات الإلكترونية في إطار قانون الملكية الفكرية، العدد 31، مجلة الحياة، الجزائر، 2014.

**10.** عمراني أحمد، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في التشريع الجزائري والمقارن، ع 16، مجلة الحضارة الإسلامية، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، جمادى الثانية 1433 هـ/ ماي 2012 م.

**11.** العيداني محمد وزروق يوسف، حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07، مجلة معالم الدراسات القانونية والسياسية، العدد 05، مجلة معالم الدراسات القانونية والسياسية، مجلة فصلية دولية علمية محكمة تصدر عن المركز الجامعي علي كافي –تندوف- الجزائر، ديسمبر 2018.

**12.** فلاح عبد القادر، نادية آيت عبد الله، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، العدد 2، المجلد 04، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، 2019.

**13.** كعيبش بومدين، أساليب التحري الخاصة في جرائم الفساد، العدد 07، مجلة القانون، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ديسمبر 2016.

**14.** ميساد أمينة، آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون(18-07)، مجلة الباحث في العلوم القانونية والسياسية، العدد 05، جامعة محمد الشريف مساعدية، سوق أهراس، 2021.

**ثالثا:المذكرات الأكاديمية**


1. إبراهيم زياد بوعرعارة، خصوصية الجريمة المعلوماتية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق، تخصص قانون جنائي، جامعة غرداية، كلية الحقوق والعلوم السياسية، قسم الحقوق 1442 هـ- 1443 هـ /2021-2022، ص 88.
2. أحمد عبد العزيز، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، جامعة الدكتور الطاهر مولاي سعيدة، كلية الحقوق والعلوم السياسة، قسم الحقوق، 2021-2022 م الموافق لـ 1442-1443 هـ.
3. البركة الطيبي، الجماية الجنائية لنظام المعالجة الآلية للمعطيات- دراسة مقارنة-، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة دكتوراه الطور الثالث، تخصص قانون جنائي، جامعة أحمد دراية -أدرار-، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020- 2021.
4. بن زرت آسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر، القانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2019.
5. بن موسى خديجة، الحماية الجنائية للمعطيات في المجال المعلوماتي، مذكرة لنيل شهادة الماستر أكاديمي حقوق، قانون جناني، حقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 1442 هـ/1444 هـ، 2022/2021.
6. بوادي حميدة وبن سالم فطيمة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مذكرة لنيل شهادة الماستر، تخصص إعلام آلي وانترنت، كلية الحقوق والعلوم السياسية، جامعة البشير الإبراهيمي، برج بوعريريج، 2022-2023.
7. بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزاري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر في مهني في الحقوق، تخصص قانون الإعلام

الآلي والانترنت، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحقوق والعلوم السياسية، 2022/2021.

8. حشمان عمار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، تخصص إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح، ورقلة، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم علوم التسيير، 2019.

9. خداوي مختار، إجراء البحث والتحري الخاصة في التشريع الجزائري، مذكرة التخرج لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، جامعة د الطاهر مولاي سعيدة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2015- 2016.

10. الدزيري هيبة، جريمة الدخول الغير مشروع لنظام المعالجة الآلية للمعطيات، مذكرة نهاية الدراسة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2019-2020.

11. ربيعي حسين، آليات التحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في الحقوق، تخصص قانون العقوبات العلوم الجنائية، جامعة باتنة 1، السنة الجامعية 2015-2016.

12. زهية معمش، نسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمن ميرة – بجاية- كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2012-2013.

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

14. شنبر خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة أحمد دراية أدرار، 2021/2020.

15. عاصف أسماء، الجرائم الرقمية وطرق إثباتها، مذكرة نهاية الدراسة لنيل شهادة الماستر، تخصص قانون قضائي، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم قانون خاص، 2024.

16. العاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، جامعة أكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014-2015.

17. عوادي فاطمة الزهراء، الحماية الجزائية للبيانات الشخصية المعالجة آليا، مذكرة لنيل شهادة الماستر، قسم الحقوق، ، كلية الحقوق والعلوم السياسية، جامعة سعيدة، 2020/2019.

18. نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، جامعة أحمد دراية – أدرار-كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016-2017م.

**رابعا: المواقع الإلكترونية**

1. الموقع الرسمي لقيادة الدرك الوطني:

http:www.mdn.dw/site/dz

## فهرس المحتويات

**ملخص:**

يتناول موضوع هذا البحث الجريمة المعلوماتية في التشريع الجزائري، بالنظر إلى التطور السريع في تكنولوجيا المعلومات والاتصال، الأمر الذي نجم عنه ظهور عدة جرائم جديدة ذات طبيعة إلكترونية معقدة تهدد الأمن العام والاقتصادي والاجتماعي للدولة .

يركز البحث على إبراز كيفية تعامل المشرع الجزائري مع هذه الجرائم من خلال استعراض النصوص القانونية خاصة قانون العقوبات بالإضافة الى قوانين أخرى متفرقة .

وتخلص الدراسة إلى أن الجريمة المعلوماتية تمثل تحديا حقيقيا يتطلب مواكبة تشريعية وتقنية، وتوصي بضرورة تحديث الإطار القانوني وتعزيز القدرات الفنية والبشرية للجهات المختصة .

**الكلمات المفتاحية:** الجريمة المعلوماتية، قانون العقوبات، الجهات المختصة لمكافحة الجريمة المعلوماتية، التشريع الجزائري.

**Abstract:**

The topic of this research deals with the information crime in Algerian legislation, given the rapid development of information and communication technology, which resulted in the emergence of several new crimes of a complex electronic nature that threatens the state, economic and social security of the state.

The research focuses on highlighting how the Algerian legislator deals with these crimes by reviewing the legal texts, especially the Penal Code, in addition to other separate laws.

-And the study concludes that the information crime represents a real challenge that requires legislative and technical abandonment. It recommends the necessity of updating the legal framework and enhancing the technical and human capabilities of the competent authorities.

**Keywords:**

Information crime, penal code, Algerian legislation, and the competent authorities to combat information crime.