جامعة أكلي محند أولحاج – البويرة
كلية الحقوق والعلوم السياسية
قسم القانون العام

# الحماية الجنائية للنظم المعلوماتية في التشريع الجزائري

مذكرة
لنيل شهادة الماستر في القانون العام
تخصص القانون الجنائي والعلوم الجنائية

إعداد الطالبين:

- حدو نور الدين
- ساسي مروان

تحت إشراف:

د. محمـودي محمد لمين

لجنة المناقشة:

د. غنيمي طارق ..... رئيسا

د. محمدودي محمد لمين ..... مشرفا

د. نبهي محمد..... ممتحنا

السنة الجامعية: 2026/2025


الحمد لله كما ينبغي لجلال وجهه وعظيم سلطانه حمدا كثيرا طيبا يوافي نعمه الذي وفقنا وأعاننا على إتمام هذا العمل بعد جهدٍ وصبرٍ ومثابرة.

نتقدم بجزيل الشكر وعظيم الامتنان إلى الأستاذ المشرف محمودي محمد لمين الذي لم يبخل علينا بتوجيهاته ونصائحه السديدة، فكان خير داعم ومرشد طوال فترة إنجاز هذه المذكرة.

كما نتوجه بخالص الشكر والتقدير إلى كافة أساتذة قسم القانون العام على ما قدموه لنا من علم ومعرفة طيلة مشوارنا الدراسي.

ونخص بالشكر كل من ساهم في مساعدتنا من قريب أو بعيد، وكل من مدّ لنا يد العون والدعم، وساهم بكلمة طيبة أو تشجيع كان له الأثر الجميل في نفوسنا.

وفي الأخير، نسأل الله أن يوفق الجميع لما فيه الخير والنجاح.

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

الحمد الله الذي بنعمته تتم الصالحات وبفضله تنزل الخيرات والصلاة والسلام على أشرف المرسلين، بعد رحلة بحث وصبر وبين طيات الورق والكتب حان أوان قطف ثمار النجاح الذي لا يكتمل الا بمن شاركونا الدرب اهدي ثمرة جهدي المتواضع

إلى من كلّله الله بالهيبة والوقار، إلى من كان كفاحه سبيلاً لنجاحي.. والدي العزيز.

إلى من جعل الله الجنة تحت قدميها، إلى نبع الحنان ومنبع الرضا.. أمي الغالية.

إلى زوجتي الكريمة وولدي محمد أمير، شكراً لكونكم السند والملجأ دائماً.

إلى كل هؤلاء، وإلى كل من دعا لي بظهر الغيب.. أهدي ثمرة جهدي وتخرجي.

نور الدين حدو


بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

إلى من كان دعاؤهما سر نجاحي ووجودهما أعظم نعمة في حياتي.. والديا

أطال الله في عمرهما ورزقهما وافر الصحة والعافية.

مروان ساسي

# مقدمـــــة

ان التحول التكنولوجي الذي شهده العالم في الآونة الأخيرة أحدث تحولا جذريا في كافة مجالات الحياة، بحيث امتد تأثيره الى جميع الدول من خلال تقليص المسافات بين الأشخاص والمؤسسات عن طريق توفير سرعة تداول المعلومات والبيانات في وقت قصير، وبجهد بسيط.

ومع تنامي استعمال التقنيات الرقمية الحديثية لما تحتويه من إيجابيات تعود بالمنفعة على الفرد والمجتمع، بدأت تتراءى عمليا مجموعة من السلبيات النابعة عن سوء استخدام التكنولوجيا والاستعمال غير المشروع لها، مما بات يشكل تهديدا حقيقيا على الافراد والمؤسسات وطنيا ودوليا.

ونتيجة لبزوغ هذا النوع من السلبيات المتمثل في الاجرام الالكتروني، أصبح لزاما التجند لمواجهته سواء بالوقاية منه أو مكافحته، ولا يتأتى ذلك الا بتشخيص المخاطر التي يشكلها بداية من الانتهاكات الخطيرة التي تطال الحياة الخاصة للأفراد وتصادر حرياتهم، أو التهديدات التي تواجهها الدول من خلال التعدي على سيادتها الوطنية واستقرارها الوطني بما فيها الجزائر.

ولحتمية تفرضها الظروف بادرت الجزائر بتعزيز ترسانتها القانونية لمواجهة هذه المخاطر، مع تدعيمها باليات تنظيمية وتقنية تمكنها من الوقاية عبر الاستباقية في وضع استراتيجيات تعيق تحقق الاضرار الناجمة عن الاجرام الالكتروني، إضافة الى تطوير الجانب الردعي لتوقيع الجزاء وكبح الاعتداءات على النظم المعلوماتية، بالإضافة الى توسيع اطر التعاون الدولي في هذا المجال.

تكمن أهمية هذا الموضوع، في حداثة هذا النوع من الجرائم مما قد يدعم مجال البحث الأكاديمي والاثراء القانوني علميا، مع إضفاء تحليل يمكننا من فهم الربط بين مختلف الاليات التشريعية، والتنظيمية، والتقنية عمليا، ومنه الالمام بكافة السبل الموضوعية والاجرائية التي تتطلب مناقشتها وفقا للبحث العلمي.

وقع اختيارنا لهذا الموضوع لأسباب موضوعية تتمثل في حداثة الموضوع نسبيا وإمكانية الاسهاب فيه بجمع أكبر قدر ممكن من المعلومات في بحث واحد، يمكن الباحثين المستقبليين من الانطلاق في بحوثهم بداية منه.

أما بالنسبة لأهداف الدراسة فتناولنا لهذا الموضوع، يصبوا إلى ما يلي:

- تسليط الضوء على ماهية الجرائم المعلوماتية والنظم التي تستهدفها.
- ابراز اهم الاليات المستحدثة في مجال الوقاية من الجرائم المعلوماتية ومكافحتها.

- تسليط الضوء على اطر التعاون الدولي والمساعي الرامية اليه، فيما يتعلق بالوقاية من الجرائم المعلوماتية ومكافحتها.

من بين الصعوبات التي واجهتنا أثناء اعداد هذه المذكرة، هي بذل جهد كبير للتوفيق بين الحياة المهنية والاجتماعية والدراسة، بالإضافة الى قلة المراجع الجزائرية المتخصصة خاصة في ظل التعديلات الأخيرة للقوانين الجزائرية التي تتناول موضوع الاجرام المعلوماتي مع نقص الكتابات في هذا الشأن.

من أجل دراسة الموضوع بإسهاب والتطرق الى كافة جوانبه ارتأينا طرح الإشكالية التالية:

**كيف عالج المشرع الجزائري مسألة الحماية الجنائية للنظم المعلوماتية من حيث التجريم والعقاب والإجراءات المتبعة في ذلك؟**

للإجابة على هذه الإشكالية اعتمدنا على المنهج الوصفي لعرض المفاهيم المتعلقة بالحماية الجنائية للنظم المعلوماتية واليات تطبيقها، كما اعتمدنا على المنهج التحليلي في معالجة بعض النصوص القانونية ذات الصلة بهذا الموضوع، بحيث ارتأينا اعتماد خطة ثنائية متوازنة تنقسم الى فصلين، يتضمن كل فصل منها مبحثين.

فقد تناولنا في الفصل الأول: الإطار المفاهيمي والقانوني للحماية الجنائية للنظم المعلوماتية، تطرقنا من خلاله الى: ماهية النظم المعلوماتية والحماية الجنائية الخاصة بها (المبحث الأول)، والجرائم الماسة بالنظم المعلوماتية وأركانها (المبحث الثاني).

أما الفصل الثاني فخصصناه لدراسة اليات الحماية الجنائية للنظم المعلوماتية وفق التشريع الجزائري، حيث تطرقنا الى: السبل الجنائية والجزاءات المقررة لحماية النظم المعلوماتية (المبحث الأول)، والإطار الاجرائي والتعاون الدولي في مكافحة الجرائم المعلوماتية (المبحث الثاني).

# الفصل الأول

# الفصل الأول:

# الإطار المفاهيمي والقانوني للحماية الجنائية للنظم المعلوماتية

يشهد العالم حضورا متسارعا في مجال استخدام وسائل وتكنولوجيا الاعلام والاتصال، والتي ترتكز على المعالجة الآلية للمعطيات واستخدام النظم المعلوماتية بشكل كبير، حيث أصبحت الدول والكيانات لا تستغني عن هذه الأنظمة في تسيير شؤونها وبالخصوص فيما يتعلق بالجوانب الاقتصادية والإدارية، ولكن بالموازاة مع هذا التطور كان هناك تطور آخر من جانب الإجرائي الذي تستخدم فيه نفس الوسائل والتكنولوجيا المتعلقة بالمعالجة الآلية للمعطيات والتي أصبحت بدورها تشكل خطرا يستهدف هذه الدول والكيانات والأشخاص من حيث محاولة التعدي على الأنظمة المعلوماتية الخاصة بهم أو بالأحرى التي يمتلكونها ويسيرونها وهذا الأمر استدعى تدخل المشرع لوضع قواعد قانونية تضمن حمايتها من مختلف الاعتداءات السيبرانية أو التقليدية

وعليه سنتناول في هذا الفصل الإطار المفاهيمي والقانوني للحماية الجنائية للنظم المعلوماتية من خلال تحديد ماهيتها ثم التطرق إلى الجرائم الماسة بها وأركانها القانونية.

## المبحث الأول:

## ماهية النظم المعلوماتية والحماية الجنائية

لفهم الحماية الجنائية المقررة للنظم المعلوماتية، لا بد أولًا من تحديد مفهوم هذه النظم وخصائصها، ثم بيان المقصود بالحماية الجنائية وأهميتها في البيئة الرقمية، باعتبارها الإطار الذي ينظم تدخل القانون الجنائي لمواجهة الاعتداءات المعلوماتية.، وهذا من خلال مطلبين.

### المطلب الأول:

### مفهوم النظم المعلوماتية وخصائصها

تُعد النظم المعلوماتية من الركائز الأساسية التي يقوم عليها المجتمع الرقمي، حيث تساهم في معالجة وتخزين وتبادل المعلومات، لذلك، فإن تحديد مفهومها وبيان خصائصها يُعد أمرًا ضروريًا لفهم طبيعتها القانونية والتقنية.

#### الفرع الأول: مفهوم النظم المعلوماتية

يختلف تعريف النظم المعلوماتية باختلاف الزاوية التي يُنظر منها إليها، سواء من الجانب التقني أو القانوني، مما يستدعي تقديم تعريف شامل يبرز عناصرها الأساسية ووظيفتها.

**أولاً: تعريف النظم**

على الرغم من أن النظم قد وجدت قبل وجود الإنسان إلا أن استخدام هذا المفهوم في مجالات العلم لم يكن إلا منذ 1939 فأصبح يلعب مفهوم النظم دورا هاما في العلم الحديث وقد شغل ذلك تفكير العلماء والمختصين بصفة عامة وانعكس أثره بين علماء الإدارة بصفة خاصة، حيث يعتبر أسلوب النظم بالنسبة لهم أداة أساسية وفعالة للتغلب على بعض المشاكل والصعاب التي تواجههم، فالنظام هو مجموعة أو تجمع من الأشياء المرتبطة ببعض التفاعلات المنتظمة أو المتبادلة لأداء وظيفة معينة"؛ ويعرف أيضاً بأنه مجموعة من الأجزاء التي تتفاعل وتتكامل مع بعضها البعض ومع بيئتها لتحقيق هدف أو أهداف معينة".[1]

[1] إبراهيم سلطان، نظم المعلومات الإدارية مدخل إداري الدار الجامعية، الإسكندرية، 2000، ص 18.

فالنظام مجموعة من العناصر المرتبطة التي تعمل معا لتحقيق هدف محدد، أو مجموعة أجزاء أو عناصر أو أقسام، ترتبط مع بعضها البعض بغرض أداء أهداف معينة وذلك عن طريق تحويل المدخلات إلى مخرجات.[1]

أو أنه مجموعة من العناصر والأجزاء التي تتكامل مع بعضها وتحكمها علاقات وآليات عمل معينة وفي نطاق محدد بقصد تحقيق هدف معين، فهو مجموعة من الأجزاء التي ترتبط ببعضها، ومع البيئة المحيطة بها وهذه الأجزاء تعمل كمجموعة واحدة من أجل تحقيق أهداف النظام. [2]

نستخلص من هذه التعاريف أن النظام يضمن عدد من العناصر والتي يمكن أن تمثل نظم فرعية داخل النظام ذاته وتتفاعل مع بعضها البعض من أجل تحقيق هدف أو مجموعة أهداف يسعى النظام لتحقيقها في ظل معطيات بيئة معينة.

إذن مما يتبين أن النظم أو الأنساق تشترك في عوامل هي:

- النظام يتكون من مجموعة أجزاء وعلاقات متبادلة.
- أن يكون بين هذه الأجزاء علاقات متبادلة أو متداخلة أو معتمدة ببعضها البعض.
- أنها تعمل معا في سبيل تحقيق هدف مشترك.[3]

**ثانياً: المكونات الأساسية للنظام**

انطلاقاً من تعريف النظام يمكن تحديد العناصر المكونة له والمتمثلة في:

**1- المدخلات:** تمثل المدخلات الموارد اللازمة للنظام ليتمكن من القيام بالأنشطة المختلفة لتحقيق الأهداف المسطرة، وتشمل المدخلات العديد من العناصر الغير متجانسة كالخامات والطاقة والمعلومات والآلات، وتعتبر المدخلات مخرجات لنظم أخرى سواء تلك النظم الموجودة في بيئة النظام أو نظم فرعية داخل النظام ذاته.[4]

---

[1] أحمد حسين علي حسين، نظم المعلومات المحاسبية، مطبعة الإشعاع، الإسكندرية، 1997، ص 26.

[2] نفس المرجع، ص 26.

[3] نفس المرجع، ص 26.

[4] أحمد رجب عبد العالي، المعاصرة في المحاسبة الإدارية، الدار الجامعية للطباعة والنشر، بيروت، 1992، ص 31.

**2- العمليات (التحويل):** يقصد بالعمليات تحويل المدخلات إلى مخرجات وقد تكون عملية التحويل عبارة عن آلة أو إنسان أو آلة وإنسان.

**3- المخرجات:** هو ناتج عن عملية تحويل المدخلات إلى مخرجات وقد تكون هذه المخرجات عبارة عن سلعة، خدمة أو معلومة، وتعد المخرجات الأداة التي من خلالها يتم التحقق من أداء النظام وقدرته على تحقيق أهدافه.

**4- المعلومة المرتدة:** تعتبر المعلومات المرتدة الأداة التصحيحية للمخرجات أي أداة لتحقيق الرقابة على أداء النظام، ويمكن تقسيم المعلومات المرتدة إلى نوعين معلومات مرتدة تصحيحية يقصد بها إرجاع الأشياء إلى وضعها الصحيح، ومعلومات مرتدة تطويرية تعمل على تطوير أداء النظام أو تغيير الأهداف. [1]

**5- العلاقات:** تمثل الوسيلة التي من خلالها يتم ربط النظم الفرعية ببعضها البعض، وأيضا ربط النظام ببيئته.

**6- بيئة النظام:** أي أن النظام لا يوجد في معزل عن النظم الأخرى، فتواجده في البيئة يسمح له باستقطاب مدخلاته منها كما أنه يلقي بمخرجاته إليها وبالتالي فعدم وجود تفاعل بين النظام وبيئته يؤدي إلى فشل النظام وعدم فاعليته التي كانت متوقعة منه.

**7- حدود النظام:** تتمثل حدود النظام في الغشاء الذي يحيط به ويفصله عن بيئته، فهي غير ثابتة لأنها تتوقف على أهداف النظام ودرجة تعقيده.

**ثالثاً: تعريف نظم المعلومات:**

انطلاقاً من ظاهرة المعلومات التي يتسم لها العصر الحديث والحاجة الملحة للحصول على المعلومات سواء للفرد أو المؤسسة، وفي إطار مدخل النظام المستخدم في إدارة المنشآت المعاصرة، ارتبطت هذه النظم بالمعلومات وكونت ما أتفق عليه حديث ينظم المعلومات".[2]

يمكن تعريف المعلومة على أنها هي المعرفة التي لها معنى ومفيدة في تحقيق الأهداف، ويجب أن تتصف المعلومة بالدقة في الوصف والسرعة في تحضيرها وجلبها إضافة إلى تميزها بالبساطة.[3]

---

[1] إسماعيل السيد، نظم المعلومات لإيجاد القرارات الإدارية، المكتب العربي الحديث، الإسكندرية، 2001، ص 102.

[2] إيمان فاضل السامرائي وهثم محمد الزعبي، نظم المعلومات الإدارية، دار صفاء، الأردن، 2004، ص ص 9-10.

[3] سعد غالب ياسين، نظم المعلومات الإدارية، دار اليازوري، عمان، الأردن، 1997، ص 22.

تعددت واختلفت تعاريف نظم المعلومات وتذكر منها ما يلي فهي:

– مجموعة من العناصر (وسائل، برمجيات أو أفراد تسمح بحيازة، ومعالجة، وتخزين وإرسال المعلومات.[1]

– عبارة عن كل الأشخاص الذين يستقبلون يستعملون ويرسلون المعلومات من خلال مختلف الآلات الكاتبة والناسخة والحاسبة، تعمل على تسجيل وتخزين وترتيب وإرسال المعلومات للأطراف المعنية.

– مجموعة من الإجراءات والوثائق التي تعطي المعلومات المفيدة وتساعد في وظائف التسيير، ومن جهة ثانية الوسائل المادية والبشرية الضرورية للمعالجة، تخزين وتحويل المعلومات بهدف استغلالها الجيد والصحيح.[2]

– يخص نظم المعلومات المتعلقة بالمؤسسات من خلال ما تعطيه هذه النظم من معلومات مفيدة للتسيير، حيث تعمل الموارد البشرية والوسائل المادية على الحصول عليها ومعالجتها وتخزينها وتحويلها إلى معلومات صالحة وذات كفاءة عالية.

– مجموعة من الموارد والوسائل والبرامج والأفراد والمعطيات والإجراءات التي تسمح بجمع ومعالجة وإيصال المعلومات على شكل نصوص، صور، رموز في المؤسسة.[3]

– مجموعة من الإجراءات التي يتم من خلالها تجميع أو استخراج، تشغيل تخزين ونشر المعلومات، بغرض دعم عمليات وضع القرار وتحقيق الرقابة داخل المؤسسة.[4]

– نشاط المشروع الذي ينطوي على تجميع وتصنيف وتبويب وتوزيع البيانات.[5]

كما يعمل نظام المعلومات على تحقيق الأهداف التالية:

---

[1] سليم إبراهيم الحسينه، نظم المعلومات الإدارية، مؤسسة الورق، عمان الأردن، 1998، ص 63.

[2] سونيا محمد البكري وإبراهيم سلطان، نظم المعلومات الإدارية، دار النشر الجامعية الجديدة، مصر، 2002، ص 13.

[3] صلاح الدين عبد المنعم مبارك، اقتصاديات نظم المعلومات المحاسبية والإدارية، دار الجامعة الجديدة، الإسكندرية، 2001، ص 17.

[4] سونيا محمد البكري وإبراهيم سلطان، مرجع سابق، ص 23.

[5] نفس المرجع، ص 26.

– المراقبة: إذ أنه بمثابة ذاكرة للمؤسسة بما يعالجه من معلومات تسمح بتكوين وصف تاريخي لأحوالها، يسهل اكتشاف الأخطاء التي قد تقع، أي أن نظام المعلومات ينبغي أن يحقق الثقة كي تكون المراقبة فعالة.

– التنسيق والاتصال بين مختلف المصالح عن طريق تبادل المعلومات والوثائق المرافقة المختلف التدفقات.

– مساعدة المسيرين في عملية اتخاذ القرار عن طريق إيجاد أساس أو قاعدة لتحليل الإشارات التحذيرية الأولية التي تبرز داخلياً وخارجياً.

– هدف نظام المعلومات إذن هو توفير المعلومات الضرورية لكل مستويات التسيير عن حالتها الحالية، والتنبؤ عن طريق تجميع هذه المعلومات حفظها، تحليلها ووضعها معاً، بطريقة تساعد على الإجابة على أسئلة استراتيجية، تسييرية وتنفيذية مهمة. [1]

– إنتاج معلومة مفيدة.

– تقديم وصف دقيق للمؤسسة.

– تسهيل وضع التقديرات.

– توضيح القرارات الضرورية الواجب اتخاذها.

– استخراج الانحرافات بين التقديرات والإنجازات، وإمكانية تحديد أسبابها وتقليصها.

– يسمح بوضع إجراءات تصحيحية مفيدة لحركة المؤسسة.

– ينبه المؤسسة قبل وقوع الخطأ (نظام تنبئي).

– يساعد المسيرين والعاملين في تحديد المشاكل، وتطوير المنتجات وإنشاء منتجات جديدة.

**رابعاً: مبادئ نظم المعلومات الجديدة**

إن العصر الذي تشهده الآن هو عصر المعلومات وبالتالي فإنه مما لا شك فيه أن تكون المعلومات أساس كل قرار، لذلك لابد من أن تتوفر في نظم المعلومات الحديثة المبادئ التالية:

[1] كامل السيد غراب وآخرون، نظم المعلومات الإدارية، جامعة الملك سعود، 1997، ص 20.

**1- الخدمة:** ينبغي أن يصمم النظام وأن يدار بالطريقة التي تضمن أعلى كفاءة في تقديم الخدمات للمستفيدين.[1]

**2- التوقيت:** ينبغي أن يعمل النظام على تقديم المعلومات لطالبها حين يحتاجها وليس عندما يستطيع النظام أن يحصل عليها،[2] حيث أن الاستجابة السريعة للنظام هي مؤشر على عمله بكفاءة وفاعلية.

**3- التوحيد:** تتطلب سهولة تداول المعلومات بين أجزاء النظام ذاته وبين غيره من النظم، ضرورة اتباع طرق التوحيد القياسي في معالجة المعلومات.

**4- التطوير:** وهو أساس المحافظة على استمرار كفاءة النظام في مواجهة التغيرات المتعددة لتحسين طرق المعالجة وزيادة سرعة توصيل المعلومات. [3]

**خامساً: عوامل تطور نظم المعلومات**

كانت نظم المعلومات في الخمسينات عبارة عن نظم التشغيل البيانات، أما في السبعينات ظهرت نظم تخدم المستويات الإدارية، ثم ظهرت نظم أخرى تخدم المستويات التي تحدد استراتيجيات المنظمة في الثمانينات، ويمكننا إيضاح العوامل التي أدت إلى هذه التطورات في نظم المعلومات في النقاط التالية:

**1- التطور في تكنولوجيا المعلومات:** أدى نمو تكنولوجيا المعلومات إلى تزايد الدور الذي تلعبه نظم المعلومات داخل المؤسسات، هذا النمو أدى إلى ضرورة استخدام الحاسبات في كافة المستويات خاصة إذا أخذنا بعين الاعتبار سهولة تعلم البرمجيات الجديدة وأيضاً انخفاض التكاليف التي أصبحت في متناول أغلبية المؤسسات.

**2- التطور في خصائص التطبيقات:** بدأت نظم المعلومات بتقديم نظم ذات أغراض عامة متعلقة بالوظائف المتداولة في أغلبية المؤسسات مثل تلك المتعلقة بالمخزون المبيعات الإنتاج التسويق والتمويل، لكن مع تطور دور نظم المعلومات وتطور تكنولوجيا الحاسبات الآلية ظهرت برامج حديدة تهدف إلى خدمة

[1] كمال الدين الدهراوي، مدخل معاصر في نظم المعلومات المحاسبية، الدار الجامعية، الإسكندرية، 2003، ص 11.
[2] كامل السيد غراب وآخرون، مرجع سابق، ص 21.
[3] محمد حسين آل فرج الطائي، المدخل إلى نظم المعلومات الإدارية، دار وائل، الأردن، 2005، ص 14.

تخصصات محددة لأفراد أو مجموعات معينة داخل المؤسسة مثل نظم دعم القرار للإدارة الوسطى والنظم الخبيرة.[1]

**الفرع الثاني: خصائص النظم المعلوماتية**

يمكن إجمال خصائص نظم المعلومات في العناصر التالية:

**أولا – شبكة الاتصال:** يشبه نظام المعلومات حالة شبكة الاتصال في أنه يزود بمسارات معلوماتية إلى الكثير من النقاط، وهو يساعد المعلومات على التدفق في كل مكان بالمشروع وربما إلى أماكن خارج المشروع.

بينما يتم الحصول على المعلومات خلال مرحلة للمخرجات، وعليه فان البيانات هي الخامات التي تتحول إلى منتجات معلوماتية، كما تنتج المعلومات المختلف الأهداف والمستخدمين.

**ثانيا– أداة التحويل وتوظيف البيانات:** تقوم نظم المعلومات بتحويل المدخلات إلى مخرجات، وهنا توجد ثلاثة مراحل أساسية في هذا التحويل وهي مرحلة الإدخال ومرحلة التشغيل ومرحلة الإخراج، وترتبط بهذه المراحل عدة وظائف هي تجميع البيانات وتشغيلها وإنتاج المعلومات، كما يتم تنفيذ وظائف أخرى هي رقابة وإدارة البيانات.

**ثالثا – أداة لإدخال البيانات وإخراج المعلومات:** يتم إدخال البيانات خلال مرحلة الإدخال، بينما يتم الحصول على المعلومات خلال مرحلة المخرجات، وعليه فإن البيانات هي الخامات التي تتحول إلى منتجات معلوماتية، كما تنتج المعلومات المختلف الأهداف والمستخدمين.

**1– مستخدمو المعلومات:** يتم إنتاج المعلومات من نظام المعلومات بالمشروع وذلك لاستخدامه من طرف المستخدم الداخلي أو الخارجي، ويشمل المستخدم الداخلي المديرين والموظفين بالمشروع، أما المستخدم الخارجي فيشمل كافة الجهات المهتمة خارج المشروع مثل الدائنين والموردين وحملة الأسهم والوكالات الحكومية واتحاديات العمال.[2]

**2– الأهداف:** أي نظام معلومات بأي مشروع له ثلاثة أهداف أساسية هي:[3]

---

[1] محمد حسين آل فرج الطائي، مرجع سابق، ص 15.

[2] كامل السيد غراب وآخرون، مرجع سابق، ص 22.

[3] محمد حسين آل فرج الطائي، مرجع سابق، ص 16.

* التزويد بالمعلومات المساندة لعملية اتخاذ القرار.

* التزويد بالمعلومات المساندة للعمل اليومي الروتيني.

* التزويد بالمعلومات المساندة.

## المطلب الثاني:

## مفهوم الحماية الجنائية للنظم المعلوماتية وأهميتها

وظيفة القانون الجنائي هي الوقاية والردع وبالتالي فالغاية التي يسعي إليها تتمثل في حماية وصيانة المصالح الجوهرية للمجتمع، بتقرير الجزاء الجنائي وتوقيع عقوبات على كل من يخالف أحكام قانون العقوبات، وتحقيق الاستقرار وإقرار العدالة، وهذا ما سنعالجه من خلال فرعين.

### الفرع الأول: مفهوم الحماية الجنائية للنظم المعلوماتية

رغم الخصوصية التي تتميز بها المصطلحات القانونية، يبقى إرجاع المصطلح لأصله اللغوي أمر مهما من الناحية العملية والمنهجية، يتضمن الأول التعريف اللغوي، والثاني التعريف الاصطلاحي.

**أولا- التعريف اللغوي:**

لفظ الحماية الجنائية، مركب وصفي من لفظين الحماية والجناية:

**1- الحماية**

الحماية لغة: من الفعل (حمى) فيقال حمى الشيء فلانا، حميا وحماية: منعه ودفع عنه ويقال حماه من الشيء وحماه الشيء، والحماية احتياط يرتكز، إذ يتجاوب مع من يحميه أو ما يحميه ويناظر عموماً واجباً لمن يؤمنه على وقاية شخص أو مال ضد المخاطر وضمان أمنه وسلامته عن طريق وسائل قانونية أو مادية، تدل كذلك على عمل الحماية ونظامها على حد سواء (تدبير، نظام) ومرادفها الوقاية.[1]

[1] إسراء محمد علي سالم، الحماية الجنائية للعتبات المقدسة، دراسة مقارنة، مجلة المحقق الحلي جامعة بابل ، للعلوم القانونية والسياسية، المجلد 06، العدد 01،2014، ص 82.

**2- الجناية**

الجناية لغة: مصدر جنى جناية وجمعه جنايات وجمعت – وإن كانت مصدرا – لتنوعها إلى عمد وشبه عمد وخطأ، والجناية الذنب والجرم وما يفعله الإنسان مما يوجب عليه القصاص والعقاب في الدنيا والآخرة، يقال: حتى جناية إذا جر جريرة على نفسه أو على قومه.[1]

الجناية أو الجريمة لغة هي الذنب أو المعصية، أو كل ما يجنيه المرء من شر اكتسبه. ولها في الشرع معنى عام وخاص. أما الأول فالجناية: هي كل فعل محرم شرعاً، سواء وقع الفعل على نفس أو مال أو غيرهما وعرفها الماوردي بقوله: الجرائم محظورات شرعية زجر الله تعالى عنها بحد أو تعزير. والمحظور: إما إتيان منهي عنه، أو ترك مأمور به.[2]

**ثانيا- التعريف الاصطلاحي**

وضع الفقه الجنائي تعريف جامع مانع للحماية الجنائية بتحليله يمكن تقسيم هذا الفرع إلى عنصرين: الأول المقصود بالحماية الجنائية والثاني خصائص هذه الحماية.

**1- المقصود بالحماية الجنائية**

يستمد قانون العقوبات أهميته من الغاية التي يسعي إلي تحقيقها والمتمثلة في صيانة امن المجتمع واستقراره وإقامة العدالة فيه ، وبهذا الوصف فان قانون العقوبات هو سيف السلطة العامة في مواجهة الذين يخرجون عن إرادة الجماعة بالاعتداء علي المصالح الجوهرية للحياة الاجتماعية التي يحرم المساس بها بتوفيره الجزاء الجنائي الذي يعد أقصي مراتب الحماية القانونية[3]، وتتخذ الحماية الجنائية في ظل قوانين العقوبات صورتين وذلك باعتبار نوع المصلحة محل الحماية، فالصورة الأولى هي الحماية الجنائية للمراكز الشخصية وتتحقق عندما يتولى المشرع الجنائي حماية المراكز القانونية الشخصية ، أي عندما تطبق القواعد القانونية في حالة تغلب عليها الصفة الفردية فمثلاً في جريمة السرقة يعاقب المشرع الجنائي على الاعتداء على ملكية الغير باعتبارها مركزاً قانونياً فردياً يعتدي عليه السارق أما الصورة الثانية للحماية الجنائية فهي حماية المراكز الموضوعية وذلك عندما يسبغ المشرع حمايته على المراكز القانونية الموضوعية بتطبيق

---

[1] احمد عبد السلام، على الموقع www.fiqh.islammessage.com ، ، اطلع عليه 10 مارس 2026، الساعة: 13:55.

[2] وهبة الزحيلي، الفقه الإسلامي وأدلته، دار الفكر دمشق، الطبعة الرابعة، عدد الأجزاء 10، على الموقع WWW. islamport.com، اطلع عليه ، 10 مارس 2026، الساعة 17.40.

[3] سليمان بارش، شرح قانون العقوبات الجزائري، الجريمة، ديوان المطبوعات الجامعية، الجزائر، سنة 1995، ص 10.

القاعدة القانونية بصفة عامة تحقيقاً للصالح العام ففي جريمة الزنا يتولى المشرع بالحماية الزواج باعتباره مركزاً قانونياً موضوعياً يتمتع بصفة العموم[1]، إذن الحماية الجنائية هي احد أنواع الحماية القانونية بل و أهمها و أخطرها أثرا علي كيان الإنسان وحرياته ووسيلتها القانون الجنائي الذي قد تنفرد قواعده ونصوصه تارة بتحقيق هذه الحماية و قد يشترك معها في ذلك فرع آخر من فروع قانون تارة أخري ، فوظيفة القانون الجنائي الحماية، إذ يحمي قيما أو مصالح أو حقوق بلغت من الأهمية حدا يبرر عدم الاكتفاء بالحماية المقررة لها بالنسبة لفروع القانون الأخرى ، فالمشرع يعبر عن إرادته في نصوص تتضمن قواعد قانونية ، يمكن ردها إلي عدة تقسيمات هو المصلحة التي يحميها القانون بقاعدته فهناك قواعد قانونية تتبع القانون المدني و أخري تتبع القانون التجاري أو الإداري أو الدستوري أو الجنائي. [2]

ومن هنا تتضح خصوصية وظيفة القانون الجنائي بالنسبة لوظيفة باقي فروع القانون وتتجلي هذه الخصوصية من ناحيتين أولهما: تتعلق بطبيعة الجزاء المقرر، وثانيهما ترتبط بطبيعة المصلحة المحمية قانونا.[3]

ومن خلال التوازن الذي يقيمه القانون الجنائي بين المصلحة العامة والمصلحة الخاصة فان هذا القانون لا يتواني عن حماية حق الفرد في الحرية بطريقتين: الأولى هي معاقبة الاعتداء علي حق الفرد في الحرية سواء وقع هذا الاعتداء بواسطة أحد الأفراد أو بواسطة أحد رجال السلطة العامة، أما الثانية فمؤداها تقرير الضمانات التي تكفل الحرية ضد أي إجراء جنائي تتخذه السلطة العامة وهذا قوام الدولة القانونية.[4]

**2- خصائص الحماية الجنائية**

طبيعة القاعدة الجنائية مقارنة بباقي قواعد النظام القانوني العام والخاص، تضفي على نوع الحماية التي تقدمها خصائص تميزها عن غيرها من أنواع الحماية القانونية وتظهر أساسا في:

[1] إسراء محمد علي سالم، مرجع سابق، ص 83.

[2] رمزي حوحو، الحماية الجنائية الدولية لحقوق الإنسان، مجلة المفكر، المجلد 1، العدد 5، جامعة محمد خيضر بسكرة، 2010، ص 196.

[3] نفس المرجع، ص 196.

[4] نفس المرجع، ص 197.

**أ – طبيعة الجزاء المقرر فيها**

بعد الجزاء الجنائي ذلك الأثر الذي يترتب قانونا علي سلوك يعد جريمة في قانون العقوبات ، فالقاعدة الجنائية تتضمن عنصرين هما التكليف و الجزاء ، فأما التكليف فهو الخطاب الموجه إلى كافة الناس ويأمرهم بضرورة الابتعاد عن العمل الإجرامي ، أما الجزاء فيتضمن إنزال العقاب بكل من يتجرأ علي مخالفة هذه الأوامر والقاعدة التي لا تتضمن النص علي الجزاء هي مجرد قاعدة أخلاقية ، يعرف الفقه الجزاء الجنائي بأنه "عبارة عن إجراء يقرره القانون ويوقعه القاضي علي شخص ثبتت مسؤوليته عن جريمة".[1]

**ب– طبيعة المصلحة المحمية جنائيا**

السياسة الجنائية ماهي إلا انعكاس لحاجات الجماعة ومصالحها وقيمها لذلك نجد أن الحماية الجنائية لتلك المصالح، كي تكون لها فعاليتها لابد وان تحيط بأي فعل من شانه أن يضر بها أو يهددها بالضرر، وطبيعي للوصول إلى حماية هذه المصالح الأساسية، يتعين حماية المصالح الجزئية والتي من مجموعها تتكون القيم والمصالح العامة لذات الجماعة[2]، إذن فالحماية الجنائية نوع من أنواع الحماية القانونية تعبر فيها إرادة المشرع في صورة جزاء صارم يحافظ على المصالح والحقوق العامة والخاصة بشكل دقيق وفعال.

**الفرع الثاني: أهمية الحماية الجنائية للنظم المعلوماتية**

تكتسي الحماية الجنائية أهمية بالغة في ظل التحول المتسارع نحو الرقمنة، حيث أصبحت النظم المعلوماتية تمثل العمود الفقري لمختلف الأنشطة الاقتصادية والإدارية وحتى الاجتماعية، ولم يعد الأمر يقتصر على مجرد استخدام التكنولوجيا، بل تجاوز ذلك إلى الاعتماد الكلي عليها في تسيير المرافق العامة والخاصة، الأمر الذي يجعل أي اعتداء عليها يشكل تهديدًا مباشرًا لاستقرار المجتمع وأمنه المعلوماتي.

وتبرز أهمية الحماية الجنائية في كونها الوسيلة القانونية الأنجع لردع السلوكات الإجرامية التي تستهدف النظم المعلوماتية، إذ يعمل القانون الجنائي على تجريم الأفعال التي تمس بسرية البيانات وسلامتها

[1] عبد الرحمان خلفي، محاضرات في القانون الجنائي، دار الهدى للطباعة والنشر، الجزائر، 2012، ص ص 190–191.

[2] رفيق شاوش، المصلحة المحمية في الجرائم المضرة بالإدارة العامة في التشريع الجنائي المقارن، مجلة المفكر، المجلد 11، العدد 01،2016، ص 586.

وتوافرها، وهي المبادئ الأساسية التي يقوم عليها أمن المعلومات، فبدون وجود نصوص قانونية رادعة، قد تتفاقم الجرائم المعلوماتية وتؤدي إلى أضرار جسيمة يصعب تداركها[1].

كما تساهم الحماية الجنائية في تعزيز الثقة في البيئة الرقمية، سواء بالنسبة للأفراد أو المؤسسات، حيث أن الشعور بوجود حماية قانونية فعالة يشجع على استخدام الوسائل الإلكترونية في المعاملات المختلفة، خاصة في مجالات التجارة الإلكترونية والخدمات الرقمية، فالثقة تعد عنصرًا أساسيًا في نجاح أي نظام معلوماتي، ولا يمكن تحقيقها إلا من خلال ضمان حماية قانونية صارمة[2].

ومن جهة أخرى، تلعب الحماية الجنائية دورًا مهمًا في حماية المصالح الاقتصادية، إذ أن الاعتداءات على النظم المعلوماتية قد تؤدي إلى خسائر مالية كبيرة نتيجة سرقة البيانات أو تعطيل الأنظمة أو اختراقها، وهو ما يؤثر سلبًا على الاستثمار والتنمية الاقتصادية، كما أن هذه الجرائم قد تستهدف مؤسسات حساسة كالبنوك والإدارات الحكومية، مما يزيد من خطورتها. [3]

إضافة إلى ذلك، تساهم الحماية الجنائية في صون الحقوق والحريات الفردية، خاصة الحق في الخصوصية وحماية المعطيات الشخصية، حيث أن الاستخدام غير المشروع للبيانات قد يؤدي إلى انتهاك الحياة الخاصة للأفراد، ومن هنا فإن تدخل المشرّع الجنائي يعد ضرورة لضمان التوازن بين حرية استخدام التكنولوجيا وحماية الحقوق الأساسية. [4]

وأخيرًا، فإن فعالية الحماية الجنائية في البيئة الرقمية تظل مرتبطة بمدى مواكبة التشريعات للتطورات التكنولوجية، إذ أن الطابع المتجدد للجرائم المعلوماتية يفرض على المشرّع تحديث القوانين بشكل مستمر، إلى جانب تعزيز التعاون الدولي لمكافحة هذا النوع من الجرائم العابرة للحدود.[5]

---

[1] سعد غالب ياسين، مرجع سابق، ص 23.

[2] إيمان فاضل السامرائي وهيثم محمد الزعبي، مرجع سابق، ص ص 12-13.

[3] صلاح الدين عبد المنعم مبارك، مرجع سابق، ص 18.

[4] رمزي حوحو، مرجع سابق، ص 197.

[5] عبد الرحمان خلفي، مرجع سابق، ص 192.

## المبحث الثاني:

## الجرائم الماسة بالنظم المعلوماتية وأركانها

تتعدد الجرائم التي تستهدف النظم المعلوماتية، وتتخذ صورًا مختلفة تتراوح بين البسيطة والمشددة، وهو ما يتطلب دراستها من حيث صورها المختلفة وأركانها القانونية لفهم كيفية قيام المسؤولية الجنائية عنها، وهذا من خلال مطلبين.

### المطلب الأول:

### صور الجرائم الواقعة على النظم المعلوماتية.

حاول المشرع الجزائري خلال الفترات الأخيرة من الزمن تدارك الفراغ القانوني الذي عرفه مجال الإجرام الإلكتروني، فقام بتعديل أحكام قانون العقوبات الجزائري، بموجب القانون رقم 04-15، مستحدثا فيه مجموعة من النصوص التي جرم من خلالها كل الأفعال والسلوكيات المرتبطة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها جزاء.[1]

ويمكن الإشارة قبلها، إلى تعريف الجريمة المعلوماتية أو الجريمة السيبيرانية أو جريمة الفضاء الالكتروني مثلما يسميها البعض، وهي جريمة يستخدم الحاسوب في ارتكابها، وهي عبارة عن مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي وسواء كان ذلك بطريقة مباشرة أو غير مباشرة، والمهم في ذلك هو استخدام وسائل الاتصال الحديثة بشأنها من كمبيوتر، أو أية آلة ذكية أخرى.

وتجدر الإشارة إلى أن الجرائم الواقعة على النظم المعلوماتية تتحقق في صورتين:

تبرز الأولى في جريمتي الدخول والبقاء غير المرخص بهما في النظام، وبينما تظهر الصورة الثانية في تلك النتائج غير المشروعة ضد معطيات النظام المترتبة عن فعل الدخول أو البقاء.

[1] قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم ال أمر66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، الصادر بتاريخ 10 نوفمبر 2004، ص8.

**الفرع الأول: الصور البسيطة للاعتداء على النظم المعلوماتية**

تتمثل الصورة البسيطة للاعتداء على النظم المعلوماتية في شكل الدخول (أولا) أو البقاء (ثانيا) غير المرخص بهما.

**أولا- الدخول غير المرخص به**

تنص المادة 394 مكرر من قانون العقوبات الجزائري أنه: يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 60000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك».[1]

يفهم من نص الفقرة الأولى في المادة أعلاه، أن الجزاء عن مثل هذه المخالفات يكون بمجرد تحقق الركن المادي للجريمة، والذي يكمن في فعل الدخول، وطبعا هنا يكون الدخول باستعمال الوسائل الفنية والتقنية للنظام المعلوماتي، وبغض النظر إن كان الدخول إلى النظام بأكمله أو إلى جزء منه فقط.

كما يفهم من نص الفقرة أيضا أن المشرع لا يعاقب على الفعل الكامل، أي على الجريمة التامة، وإنما يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى بالبعض إلى الإقرار أن هذه الجرائم من قبيل الجرائم الشكلية، التي لا تشترط لقيامها تحقق النتيجة الإجرامية، والشرط الوحيد في البند هو أن يكون الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش، أي لن يكون مشروعا، كالدخول من دون وجه حق أو من دون ترخيص مسبق، بمعنى ألا يكون الدخول صدفة أو عن طريق الخطأ.[2]

وتجدر الإشارة هنا، إلى أن المشرع الجزائري لم يشترط في نص الفقرة الأولى من المادة أعلاه، طبيعة خاصة لهذا النظام، أي أن المادة 394 مكرر لم تشترط لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق، بل جاءت عامة ومطلقة وتحمي كل الأنظمة المعلوماتية وبدون أي استثناء سواء كان النظام المعلوماتي محميا أو غير محمي.

وبذلك يكون المشرع الجزائري قد أصاب بشكل كبير في تنظيمه لهذه المسألة، حيث وبتمييز المشرع بين تجريم الدخول غير المرخص به إلى نظام معلوماتي محاط بحماية فنية وعدم التجريم للدخول غير

[1] المادة 394 مكرر من القانون 04-15، سالف الذكر.

[2] نفس المرجع.

المرخص به إلى نظام معلوماتي غير محاط بحماية فنية، سيؤدي حتما إلى فتح المجال للمجرمين من التهرب من المسؤولية الجزائية عن فعل الاعتداء، بحجة أن النظام المعتدى عليه غير محاط بحماية فنية، وبذلك، فيكون المشرع قد أحسن فعلا عندما لم يفصل بين النظام المحاط بالحماية الفنية، وذلك النظام غير المحاط بها. [1]

**ثانيا- البقاء غير المرخص به**

يقصد بالبقاء غير المرخص به هنا الدخول إلى النظام المعلوماتي والاستمرار في التواجد داخله وذلك دون إذن من صاحبه، رغم علم الشخص الذي قام بالفعل بأن بقاءه فيه غير مرخص.

ولقد سوى المشرع الجزائري بموجب المادة 394 مكرر من قانون العقوبات السابق بين كل من جريمة الدخول غير المرخص به والبقاء غير المرخص به، وذلك على غرار ما اتخذه المشرع الفرنسي في منظومته الجزائية، وهو ما تأكد بتطبيق الجزاء نفسه على السلوكين وهي عقوبة الحبس من ثلاثة (06) أشهر إلى سنة، وغرامة مالية من 60000 دج إلى 200000 دج ويعتبر فعل البقاء مثله مثل فعل الدخول، بمثابة الركن المادي للجريمة، ونضيف هنا ونؤكد أن البقاء قد يأخذ شكل إحدى الصورتين الآتيتين:

تتمثل الصورة الأولى في حالة تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول ويكون الدخول إلى نظام المعالجة مشروعا، حتى وإن كان خطأ أو صدفة، غير انه وبتفطن الفاعل للوضع وبدلا من الانسحاب أو مغادرة النظام فورا، فإنه يستمر في استغلال النظام، فهنا يعاقب على جريمة البقاء غير المرخص به.

بينما تكمن الصورة الثانية، في حالة تحقق فعل البقاء غير المرخص به متصلا ومجتمعا مع فعل الدخول وهي حالة أكثر تشديدا من سابقتها كون فعل الدخول وفعل البقاء مجتمعين وينشأن بصفة غير مشروعة، كأن يتم الدخول دون ترخيص أو إذن سابق، ثم يستمر في البقاء داخله. [2]

والإشكال الذي يمكن أن يثيره هذا الاجتماع والتداخل للسلوكين من دخول إلى النظام والبقاء فيه، هو تحديد النطاق الزمني لكل واحدة منها، بمعنى متى تنتهي جريمة الدخول؟ ومتى تبدأ جريمة البقاء؟

---

[1] أمال قارة، الحماية الجزائية المعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص 102.

[2] نفس المرجع، ص 103.

ومن أجل الإجابة عن الإشكال، فلقد تضاربت آراء فقهية عن المسألة، إذ هناك من يرى بأن الجريمة المتعلقة بالبقاء داخل النظام تبدأ من اللحظة التي يتم فيها الدخول الفعلي للمجرم إلى النظام، وذلك بتجوله وتنقله داخل هذا الأخير، وهنا تكون جريمة الدخول مكتملة، وهناك من يرى بأن جريمة البقاء تكون في الوقت الذي يعلم فيه المتدخل بأن بقاءه في النظام غير مشروع، ولم ينسحب من النظام، بل يبقى يتجول داخل النظام المعلوماتي بعد علمه بأن هذا البقاء ليس له الحق فيه ويشكل جريمة يعاقب عليها القانون. [1]

ومهما يكن من أمر، فإن المشرع الجزائري ومن خلال المادة 394 مكرر قد تطرق إلى فعل الدخول ثم إلى فعل البقاء، وكأن المشرع يصنف الفعل الأول بأنه جريمة وقتية كون فترة استمرارها قصيرة جدا والفعل الآخر على أنه جريمة مستمرة، مقارنة بالأولى.

**الفرع الثاني: الصور المشددة للاعتداء على النظم المعلوماتية**

يشدد المشرع الجزائري من العقوبة المقررة الدخول والبقاء بدون ترخيص في النظم المعلوماتية، وذلك بموجب الفقرة الثانية من المادة 394 مكرر من قانون العقوبات التي تنص أنه: .... تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة أو ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة بعقوبة الحبس من سنة إلى 03 سنوات والغرامة من 100000 دج إلى 300000 دج». [2]

تبعا لذلك، فإن المادة تحدد ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في النظم المعلوماتية وهما:

– حالة الدخول أو البقاء مع محو أو تعديل في البيانات التي يحتويها النظام المعلوماتي.

– ويتحقق الثاني عندما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة المعلوماتية وإعاقته عن أداء وظيفته.

وتجدر الإشارة هنا إلى أن الصورة البسيطة للاعتداء على النظام المحددة في المادة 394 مكرر 01 السابقة لم تشترط البحث في النتيجة الإجرامية، بينما وباستقراء الفقرة 02 من المادة 394 مكرر يفهم أن

[1] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص 28.
[2] المادة 394 مكرر من القانون 04-15، سالف الذكر.

النتيجة الإجرامية واجبة الإثبات، فيجب إثبات المحو أو التعديل أو التخريب للإقرار بالصورة المشددة للجريمة، وإلا كنا بصدد الصورة الأولى والبسيطة لا أكثر.[1]

من هنا نلاحظ أن المشرع قام بتشديد العقاب، والهدف طبعا هو الحد من تفاقم الإجرام المعلوماتي وما يرتبه من أضرار بالغة ووخيمة على الفرد والمجتمع والدولة ككل، وذلك من الناحية المعلوماتية.

## المطلب الثاني:

## الأركان القانونية للجرائم الماسة بالنظم المعلوماتية

تشمل الصور البسيطة الأفعال التي لا تنطوي على ظروف مشددة، مثل الدخول غير المشروع أو الاستخدام غير المصرح به، والتي تشكل الأساس العام للجرائم الواقعة على النظام المعلوماتي، حيث سيتم التطرق من خلال هذا المطلب إلى أركان جريمة الدخول أو البقاء في النظام المعلوماتي في الفرع الأول، وأركان جريمة الاعتداء على سير النظام المعلوماتي واتلاف المعلومات في الفرع الثاني.

### الفرع الأول: أركان جريمة الدخول أو البقاء في النظام المعلوماتي

يذهب غالبية الفقه إلى تقسيم أركان الجريمة إلى ثلاثة أركان وهي الركن الشرعي والركن المادي والركن المعنوي.

وهذه الأركان يتعين أن تتوافر في كل الجرائم أيا كانت طبيعتها وسنركز في هذه الدراسة على الركن المادي والركن المعنوي باعتبار أن الركن الشرعي بالنسبة للجرائم الواقعة على النظام المعلوماتي هو واضح بالنسبة لجريمة الدخول أو البقاء وذلك بموجب المادة 394 مكرر التي تندرج ضمن القسم السابع مكرر من قانون العقوبات الجزائري المعدل والمتمم، وسنحاول فيما يلي التطرق الى اركان هذه الجريمة:

#### أولا- الركن المادي لجريمة الدخول والبقاء في النظام المعلوماتي

الركن المادي للجريمة هو الذي يعبر عن المظهر الخارجي للإرادة الآثمة ولا تقوم الجريمة إلا بتوافره، فالقانون لا يعاقب على النوايا مهما أضمرت من الشر، إلا إذا اتخذت مظهرا خارجيا يعبر عنها، فهو كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا يؤدي إلى نتيجة تمس حقا من

[1] خذير مسعود الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010، ص 123.

الحقوق المصانة دستوريا وقانونيا[1]، ووفقا للقواعد العامة يقوم الركن المادي للجريمة على مجموعة من العناصر المادية التي تلحق ضررا ما بمصلحة يحميها القانون جنائيا.[2]

**1- الركن المادي لجريمة الدخول**

يمثل الركن المادي الجانب المادي للجريمة الذي يدخل في تكوينها ، ويبرز هذا الجانب إلى العالم الخارجي بمظهر مادي يعبر عن سلوك ونتيجة ويتكون الركن المادي من ثلاث عناصر هي، السلوك الإجرامي والنتيجة التي تحققت والعلاقة السببية التي تربط بين السلوك و النتيجة، وقد لا يتوفر الركن المادي دائما على هذه العناصر في جميع الجرائم، فقد يكتفي المشرع بالسلوك وحده للقول بقيام الركن المادي للجريمة دون اشتراط أن تتحقق النتيجة الإجرامية وصورة ذلك ما يسمى بالجرائم الشكلية وبالرجوع الى قانون العقوبات الجزائري نجده يعاقب كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك[3]، فقد نص المشرع الجزائري على فعل مادي وهو الدخول عن طريق الغش، إلا أنه لم يقدم تعريفا له بل اكتفى بالقول في المادة 394 مكرر .... كل من يدخل أو يبقى عن طريق الغش." وفيما يلي سنحاول توضيح اهم الطرق التي تستخدم للدخول الى النظام المعلوماتي حيث تتم عملية الدخول الى النظام المعلوماتي بعدة طرق نذكر أهمها:

**أ- الاتصال المادي المباشر بالنظام المعلوماتي :** ويقصد به الدخول إلى النظام دون الحاجة الى شبكة اتصال معلوماتي أو الكتروني لتحقيق الجريمة اي الجاني موجود في نفس المكان الذي يوجد فيه النظام محل الجريمة وما عليه في هذه الحالة الا إجراء عمليات سواء مادية مثلا إدخال دعامة مادية كالقرص المضغوط تحتوي على برنامج فك الرموز للدخول في النظام المعلوماتي المحمي تقنيا أو إزالة أو حذف عنصر مادي من الكمبيوتر محل الجريمة لتسهيل عملية الدخول في النظام ، كما قد يتم الدخول في النظام بإجراء عمليات الكترونية كالتلاعب في عين المكان بنظام معطيات او برامجه او إجراء تعديلات فيها بهدف تسهيل عملية الدخول.

---

[1] إبراهيم بلعليات ، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية للنشر والتوزيع، 2007، ص 95.

[2] يسر أنور علي، شرح قانون العقوبات، النظرية العامة، دون طبعة، دار النهضة العربية، القاهرة، مصر، 1998، ص 286.

[3] المادة 394 مكرر من القانون 04-15، سالف الذكر.

**ب- الاتصال المعنوي عن بعد بالنظام المعلوماتي:** ويقصد به الدخول في النظام المعلوماتي محل الجريمة باستعمال وسائل الاتصال عن بعد المستحدثة (الشبكات المعلوماتية أو الالكترونية السلكية أو اللاسلكية)، وفي هذه الحالة لا يشترط حتى تقوم الجريمة ان يكون الجاني موجود في نفس مكان وجود الكمبيوتر محل الجريمة.[1]

ومن خلال ما سبق نصل الى القول بان الجريمة تقوم بمجرد فعل الدخول دون ضرورة حدوث اية نتيجة أخرى، فلا يشترط لقيامها التقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها او استعمال تلك المعلومات، بل أن الجريمة تقوم حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام.[2]

**2- الركن المادي لجريمة البقاء الاحتيالي**

لقد اعتبر المشرع الجزائري البقاء الاحتيالي جريمة بموجب نص المادة 394 مكرر في فقرتها الأولى من قانون العقوبات بقوله " كل من يدخل او يبقى عن طريق الغش في كل او جزء من منظومة للمعالجة الآلية للمعطيات ..."[3]، ويتحقق الركن المادي في جريمة البقاء الاحتيالي إذا اتخذ صورة البقاء داخل النظام ويقصد بفعل البقاء كما سبق وان وضحنا "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام".

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، ويظهر ذلك عندما لا يكون للجاني الحق في الدخول الى النظام ويدخل اليه فعلا ضد ارادة من له الحق في السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق هذا الفرض في الاجتماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام.[4]

وتعتبر هذه الجريمة من الجرائم المستمرة، فالجريمة تستمر كلما زادت مدة البقاء غير المشروع داخل النظام المعلوماتي، كما أن جريمة البقاء الاحتيالي لا يشترط فيها ان تتوافر لدى المجرم نية الاضرار بالنظام المعلوماتي بل يكفي ان يقوم بمجرد البقاء فقط إذا كان غير مشروع، وقد يتسبب المجرم زيادة عن بقائه الغير مشروع في النظام الى الاضرار بهذا الأخير.[5]

---

[1] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999، ص 130.

[2] أمال قارة، مرجع سابق، ض 143.

[3] المادة 394 مكرر من قانون 04-15، سالف الذكر.

[4] علي عبد القادر القهوجي، مرجع سابق، ص 133.

[5] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 18، دارهومة، الجزائر،2019، ص 55.

**ثانيا: الركن المعنوي لجريمة الدخول والبقاء في النظام المعلوماتي**

لا يكفي لقيام الجريمة ارتكاب عمل مادي ينص ويعاقب عليه القانون، بل لابد أن يصدر هذا العمل المادي عن إرادة الجاني، وهذه العلاقة التي تربط العمل المادي بالفاعل تسمى الركن المعنوي[1]، والعلاقة النفسية بين الجاني وماديات الجريمة تتخذ إحدى الصورتين إما القصد الجنائي أو العمد واما الخطأ غير العمدي.

ويتكون القصد الجنائي من عنصري العلم والإرادة ويتحقق متى اتجهت إرادة الجاني إلى فعل الدخول بمحض إرادته وليس على سبيل الصدفة، وكان يعلم بأنه يدخل إلى نظام معلوماتي خاص بالغير، ويمكن للقاضي الجزائي أن يستدل على توافر القصد الجزائي لدى الجاني إذا كان النظام المعلوماتي محاط بنظام أمني وتم اختراقه، وقد يكون القصد عاما أو خاصا، فالقصد الجنائي العام هو الهدف المباشر للسلوك الاجرامي وينحصر في حدود ارتكاب الفعل، أما القصد الخاص فهو الغاية من تحقيق النتيجة. [2]

**1- الركن المعنوي في جريمة الدخول**

الأصل ان الفاعل في جريمة الاعتداء على المعطيات الرقمية يوجه سلوكه إجرامي نحو ارتكاب فعل غير مشروع او غير مسموح به مع علمه وقاصدا ذلك، ومهما يكن لا يستطيع اثبات انتفاء علمه كركن للقصد العام، إذن فالقصد الجنائي العام متوفر في جميع الجرائم المعلوماتية او الالكترونية دون استثناء، ولكن هذا لا يمنع أن بعض الجرائم الالكترونية تتوافر على القصد الجنائي الخاص مثل جريمة تشويه السمعة عبر الانترنت.[3]

**2- الركن المعنوي في جريمة الدخول والبقاء غير المشروع داخل النظام المعلوماتي**

يحتل الركن المعنوي اهمية في قيام جريمة الدخول غير المصرح به الى نظام الكمبيوتر، فالأفعال لتي تقوم عليها هذه الجريمة يقوم بها كل مستخدمو الكمبيوتر، ومن بين هذه الافعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي، كما ان القصد الجنائي يتوافر ولو لم يتوقع الجاني الآثار، فيتعين

[1] عبد الله سليمان، شرح قانون العقوبات، القسم العام، الطبعة الخامسة، ديوان المطبوعات الجامعية، الجزء الأول، الجزائر، 2004، ص 249.

[2] صالح شنين، الحماية الجزائية لبرامج الحاسب الآلي، مذكرة ماجستير في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، السنة الجامعية 2007/2006، ص 91.

[3] خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 260.

اذن ان يتوقع الجاني انه سوف يدخل الى نظام غير مصرح له بالدخول اليه ولا يشترط ان يتوقع الضرر الذي سوف يلحق النظام من جراء هذا الدخول.[1]

كذلك من بين صور الدخول غير المصرح به ان يكون مالك النظام قد وضع قيودا للدخول الى النظام ولم يلتزم الجاني بهذه القيود ، أو كان الأمر يتطلب سداد مبلغ نقدي لم يسدده الجاني وقام بالدخول غير المشروع الى النظام ، ويلاحظ في هذا الصدد ان المشرع الجزائري يعاقب على الدخول المجرد الى النظام المعلوماتي ، فمجرد الدخول تقوم به الجريمة حتى ولو لم يترتب على دخوله ضرر أو يتحقق له من وراء الدخول نفع أو فائدة طالما الدخول غير مشروع.[2]

**الفرع الثاني: اركان جريمة الاعتداء على سير النظام المعلوماتي واتلاف المعلومات**

سنتطرق في هذا الفرع الى كل من الركن المادي وكذا الركن المعنوي لجريمتي الغش المعلوماتي، وكذا جريمة اتلاف المعلومات:

**أولا: الركن المادي لجريمة الاعتداء على سير النظام المعلوماتي واتلاف المعلومات**

**1- الركن المادي لجريمة الاعتداء على سير النظام المعلوماتي**

تعد جريمة الغش المعلوماتي في مجال المعالجة الآلية للمعطيات من أخطر طرق الغش التي تقع في هذا المجال ولاسيما بعد تراجع التعامل بالمحررات والمستندات والوثائق والصكوك الورقية في حين غزت المعاملات الإلكترونية كل المجالات مما زاد من صعوبة اكتشاف وإثبات الغش في هذا المجال، أو هو تغيير الحقيقة في مستند رسمي، ولكن المستند هنا ليس مستندا عاديا بل هي عبارة عن تسجيلات إلكترونية أو محررات إلكترونية.

وقد أشار المشرع الجزائري بخصوص الغش بقوله :.... عن طريق الغش ..... خاصة مع تزايد حجم الإعتداءات الواقعة على المعطيات المخزنة داخل الحاسب الآلي التي تمس الأفراد في حقوقهم وأموالهم وحياتهم الخاصة وأمام تزايد فرص الأشخاص للعبث والتلاعب في معطيات الحاسب بتبديلها وتحويرها

[1] بدرة عمارة، الحماية الجنائية للمعلومات الإلكترونية دراسة في القانون 04-15، مجلة البحوث القانونية والسياسية، جامعة الطاهر مولاي بسعيدة، المجلد 01، العدد 02، 2014، ص 438.

[2] خالد ممدوح، مرجع سابق، ص 260.

بالشكل الذي يفقد الثقة بالتقنية ويمس مراكز الأفراد بات من الواجب بسط الحماية لهذه المعلومات وضمان أمنها وسلامتها من كل تبديل وغش.[1]

ويتمثل الركن المادي لجريمة الغش المعلوماتي في تغيير الحقيقة في محرر معلوماتي بإحدى الطرق التي نص عليها القانون، ومن هنا والقيام هاته الجريمة لا بد من إحداث تغيير من شأنه أن يسبب ضرر بتوافر ثلاثة عناصر أساسية:

**أ- وجود محرر:** وهو من اهم العقبات التي واجهت تطبيق هذا النص لهذا اعتبر البعض برنامج الكمبيوتر المضغوط على اقراص مرنة أو غيرها محررا.

**ب- تغيير الحقيقة:** ويتضمن ذلك تغير الحقيقة وابدالها بما يغايرها ولا يعتبر تغيرا للحقيقة اي اضافة المضمون المحرر طالما ظل مضمون المحرر على حالته قبل الاضافة او الحذف.

**ج- الضرر:** يعتبر الضرر عنصرا جوهريا في جريمة الغش المعلوماتي ولا يشترط وقوعه بالفعل بل يكفي احتمالية وقوعه.[2]

**2- الركن المادي لجريمة إتلاف المعلومات**

قد يتخذ الركن المادي لجريمة إتلاف المعلومات إما صورة إجراء تعديلات غير مشروعة لها، أو تدميرها أو الإدخال غير المشروع للمعلومات داخل أنظمة الحاسبات الآلية:

**أ- فعل الإدخال:** هو إضافة معطيات جديدة على الدعامة الخاصة بها سواء خالية أو يوجد عليها معطيات من قبل، وقد يكون بإدخال معطيات وهمية إلى النظام المعلوماتي بقصد التشويش على صحة البيانات القائمة.[3]

**ب- تدمير المعلومات:** يعد تدمير المعلومات بدوره صورة من صور الإتلاف وإن كان أبعد أثار من مجرد إجراء بعض التعديلات للمعلومات[4] ويتم ذلك من خلال ما يلي:

---

[1] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2004، ص 107.

[2] مسعود خثير، الحماية الجنائية (لبرامج الكومبيوتر أساليب وثغرات)، دار الهدى، الجزائر، 2010، ص 135.

[3] غنية باطلي، الجريمة الالكترونية (دراسة مقارنة)، الدار الجزائرية، الجزائر، 2015، ص 174.

[4] خالد ممدوح ابراهيم، مرجع سابق، ص 419.

– **فعل المحو أو الإزالة:** يقصد به إزالة كل أو جزء من المعطيات الموجودة داخل النظام أو نقل وتخزين المعطيات إلى المنطقة الخاصة بالذاكرة، ويعتبر المحو جريمة إتلاف طالما وقع ثمة إتلاف أو تخريب للشيء موضوع الجريمة وتعطيله أيا كانت الوسيلة المستخدمة.

– **فعل التعديل:** يقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، وقد يكون عن طريق المصيدة أو المداخل المميزة التي هي عبارة عن ممرات خالية يمكن من خلالها الولوج الى التعليمات المخزنة ومن ثمة التوصل الى الشفرات والتعليمات[1]، وقد ترتكب هذه الجريمة من قبل أشخاص معينين كان يكون المسؤول عن المعالجة هو مرتكب الجريمة نفسه او المعالج من الباطن هو الذي قام بارتكاب الجريمة.[2]

**ثانيا: الركن المعنوي لجريمة الاعتداء على سير النظام المعلوماتي واتلاف المعلومات**

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي، فيجب ان تتجه إرادة الجاني إلى فعل الإدخال أو الإزالة أو التعديل مع علمه بأن نشاطه يترتب عليه اعتداءا على المعطيات، وأنه ليس له الحق في القيام بذلك دون إذن من صاحب الحق في السيطرة على تلك المعطيات[3]، وفيما يلي سنوضح ذلك بشيء من التفصيل:

**1- في جريمة الاعتداء على سير النظام المعلوماتي**

نصت المادة 394 مكرر 5 من قانون العقوبات على " كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد الجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان التحضير مجسدا بفعل أو عدة أفعال مادية ...[4]، لذلك تعتبر جريمة الاعتداء في هذا القسم على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية لأن أفعال الاعتداء المتمثلة في أفعال العرقلة و التعطيل تعد من الأفعال

[1] صالح شنين، مرجع سابق، ص 96.

[2] عائشة بن قارة مصطفى، آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم 18/07، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، 2019، ص 746.

[3] بدرة عمارة، مرجع سابق، ص 444.

[4] المادة 394 مكرر 5 من القانون 04-15، سالف الذكر.

العمدية، و هذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يعتبره ظرف مشددا الجريمة الدخول والبقاء غير المشروع داخل النظام، وعليه فالقصد الجنائي المفروض يتضمن طبيعة الافعال المجرمة.[1]

وجريمة الاعتداءات العمدية على المعطيات يتخذ فيها القصد الجنائي بعنصريه العلم والإرادة ، فيجب أن تتجه إدارة الجاني إلى فعل الإدخال أو المحو أو التعديل ، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ، ويعلم أيضا أنه ليس له الحق في القيام بذلك ، وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته، ويشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي نية الاعتداء لكن هذا لا يعني ضرورة توافر قصد الاضرار بالغير ، بل تتوافر الجريمة و يتحقق ركنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك وان كان الضرر قد يتحقق في الواقع او اتجاه الإرادة اليه وان كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة .

**2- في جريمة إتلاف المعلومات**

يشترط لقيام هذه الجريمة توافر القصد العام فيكفي هذا القصد لثبوت علم الجاني بأن الأموال التي يتعدى عليها بالإتلاف هي ملك للغير وأن فعله من شأنه أن يتلف الشيء أو يجعله معطل أو يجعله غير صالح للاستعمال أو ينقص قيمته، ويجب أيضا أن تتجه إرادة الجاني إلى إحداث الإتلاف أو التخريب أو التعطيل وينتج عن فعله تحقق الضرر المترتب على جريمته مع علمه أن فعله غير شرعي.

وفعل الإتلاف يتطلب وجود القصد الجنائي و يكفي قيام القصد العام في اتجاه نية الجاني إلى إتلاف الأموال الثابتة أو المنقولة و يتطلب علم الجاني بأن فعله يؤدي إلى إتلاف أموال مملوكة للغير، فإن عدم العلم هنا ينفي القصد الجنائي ، و يجب أيضا اتجاه الإرادة للفعل الذي يؤدي إلى الإتلاف ، لأن الجريمة عمدية ففي الجريمة المتعلقة بإعاقة سير نظام معلوماتي أو الجريمة المتعلقة بالاعتداء على المعلومات الموجودة داخل الجهاز تتجه إرادة الجاني إلى إتلاف المال وذلك بالقيام بوضع برنامج من شأنه أن يغير المعلومات أو يقوم بمحو البيانات فمن يعمل هذا العمل الإجرامي فهو على درجة عالية من الناحية التقنية في مجال المعلوماتية ، وبناء على ذلك فهو يعلم بالفعل بأن هذه الأموال المعلوماتية التي تتجه إرادته إلى إتلافها مملوكة للغير فإن القصد الجنائي يكون متوفرا وتقوم الجريمة المنصوص عليها باكتمال أركانها أما

[1] أمال قارة، مرجع سابق، ص 125.

لو كان الإتلاف ناتج عن حادث غير مقصود كما لو وقع شيء من العامل أو الموظف على الجهاز أدى إلى إتلاف جزء منه فلا تقوم جريمة الإتلاف العمدي التي تسبب عنها اعاقة النظام المعلوماتي.[1]

[1] خالد ممدوح ابراهيم، مرجع سابق، ص 421.

**خلاصة الفصل:**

من خلال ما تم تناوله في هذا الفصل، يتضح أن النظم المعلوماتية أصبحت تمثل حجر الزاوية في بناء المجتمع الرقمي، لما تؤديه من دور محوري في معالجة وتخزين وتبادل المعلومات، وقد استدعى ذلك ضرورة الإحاطة بمفهومها وخصائصها، حيث تبين أنها تتميز بطبيعة تقنية معقدة وخصوصية تجعلها أكثر عرضة لمختلف أشكال الاعتداء.

كما تم إبراز مفهوم الحماية الجنائية باعتبارها وسيلة قانونية أساسية تهدف إلى صون هذه النظم من الأفعال غير المشروعة، من خلال تجريم السلوكات التي تمس بها وفرض عقوبات رادعة على مرتكبيها، وهو ما يعكس أهمية تدخل القانون الجنائي لحماية البيئة الرقمية وضمان الأمن المعلوماتي.

وفي السياق ذاته، تم التطرق إلى الجرائم الماسة بالنظم المعلوماتية، حيث تبين أنها تتخذ صورًا متعددة، تتراوح بين البسيطة والمشددة، بحسب خطورة الفعل والنتائج المترتبة عنه، كما تم تحليل أركان هذه الجرائم، خاصة جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي، باعتبارها من أكثر الجرائم شيوعًا، والتي تقوم على توافر الركن المادي والمعنوي وكذا الركن الشرعي.

وعليه، يمكن القول إن الحماية الجنائية للنظم المعلوماتية تشكل ضرورة حتمية لمواكبة التطور التكنولوجي المتسارع، غير أن فعاليتها تظل مرتبطة بمدى تحديث التشريعات وتكييفها مع المستجدات التقنية، إضافة إلى تعزيز الوعي القانوني والتقني لمواجهة مختلف التهديدات الإلكترونية.

# الفصل الثاني

# الفصل الثاني:

# آليات الحماية الجنائية للنظم المعلوماتية في التشريع الجزائري.

أدى التطور السريع لتكنولوجيات الإعلام والاتصال إلى بروز تحديات جديدة مست مختلف جوانب الحياة، خاصة في ظل تزايد الاعتماد على النظم المعلوماتية في إدارة المعاملات والبيانات والخدمات المختلفة. وقد نتج عن هذا التطور ظهور أنماط حديثة من الإجرام تستهدف الأنظمة المعلوماتية والمعطيات الإلكترونية، الأمر الذي حتم على المشرع الجزائري إلى إيجاد إطار قانوني يهدف إلى توفير الحماية الجنائية لهذه النظم، من خلال سن قواعد موضوعية وإجرائية تتلاءم مع طبيعة الجرائم المعلوماتية المرتكبة وخصوصيتها.

وتقتضي الحماية الجنائية للنظم المعلوماتية اعتماد مجموعة من التدابير الوقائية والعقوبات الردعية، إلى جانب وضع إجراءات خاصة بالمتابعة والتحقيق تتناسب مع الطابع التقني لهذه الجرائم، فضلاً عن تعزيز التعاون الوطني والدولي باعتبار أن الجرائم المعلوماتية غالباً ما تتجاوز الحدود الإقليمية للدول، ومن هذا المنطلق سنتناول في هذا الفصل السبل الجنائية والجزاءات المقررة لحماية النظم المعلوماتية في المبحث الأول، ثم سنتطرق إلى الإطار الإجرائي والتعاون في مكافحة جرائم النظم المعلوماتية في المبحث الثاني.

## المبحث الأول:

## السبل الجنائية والجزاءات المقررة لحماية النظم المعلوماتية

تُعد الحماية الجنائية للنظم المعلوماتية ضرورة حتمية في ظل التطور التكنولوجي المتسارع وما يواكبه من تزايد في المخاطر والتهديدات الإلكترونية، فمع الاعتماد المتزايد على النظم المعلوماتية في مختلف مجالات الحياة – الاقتصادية والإدارية والاجتماعية – أصبحت هذه النظم تشكل العمود الفقري للمجتمع الرقمي، مما يجعل أي اعتداء عليها يشكل تهديداً مباشراً لاستقرار المجتمع وأمنه المعلوماتي.

وقد أدرك المشرع الجزائري هذه الحقيقة، فسعى إلى إرساء منظومة قانونية متكاملة تجمع بين التدابير الوقائية التي تهدف إلى منع وقوع الاعتداءات على النظم المعلوماتية، والعقوبات الزجرية التي تهدف إلى ردع المعتدين وتأمين الحماية اللازمة لهذه النظم، وتتجلى أهمية هذه المنظومة في كونها تساهم في تعزيز الثقة في البيئة الرقمية، سواء بالنسبة للأفراد أو المؤسسات، حيث أن الشعور بوجود حماية قانونية فعالة يشجع على استخدام الوسائل الإلكترونية في المعاملات المختلفة.

ويتناول هذا المبحث السبل الجنائية والجزاءات المقررة لحماية النظم المعلوماتية في التشريع الجزائري، من خلال تقسيمه إلى مطلبين رئيسيين: يتناول المطلب الأول التدابير الوقائية في مجال حماية النظم المعلوماتية، في حين يخصص المطلب الثاني لدراسة العقوبات الجنائية المقررة لجرائم النظم المعلوماتية.

### المطلب الأول:

### التدابير الوقائية في مجال حماية النظم المعلوماتية

تمثل التدابير الوقائية الركيزة الأساسية في أي استراتيجية فعالة لحماية النظم المعلوماتية، فهي تهدف إلى منع وقوع الاعتداءات قبل حدوثها، وذلك من خلال وضع إطار قانوني وتنظيمي يلزم مختلف الأطراف المعنية باتخاذ الاحتياطات اللازمة لضمان أمن وسلامة هذه النظم[1]، وقد أثبتت التجارب العملية أن الوقاية خير من العلاج، وأن توفير الحماية الاستباقية للنظم المعلوماتية أقل تكلفة وأكثر فعالية من اللجوء إلى الردع الجنائي بعد وقوع الضرر.[2]

[1] إبراهيم بلعليات ، مرجع سابق، ص 95.

[2] علي عبد القادر القهوجي، مرجع سابق، ص ص 130-131.

وقد أدرك المشرع الجزائري أهمية هذه المقاربة الوقائية، فأسس لنظام وقائي متكامل يتضمن مجموعة من التدابير القانونية والتنظيمية، إلى جانب تدابير تقنية وإدارية، وذلك سعياً منه إلى توفير الحماية الاستباقية للنظم المعلوماتية قبل اللجوء إلى الردع الجنائي، كما تجدر الإشارة إلى أن المقاربة الوقائية في التشريع الجزائري لم تقتصر على الجانب التقني فقط، بل امتدت لتشمل الجوانب المؤسسية والتنظيمية، مما يعكس رؤية شاملة لمشكلة الجرائم المعلوماتية.[1]

وفي هذا الإطار، سيتم تقسيم هذا المطلب إلى فرعين: يتناول الفرع الأول التدابير التشريعية والتنظيمية لحماية النظم المعلوماتية، في حين يخصص الفرع الثاني للتدابير التقنية والإدارية في هذا المجال.

**الفرع الأول: التدابير التشريعية والتنظيمية لحماية النظم المعلوماتية**

تشكل التدابير القانونية والتنظيمية الإطار المؤسسي والتشريعي الذي تعمل من خلاله آليات الحماية الوقائية للنظم المعلوماتية، وقد حرص المشرع الجزائري على وضع نصوص قانونية واضحة تحدد الالتزامات والمسؤوليات المختلفة في هذا المجال، مع إنشاء هيئات متخصصة تتولى الإشراف على تنفيذ هذه التدابير، وتتميز هذه التدابير بأنها تضع الأسس القانونية التي تستند إليها جميع الجهود الوقائية الأخرى، سواء كانت تقنية أو إدارية.[2]

وسيتم تناول هذا الموضوع من خلال نقطتين رئيسيتين: التدابير القانونية للوقاية من الجرائم المعلوماتية ومكافحتها، ثم دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

**أولاً: التدابير التشريعية للوقاية من الجرائم المعلوماتية ومكافحتها**

لقد أسس المشرع الجزائري لنظام وقائي متكامل في مجال حماية النظم المعلوماتية، وذلك من خلال مجموعة من النصوص التشريعية التي تهدف إلى تحقيق الوقاية قبل اللجوء إلى الردع الجنائي، وتتصدر هذه النصوص القواعد الخاصة المنصوص عليها في القانون رقم 09-04 المؤرخ في 5 غشت 2009.

---

[1] رمزي حوحو، مرجع سابق، ص 196.

[2] زكرياء ذيب، تجريم الاعتداء على نظم المعالجة الآلية للمعطيات التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، المجلد 7، العدد 2، جامعة عمار ثليجي، الأغواط، 2023، ص 1302.

**1- القانون رقم 09-04 كمرجع أساسي للوقاية**

يُعد القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المرجع الأساسي في مجال الوقاية من الجرائم المعلوماتية في الجزائر[1].

فقد جاء هذا القانون ليكمل النصوص العقابية الواردة في قانون العقوبات، حيث ركز على الجانب الوقائي والإجرائي في مكافحة الجرائم المعلوماتية، كما صدر هذا القانون استجابة للحاجة الملحة إلى تنظيم قانوني يواكب التطورات التكنولوجية المتسارعة ويوفر إطاراً قانونياً مناسباً لمكافحة الجرائم المستحدثة.

يتضمن هذا القانون جملة من التدابير الوقائية التي تهدف إلى تعزيز أمن النظم المعلوماتية، من أبرزها:

- إلزام مختلف المتعاملين في مجال تكنولوجيات الإعلام والاتصال بوضع الترتيبات التقنية اللازمة لحماية الأنظمة المعلوماتية.
- تنظيم إجراءات المراقبة الإلكترونية وحفظ المعطيات الرقمية، مع وضع ضمانات قوية لحماية الحق في الخصوصية.
- إنشاء هيئة وطنية متخصصة في الوقاية من هذه الجرائم ومكافحتها، تكون مهمتها وضع وتنفيذ السياسات الوطنية في هذا المجال.
- تحديد التزامات مقدمي خدمات الإنترنت في مجال التعاون مع السلطات القضائية والأمنية، بما في ذلك حفظ البيانات والإفصاح عنها عند الطلب.
- وضع آليات للتعاون الوطني والدولي في مجال مكافحة الجرائم المعلوماتية[2].

**2- مساهمة قانون العقوبات في الحماية الوقائية**

ساهم قانون العقوبات الجزائري، لاسيما بعد التعديلات التي أدخلت عليه بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، في تعزيز الحماية الوقائية من خلال تجريم الأفعال التحضيرية للجرائم المعلوماتية، فقد نصت المادة 394 مكرر 5 من قانون العقوبات على أنه: "كل من شارك في

[1] القانون رقم 09-04 المؤرخ في5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 49، الصادر في 16 عشت 2009، ص 5.

[2] المواد من 11 الى 15، نفس المرجع.

مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان التحضير مجسدا بفعل أو عدة أفعال مادية.... ".[1]

ويمثل هذا النص يمثل انتقالاً بالحماية الجنائية من مرحلة الردع على الجريمة التامة إلى مرحلة الوقاية من خلال تجريم الأفعال التحضيرية، وهو ما يعكس توجه المشرع نحو تعزيز المقاربة الوقائية في مجال حماية النظم المعلوماتية[2]، فبموجب هذا النص أيضا، يمكن توقيع العقاب على المجرمين حتى قبل أن يتمكنوا من تنفيذ مخططهم الإجرامي، مما يشكل رادعاً قوياً ووسيلة فعالة لتفويت الفرصة على المجرمين قبل أن يتسببوا في أضرار جسيمة.

وتكمن أهمية هذا التوجه في أن الجرائم المعلوماتية غالباً ما تتطلب تحضيرات معقدة وتخطيطاً مسبقاً، مما يجعل تجريم هذه الأفعال التحضيرية وسيلة فعالة للتدخل المبكر ومنع وقوع الضرر لا يمكن تداركها لاحقا.

**3- القانون رقم 18-07 ودوره في الحماية الوقائية:**

كما ساهم القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في تعزيز الحماية الوقائية للنظم المعلوماتية، وذلك من خلال إلزام كل شخص أو هيئة تقوم بمعالجة المعطيات ذات الطابع الشخصي باتخاذ جميع الاحتياطات الأمنية اللازمة لحماية هذه المعطيات من أي انتهاك أو إتلاف أو تغيير غير مشروع.[3]

وقد نصت المادة 33 من هذا القانون على أن: "يجب على كل شخص أو هيئة يقومون بمعالجة معطيات ذات طابع شخصي أن يتخذوا كل الاحتياطات الأمنية اللازمة لحماية هذه المعطيات، خاصة من أن يناط بها أو يتلفها أو يغيرها شخص غير مخول"، ويعد هذا النص تجسيداً لمبدأ المسؤولية الوقائية التي

[1] المادة 394 مكرر 5 من القانون رقم 04-15، سالف الذكر.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 265.

[3] القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد 36، الصادر بتاريخ 10 يونيو2018، ص 11.

تهدف إلى تجنب وقوع الضرر قبل حدوثه، حيث يتحمل القائمون على معالجة المعطيات مسؤولية توفير الحماية اللازمة لهذه المعطيات. [1]

كما أضاف هذا القانون بعداً جديداً للحماية الوقائية، من خلال إلزام المسؤولين عن معالجة المعطيات الشخصية بإشعار السلطات المختصة في حالة حدوث أي خرق أمني يمس بهذه المعطيات، مما يسمح باتخاذ الإجراءات اللازمة للحد من الآثار السلبية لهذا الخرق.

**4- القانون 25-11 المؤرخ في 24 يوليو 2025**

أتى هذا القانون ليعدل ويتمم هذا القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، إذ يتكون من ستة فصول وثمانية مواد تنصب كلها في إطار حماية المعطيات ذات الطابع الشخصي من خلال تحديد مفهوم المعطيات البيومترية وتحديد سمات الشخصية واستخدام اسم مستعار، والسلطة المختصة، وانتهاك المعطيات ذات الطابع الشخصي والمنظمة الدولية.[2]

كما استحدثت صفة مندوب حماية المعطيات ذات الطابع الشخصي في الفصل الأول مكرر من خلال مادتين 41 مكرر و41 مكرر 01، حيث تناولت المادة 41 مكرر تعيين المندوب ودوره التنسيقي، كما تناولت المادة 41 مكرر 02 مهامه بدقة.[3]

وقد استحدثت أيضا بموجب هذا القانون وتحت الفصل الأول مكرر 01 دفاتر وسجلات المعالجة وحدد شكلها ووصفها والآجال المتعلقة بالعمليات في هذا الإطار من خلال مادتين 41 مكرر 02 و41 مكرر 03.[4]

كما استحدث الباب الخامس مكرر والذي يتكون من ستة فصول تناولت على التوالي:

---

[1] المادة 33 من القانون رقم 18-07، سالف الذكر.

[2] المادة 02 من القانون رقم 25-11 المؤرخ في 24 يوليو 2025، يعدل ويتمم القانون 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، الصادر بتاريخ 24 يوليو 2025، ص 14.

[3] المادة 04، نفس المرجع.

[4] المادة 05، نفس المرجع.

– المبادئ الأساسية، التزامات المسؤول عن المعالجة، حقوق الشخص المعني، دراسة أثر المعالجة وطرق المعطيات ذات الطابع الشخصي.[1]

**5- القانون 26-02 المؤرخ في 17 فيفري 2026**

أتى القانون 26-02 المحدد القواعد العامة المتعلقة بخدمات الثقة للعلامات الإلكترونية وبالتعريف الإلكتروني، ليلغي القانون رقم 15-04 المؤرخ في الأول من فبراير سنة 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، حيث احتوى على ستة أبواب وبمجموع 116 مادة مما يعطي انطباعا على أنه ترسانة قانونية قوية.[2]

بحيث تناول هذا القانون أيضا أحكاما عامة بموجب الباب الأول المتضمن ثلاثة مواد تحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، كما قدمت المادة 02 منه مفهوما شاملا لهذا القانون عبر 33 نقطة، في حدد المادة 03 منه مجال تطبيقه والمتمثل في الأشخاص الطبيعيين والمعنويين الذين يستخدمون المعاملات الإلكترونية و/أو خدمات الثقة بالإضافة إلى المعاملات الإلكترونية والوثائق الإلكترونية وخدمات الثقة والإجراءات اللازمة لتنفيذها.[3]

أما الباب الثاني المعنون تحت عنوان تزويد خدمات الثقة فقد احتوى على ثلاثة فصول تناول بموجب الفصل الأول خدمات الثقة والفصل الثاني مزودو خدمات الثقة، الفصل الثالث السلطة الوطنية للتصديق الإلكتروني.[4]

كما ورد الباب الثالث بعنوان الوثائق الإلكترونية والتي احتوت علة أربعت فصول على النحو التالي:

الكتابة والتوقيع والختم والعقد الإلكتروني، الحفظ والشكل الأصلي وحجية الوثائق الإلكترونية، الإسناد، الإقرار بالاستلام ووقت استلام الوثيقة الإلكترونية.[5]

---

[1] المادة 05، القانون رقم 25-11، سالف الذكر.

[2] القانون 26-02 المؤرخ في 17 فبراير 2026، يحدد القواعد العامة المتعلقة بخدمات الثقة للعلامات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية، العدد 14، الصادر بتاريخ 18 فبراير 2026، ص 06.

[3] المواد من 01 إلى 03، نفس المرجع.

[4] المواد من 04 إلى 52، نفس المرجع.

[5] المواد من 53 إلى 71، نفس المرجع.

وقد تناول المشرع الجزائري وفقا للباب الرابع من هذا القانون التعريف الالكتروني والذي أتى على شكل 06 مواد قانونية حدد بموجبها هدفه ودرجاته، والهيئة المكلفة بظبط المعايير والشروط في هذا الإطار لإنتاج أثارها القانونية.[1]

**6- الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية**

أدت سياسة الحوكمة في الجزائر لاستعمال الرقمنة على كافة المستويات إلى تبني زاوية استراتيجية وتجلى ذلك من خلال المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي سنة 2020 وذلك بخلق منظومة وطنية لأمن الأنظمة المعلوماتية وهذا من أجل استباق المواقف، وتحديد النقائص ونقاط الضعف وفهم الأسباب لأجل وضع إجراءات ممكنة الغرض منها رفع الفعالية لمواجهة التهديدات السيبرانية المحيطة.[2]

وقد تناولت هذه الاستراتيجية الرؤية المستقبلية والمبادئ التوجيهية بالإضافة إلى أربعة محاور هامة مقسمة كالتالي:

- القدرات التقنية العملياتية
- الإطار القانوني والتنظيمي والمعياري
- التكوين والبحث والتطوير والتحسيس
- التعاون الوطني والدولي.[3]

**7- التزامات المؤسسات والهيئات العمومية**

لم يقتصر التنظيم التشريعي للوقاية على القوانين العامة، بل امتد ليشمل نصوصاً خاصة تلزم المؤسسات والهيئات العمومية باتخاذ تدابير وقائية محددة، فقد نص القانون التوجيهي للمؤسسات العمومية على ضرورة توفير أنظمة معلوماتية آمنة، كما ألزمت التعليمة الوزارية المشتركة المؤرخة في 2019 جميع المؤسسات العمومية بوضع مخططات لأمن الأنظمة المعلوماتية. [4]

---

[1] المواد من 72 إلى 77، من القانون 26-02، سالف الذكر.

[2] الموقع الرسمي لوزارة الدفاع الوطني، على الرابط https://www.mdn.dz/، تاريخ الاطلاع 03 جوان 2025، الساعة 14.25.

[3] نفس المرجع.

[4] عائشة بن قارة مصطفى، مرجع سابق، ص 746.

تهدف هذه الالتزامات إلى إنشاء ثقافة أمنية مؤسسية، حيث تصبح حماية النظم المعلوماتية مسؤولية جماعية تبدأ من القيادة العليا للمؤسسة وتمتد لتشمل جميع العاملين فيها، كما أن هذه الالتزامات تساهم في توحيد المعايير والممارسات الأمنية على المستوى الوطني، مما يسهل عملية التعاون وتبادل المعلومات بين المؤسسات المختلفة. [1]

**ثانياً: التدابير التنظيمية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**

**1- دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**

تُعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ركيزة أساسية في المنظومة الوقائية التي أقامها المشرع الجزائري لحماية النظم المعلوماتية، وقد تم إنشاء هذه الهيئة بموجب أحكام القانون رقم 09-04 المشار إليه سابقاً[2]، ثم تحدد تنظيمها وتشكيلها عبر عدة مراسيم كان آخرها المرسوم الرئاسي رقم 21-439[3] وذلك بهدف توفير إطار مؤسسي متخصص يتولى مكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال من خلال مجموعة من التدابير، سواء كانت وقائية أو عقابية.

**أ. طبيعة الهيئة القانونية وتنظيمها**

تتمتع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بشخصية معنوية واستقلال مالي، وهي هيئة إدارية وطنية تهدف إلى تعزيز أمن الفضاء الإلكتروني الوطني[4]، وقد تم تحديد تشكيلتها وتنظيمها بموجب المرسوم الرئاسي رقم 21-439 المؤرخ في 11 نوفمبر 2021، الذي نص على أن الهيئة تتكون من أعضاء يمثلون مختلف القطاعات المعنية بأمن الأنظمة المعلوماتية.[5]

---

[1] التعليمة الوزارية المشتركة رقم 01/2019 المؤرخة في 15 جانفي 2019، المتعلقة بوضع مخططات أمن الأنظمة المعلوماتية في المؤسسات العمومية، وزارة البريد وتكنولوجيات الإعلام والاتصال، 2019.

[2] المادة 13 من القانون رقم 09-04، سالف الذكر.

[3] المرسوم الرئاسي رقم 21-439 المؤرخ في 11 نوفمبر 2021، المحدد لتشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 73، الصادر بتاريخ 11 نوفمبر 2021، ص 5.

[4] المادة 2، نفس المرجع.

[5] المادة 3، نفس المرجع.

تتميز الهيئة بطابعها المتخصص، حيث تضم في تشكيلتها خبراء في مجال تكنولوجيات الإعلام والاتصال، وقانونيين، وممثلين عن مختلف الهيئات الأمنية والقضائية، مما يمكنها من القيام بمهامها على أكمل وجه، كما أن استقلالها المالي والإداري يضمن لها القدرة على العمل بفعالية دون التأثر بالاعتبارات السياسية أو الإدارية الضيقة. [1]

**ب. الاختصاصات الوقائية للهيئة**

تتمثل المهمة الأساسية للهيئة في مكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال من خلال مجموعة من الاختصاصات، وتنقسم هذه الاختصاصات إلى نوعين: اختصاصات وقائية واختصاصات رقابية وقمعية.[2]

في مجال الاختصاصات الوقائية، تتولى الهيئة وضع وتنفيذ السياسات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتشمل هذه المهام:

- اقتراح التدابير القانونية والتقنية اللازمة لحماية الأنظمة المعلوماتية، سواء على المستوى الوطني أو القطاعي.
- إعداد الدراسات والأبحاث المتعلقة بمخاطر الجرائم المعلوماتية وسبل مكافحتها، ونشر الوعي بهذه المخاطر.
- تنظيم حملات التوعية والتحسيس بمخاطر الاستخدام غير الآمن لتكنولوجيات الإعلام والاتصال، واستهداف مختلف فئات المجتمع.

تقديم الاستشارات والمساعدة التقنية للمؤسسات والأفراد في مجال أمن الأنظمة المعلوماتية، ومساعدتهم على تطوير قدراتهم في هذا المجال.[3]

**ج. الاختصاصات الرقابية والقمعية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**

أما في مجال الاختصاصات الرقابية والقمعية، فتساهم الهيئة في:

---

[1] المادة 4 من المرسوم الرئاسي رقم 21-439، سالف الذكر.

[2] المادة 13 من المرسوم الرئاسي رقم 21-439، نفس المرجع.

[3] نفس المرجع.

- تلقي البلاغات والشكاوى المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتحقق من جديتها.
- إجراء التحريات الأولية حول هذه الجرائم بالتنسيق مع مصالح الضبطية القضائية، وجمع الأدلة اللازمة.
- تقديم المساعدة التقنية للسلطات القضائية في إطار التحقيقات المتعلقة بالجرائم المعلوماتية، والإدلاء بالخبرة الفنية اللازمة.
- إعداد تقارير دورية حول حالة الجريمة المعلوماتية في الجزائر، ورفعها إلى السلطات العليا. [1]

**د. التنسيق مع السلطات الأمنية والقضائية**

تلعب الهيئة الوطنية دوراً محورياً في تنسيق الجهود بين مختلف الأطراف المعنية بمكافحة الجرائم المعلوماتية، فهي تعمل بتعاون وثيق مع:

السلطات القضائية، من خلال تقديم الخبرة التقنية والمساندة في مجال التحقيقات المتعلقة بالجرائم المعلوماتية، والإدلاء بالرأي الفني في القضايا المعروضة عليها.

- مصالح الأمن الوطني والدرك الوطني، من خلال تبادل المعلومات والخبرات والتنسيق في عمليات التحري والمراقبة، والمشاركة في التدريبات والمحاكاة الأمنية.
- سلطة ضبط البريد والاتصالات الإلكترونية(ARPCE) ، من خلال تطوير آليات المراقبة التقنية وحفظ المعطيات الرقمية، ووضع المعايير الأمنية اللازمة.[2]

حيث أن لهذه الهيئة صلاحية التعاون مع مختلف الهيئات القضائية والأمنية، كما يجوز لها وضع ترتيبات تقنية إلكترونية قد تصل إلى اعتراض الرسائل أو تسجيل المعطيات الشخصية، وذلك في إطار مكافحة الجرائم الإرهابية أو التخريبية والماسة بأمن الدولة، ويُشترط لممارسة هذه الصلاحيات أن تتم بإذن قضائي مسبق، وأن تخضع للرقابة القضائية، وذلك حماية للحقوق والحريات الفردية.[3]

[1] المادة 14 و15 من القانون رقم 09-04، سالف الذكر.

[2] المادة 17 و18، نفس المرجع.

[3] المادة 18 فقرة 2، نفس المرجع.

**هـ. الإطار المؤسسي للهيئة وآليات عملها**

تساهم الهيئة الوطنية أيضاً في التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، حيث تعمل كنقطة اتصال وطنية لتبادل المعلومات والخبرات مع الهيئات المماثلة في الدول الأخرى ومع المنظمات الدولية المتخصصة.[1]

كما تقوم الهيئة بإعداد تقارير سنوية عن نشاطها ونتائج أعمالها، تُرفع إلى رئيس الجمهورية والحكومة، وتُنشر في الجريدة الرسمية. وتتضمن هذه التقارير إحصائيات حول الجرائم المعلوماتية، وتحليلاً لاتجاهاتها، ومقترحات لتطوير السياسات الوقائية.[2]

لقد مثل إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نقلة نوعية في سياسة المشرع الجزائري لمكافحة الجرائم المعلوماتية، حيث انتقل من المقاربة الردعية التقليدية إلى مقاربة شاملة تجمع بين الوقاية والردع، مع إيلاء أهمية خاصة للجانب الوقائي والاستباقي.

**و. تقييم أداء الهيئة والتحديات التي تواجهها**

على الرغم من النجاحات التي حققتها الهيئة منذ إنشائها، إلا أنها تواجه بعض التحديات التي تحد من فعاليتها، من أبرز هذه التحديات:

- محدودية الموارد البشرية والمالية، خاصة في ظل تزايد حجم الجرائم المعلوماتية وتعقيدها.
- صعوبة مواكبة التطور التكنولوجي المتسارع، مما يتطلب استثمارات كبيرة في التكوين والتجهيز.
- التحديات القانونية المرتبطة بموازنة متطلبات الأمن المعلوماتي مع حماية الحقوق والحريات الأساسية، خاصة الحق في الخصوصية.
- الحاجة إلى تعزيز التعاون الدولي، خاصة مع تزايد الطابع العابر للحدود للجرائم المعلوماتية.[3]

[1] المادة 19 من القانون رقم 09-04، سالف الذكر.

[2] المادة 20، نفس المرجع.

[3] قلات سومية، مرجع سابق، ص 92.

**2- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**

إن أبرز ما جاء به القانون رقم 18-07 المؤرخ في 10 جوان 2018 هو إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كهيئة مستقلة تتمع بالشخصية المعنوية والاستقلال المالي والإداري وتعتبر من ضمن الهيئات التنظيمية ذات الطابع الضبطي والرقابي من خلال إشرافها على الفاعلين العموميين والخواص بالأحكام القانونية ذات الصلة بحماية المعطيات الشخصية.[1]

أ- **التشكيلة:** تتشكل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من 16 عضوا من بينهم الرئيس يتم تعيينهم بموجب مرسوم رئاسي لعهدة مدتها 05 سنوات قابلة للتجديد يؤدون اليمين القانونية قبل مزاولتهم لنشاطاتهم كما يختارون حسب اختصاصاتهم القانونية أو التقنية كل حسب مجاله.[2]

**ب- أهمية السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**

إن مبررات وجود سلطة وطنية مستقلة يعكس التزام الجزائر بمواكبة التطورات العالمية في مجال حماية المعطيات ذات الطابع الشخصي والمساهمة في حركة دورية تهدف إلى تعزيز سيادة الأفراد على معطياتهم الشخصية وحمايتها من الاعتداءات الإلكترونية التي تهددها.[3]

**3- القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولجيات الإعلام والاتصال**

يمثل القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولجيات الإعلام والاتصال آلية قانونية مستحدثة لمكافحة الجريمة الإلكترونية، إذ يجمع بين الخبرة والتخصص القضائي، ويهدف إلى معالجة القضايا ذات الطابع التقني المعقد اعتمادا على كفاءات بشرية مكونة ومتخصصة، ووسائل تقنية متطورة.[4]

---

[1] الموقع الرسمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، على الرابط https://anpdp.dz/ar/ ، تاريخ الاطلاع 03 جوان 2025، الساعة 15.00.

[2] نفس المرجع.

[3] نفس المرجع.

[4] السعيد بن زهرة، بلقاسم العربي، القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، دراسة في المفهوم والاختصاص، مجلة الدراسات القانونية والاقتصادية، المجلد 08، العدد 02، 2025، ص 603.

أ- **النشأة:** تم استحداث القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولجيات الإعلام والاتصال بموجب الأمر 20-05 لغرض مكافحة الجرائم الإلكترونية لغرض مكافحة الجرائم الإلكترونية المرتكبة في البيئة الافتراضية بواسطة الخوادم وأجهزة الكمبيوتر أو الهواتف الذكية

ب- **المقر والاختصاص:** باعتبار أن القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولجيات الإعلام والاتصال جهة قضائية لها اختصاص وطني فهو متواجد بمقر مجلس قضاء الجزائر، حيث يمتد اختصاص القضاة ووكلاء الجمهورية وضباط الشرطة القضائية إلى كافة التراب الوطني عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم الاختراق الإلكتروني، وجرائم الاحتيال والابتزاز عبر الأنترنت.[1]

ج- **أهمية القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولجيات الإعلام والاتصال:** إن تطور الجريمة من خلال التعقيد الذي يميز أساليب ارتكابها، وأشخاصها ووسائلها التقنية

حتم على المشرع تبني آليات حديثة ومحترفة لمواجهتها، ومن خلال ذلك تظهر أهمية القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولجيات الإعلام والاتصال كالتالي:

- الحاجة إلى قضاء متخصص لمكافحة الجرائم الإلكترونية.
- تعزيز الفعالية القضائية لمواجهة الجرائم الرقمية.[2]

**الفرع الثاني: التدابير التقنية والإدارية للوقاية من الجرائم المعلوماتية**

إذا كانت التدابير القانونية والتنظيمية تشكل الإطار المؤسسي والتشريعي للحماية الوقائية، فإن التدابير التقنية والإدارية تمثل الجانب التطبيقي والعملي لهذه الحماية، فهي تهدف إلى تنفيذ الالتزامات القانونية على أرض الواقع، من خلال وضع آليات تقنية وإدارية فعالة تضمن أمن وسلامة النظم المعلوماتية.

وتتعدد هذه التدابير وتتنوع بتنوع طبيعة النظم المعلوماتية ودرجة حساسيتها، ويمكن تصنيفها إلى نوعين رئيسيين: تدابير متعلقة بالمراقبة الإلكترونية وحفظ المعطيات الرقمية، وتدابير متعلقة بدور مزودي خدمات الإنترنت والهيئات التقنية.

[1] السعيد بن زهرة، بلقاسم العربي، مرجع سابق، ص 603.

[2] نفس المرجع، ص 604.

**أولاً: المراقبة الإلكترونية وحفظ المعطيات الرقمية**

تعتبر إجراءات المراقبة الإلكترونية وحفظ المعطيات الرقمية من أهم الركائز التقنية للوقاية من الجرائم المعلوماتية، فقد أدرك المشرع الجزائري أن الطبيعة غير المادية للجرائم المعلوماتية تتطلب آليات تقنية خاصة تمكن من تتبع الأنشطة الإلكترونية المشبوهة والحفاظ على الأدلة الرقمية. [1]

**1- مفهوم المراقبة الإلكترونية وأنواعها:**

المراقبة الإلكترونية هي إجراء تقني يهدف إلى تتبع ورصد الأنشطة الإلكترونية للمستخدمين، وذلك بغرض الكشف عن السلوكيات المشبوهة أو الإجرامية، وقد نظم المشرع الجزائري هذا الإجراء بموجب أحكام القانون رقم 09-04 وقانون الإجراءات الجزائية.

تنقسم المراقبة الإلكترونية إلى نوعين رئيسيين:

- **المراقبة الوقائية** :وهي التي تهدف إلى منع وقوع الجرائم من خلال الكشف المبكر عن الأنشطة المشبوهة، وتتم عادة بشكل استباقي دون أن يكون هناك اشتباه محدد في ارتكاب جريمة.
- **المراقبة القمعية** :وهي التي تتم في إطار تحقيقات قضائية بهدف جمع الأدلة على جرائم وقعت بالفعل، وتكون بناءً على أمر قضائي. [2]

**2- الضمانات القانونية للمراقبة الإلكترونية**

يشترط لممارسة المراقبة الإلكترونية أن تتم بإذن قضائي مسبق، باستثناء الحالات الاستثنائية التي ينص عليها القانون، وهذا الإذن يجب أن يكون كتابياً ومعللاً، وأن يحدد نطاق المراقبة ومدتها، والأشخاص المعنيين بها.[3]

---

[1] المادة 114 من القانون رقم 25-14 المؤرخ في 03 غشت 2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 54، الصادر بتاريخ 13 غشت 2025، ص 7.

[2] إبراهيم بلعليات ، مرجع سابق، ص 100.

[3] غنية باطلي، مرجع سابق، ص 180.

كما يحرر ضابط الشرطة القضائية المكلف بالمراقبة الإلكترونية محضرا عن كل عملية اعتراض وتسجيل المراسلات وعمليات وضع الترتيبات التقنية وكل عملية تتعلق بذلك، كما يقوم بنسخ هذه العمليات أو يضعها على محضر يودع مع الملف مرفقا بالدعامة الإلكترونية إذا طلبها وكيل الجمهورية.[1]

**3- حفظ المعطيات الرقمية**

يُعد حفظ المعطيات الرقمية إجراءً وقائياً ضرورياً لضمان توفر الأدلة في حالة وقوع جريمة معلوماتية، فقد ألزم المشرع الجزائري بموجب القانون رقم 09-04 مقدمي خدمات الإنترنت والاتصالات بحفظ المعطيات المتعلقة بحركة السير (بيانات الاتصال) لفترات زمنية محددة، وذلك بهدف إنشاء سجل إلكتروني يمكن الرجوع إليه في إطار التحقيقات.[2]

تشمل المعطيات الواجب حفظها عادة:

- بيانات تعريف المستخدمين (الاسم، العنوان، رقم الهاتف، البريد الإلكتروني، عنوان IP).
- بيانات الاتصال (التواريخ، الأوقات، المدة، عناوين IP المصدر والوجهة).
- بيانات الموقع الجغرافي للمستخدمين، إن كانت متاحة.
- سجلات الاتصالات والمكالمات، بما في ذلك الأرقام المتصلة والمتصلة بها.[3]

**4- مدة حفظ المعطيات وإجراءات الإفصاح عنها**

تختلف مدة حفظ المعطيات حسب نوعها وأهميتها، حيث تحدد النصوص التنظيمية هذه المدة وفقاً لمعايير موضوعية، وعادة ما تتراوح مدة الحفظ بين سنة وثلاث سنوات، مع إمكانية تمديدها في بعض الحالات الخاصة.

أما بالنسبة للإفصاح عن هذه المعطيات، فلا يمكن لأي جهة الحصول عليها إلا بناءً على إذن قضائي، وذلك باستثناء حالات الخطر الجسيم التي تمس الأمن العام، ويجب أن يكون طلب الإفصاح مسبباً ومحدداً، وأن يقتصر على المعطيات اللازمة للتحقيق.[4]

---

[1] المواد 118، 119 من القانون 25-14، مرجع سابق.

[2] المواد من 14 الى 16 من القانون رقم 09-04، مرجع سابق.

[3] المادة 16، نفس المرجع.

[4] الموقع الرسمي لسلطة ضبط البريد والاتصالات الالكترونية، على الرابط https://www.arpce.dz/ar/about ، تاريخ الاطلاع 01 جوان 2025، الساعة 20.25.

**5- الحفظ والإفشاء العاجلان للمعطيات**

استحدث المشرع الجزائري إجراءً خاصاً يُعرف بـ "الحفظ والإفشاء العاجلان للمعطيات"، وهو إجراء يسمح للسلطات القضائية بأن تأمر مقدمي خدمات الإنترنت بحفظ معطيات معينة بشكل عاجل، أو بالإفصاح عنها فوراً، وذلك في الحالات المستعجلة التي لا تحتمل اتباع الإجراءات العادية.[1]

يتميز هذا الإجراء بسرعته وفوريته، حيث يهدف إلى مواجهة خطر ضياع الأدلة الرقمية بسبب سرعة زوالها أو إمكانية العبث بها، وقد خصص المشرع هذا الإجراء للحالات الخطيرة التي تمس الأمن العام أو تتعلق بجرائم إرهابية. [2]

**6- التحديات التقنية والقانونية**

رغم فعالية هذه الإجراءات، إلا أنها تواجه بعض التحديات:

- **التحديات التقنية** :سرعة تطور وسائل الاتصال والتشفير تجعل من الصعب اعتراض بعض الاتصالات، خاصة تلك التي تستخدم تقنيات التشفير المتقدمة.
- **التحديات القانونية** :التوازن بين متطلبات الأمن وحماية الخصوصية يطرح إشكاليات قانونية معقدة، خاصة في ظل غياب نصوص واضحة في بعض المسائل.
- **التحديات العملية** :كلفة تنفيذ هذه الإجراءات كبيرة، خاصة بالنسبة لمقدمي الخدمات الصغيرة. [3]

**ثانياً: دور مزودي خدمات الإنترنت والهيئات التقنية في حماية الأنظمة**

لا تقتصر مسؤولية حماية النظم المعلوماتية على السلطات العمومية فقط، بل تمتد لتشمل مختلف الفاعلين في قطاع تكنولوجيات الإعلام والاتصال، وعلى رأسهم مزودو خدمات الإنترنت والهيئات التقنية المتخصصة[4]، فهؤلاء الفاعلون يمتلكون المعرفة التقنية والقدرات التشغيلية التي تمكنهم من المساهمة الفعالة في حماية النظم المعلوماتية.

---

[1] المادة 17 من القانون رقم 09-04، سالف الذكر.

[2] قلات سومية، مرجع سابق، ص 95.

[3] قطاف سليمان وبوقرين عبد الحليم، مرجع سابق، ص 120.

[4] نفس المرجع، ص 121.

### 1- سلطة ضبط البريد والاتصالات الإلكترونية(ARPCE)

تلعب سلطة ضبط البريد والاتصالات الإلكترونية (ARPCE) دوراً محورياً في مجال حماية النظم المعلوماتية، حيث تعمل على ضبط وتنظيم قطاع الاتصالات والبريد، حيث تتمثل أهم اختصاصات هذه السلطة في هذا المجال في:

- وضع القواعد التقنية المتعلقة بأمن شبكات الاتصالات والمعلومات، وتحديد المعايير التي يجب أن تلتزم بها شبكات الاتصالات.
- الإشراف على تنفيذ مقدمي الخدمات لالتزاماتهم في مجال حفظ المعطيات الرقمية، والتأكد من امتثالهم لها.
- التعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في مجال تبادل المعلومات والخبرات، وتنسيق الجهود.
- اقتراح التدابير اللازمة لتعزيز أمن الأنظمة المعلوماتية، سواء على المستوى التقني أو التنظيمي.[1]

تتمتع سلطة الضبط بصلاحيات رقابية هامة، حيث يمكنها القيام بعمليات تفتيش لدى مقدمي الخدمات للتأكد من امتثالهم للقواعد التقنية والأمنية، كما يمكنها توقيع عقوبات إدارية في حالة المخالفة.

### 2- التزامات مقدمي خدمات الإنترنت(ISP)

يفرض القانون رقم 09-04 على مقدمي خدمات الإنترنت – (Internet Service Providers ISPs) جملة من الالتزامات التي تهدف إلى تعزيز حماية النظم المعلوماتية، من أبرز هذه الالتزامات:

- **التزام التعاون** :يجب على مقدمي الخدمات التعاون مع السلطات القضائية والأمنية في إطار التحقيقات المتعلقة بالجرائم المعلوماتية، وذلك من خلال تقديم المعلومات والبيانات اللازمة عند الطلب، وهذا الالتزام يعد تجسيداً لمبدأ التضامن بين القطاع الخاص والسلطات العمومية في مكافحة الإجرام.

[1] الموقع الرسمي لسلطة ضبط البريد والاتصالات الالكترونية، على الرابط https://www.arpce.dz/ar/about ، تاريخ الاطلاع 01 جوان 2025، الساعة 22.05.

- **التزام الإفصاح** :يلتزم مقدمو الخدمات بالإفصاح عن البيانات والمعلومات المتعلقة بالمستخدمين والمتصلة بالجرائم المعلوماتية، وذلك بموجب أمر قضائي، ويجب أن يتم هذا الإفصاح بشكل سريع وفعال، مع احترام الضمانات القانونية. [1]

- **التزام الإبلاغ** :يجب على مقدمي الخدمات إبلاغ السلطات المختصة بأي نشاط إجرامي يكتشفونه عبر شبكاتهم، خاصة في مجال الجرائم المتعلقة بالإرهاب أو التهديدات الخطيرة، وهذا الالتزام يساهم في الكشف المبكر عن الأنشطة الإجرامية.

- **التزام الحماية** :يُطلب من مقدمي الخدمات اتخاذ التدابير التقنية اللازمة لحماية أنظمتهم من الاختراق والهجمات الإلكترونية، وإخطار السلطات في حالة تعرضهم لأي خرق أمني، وهذا الالتزام يهدف إلى منع استخدام شبكاتهم كمنصة لشن هجمات على أنظمة أخرى.

- **التزام الإخطار** :في حالة حدوث خرق أمني يؤثر على البيانات الشخصية للمستخدمين، يجب على مقدم الخدمة إخطار المتضررين والسلطات المختصة دون تأخير. [2]

**3- وحدات الأمن السيبراني**

تساهم أيضاً وحدات الأمن السيبراني (Cyber Security Units) المنتشرة في مختلف القطاعات الحيوية (مثل البنوك، المؤسسات الحكومية، شركات الطاقة والاتصالات) في حماية الأنظمة المعلوماتية[3]، وتتمثل المهام الأساسية لهذه الوحدات في:

- مراقبة الأنظمة والشبكات بشكل مستمر للكشف عن أي نشاط مشبوه أو هجوم إلكتروني، باستخدام أنظمة كشف الاختراق (IDS) وأنظمة منع الاختراق(IPS) .

- الاستجابة السريعة للحوادث الأمنية والهجمات الإلكترونية، من خلال تنفيذ إجراءات احتواء الهجوم وإزالة آثاره.

- تنفيذ السياسات والإجراءات الأمنية المحددة لحماية الأنظمة، والتأكد من الامتثال لها.

---

[1] المواد من 10 الى 12 من القانون 09-04، سالف الذكر.

[2] المواد من 10 الى 15، نفس المرجع.

[3] خالد ممدوح إبراهيم، مرجع سابق، ص 270.

- رفع الوعي الأمني لدى المستخدمين والعاملين في المؤسسة، من خلال تنظيم دورات تدريبية وحملات توعوية.
- إجراء تقييم دوري للمخاطر ونقاط الضعف في الأنظمة، واقتراح التدابير التصحيحية اللازمة. [1]

**4- المركز الوطني لأمن الأنظمة المعلوماتية**

لقد تم إطلاق إطار وطني واستراتيجية وطنية حديثة لأمن الأنظمة المعلوماتية في الجزائر، خاصة مع المصادقة على قانون المالية 2025 الذي خصص موارد إضافية لتعزيز الأمن السيبراني[2]، تهدف هذه الاستراتيجية إلى حماية الفضاء الإلكتروني الوطني من التهديدات المتزايدة، وذلك من خلال عدة محاور رئيسية:

- تطوير القدرات الوطنية في مجال كشف ومنع الهجمات السيبرانية، من خلال إنشاء مراكز عمليات أمنية (SOC) على المستوى الوطني والقطاعي.
- تعزيز التعاون بين القطاعين العام والخاص في مجال أمن المعلومات، من خلال إنشاء آليات لتبادل المعلومات والخبرات.
- تطوير إطار قانوني وتنظيمي ملائم لمواجهة التحديات الجديدة، خاصة في مجالات الذكاء الاصطناعي وإنترنت الأشياء.
- بناء قدرات بشرية وطنية متخصصة في مجال الأمن السيبراني، من خلال برامج التكوين والتدريب المتخصصة.[3]

[1] زكرياء ذيب، مرجع سابق، ص 28.

[2] قانون رقم 24-08 المؤرخ في 26 ديسمبر 2024، يتضمن قانون المالية لسنة 2025، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، الضادر في 31 ديسمبر 2025، ص 02.

[3] محمود أحمد عبابنة، مرجع سابق، ص 115.

**5- مسؤولية المستخدمين والعاملين**

لا تقتصر مسؤولية حماية النظم المعلوماتية على المؤسسات والهيئات، بل تمتد لتشمل كل مستخدم للنظم المعلوماتية، فالمستخدمون هم خط الدفاع الأول في مواجهة التهديدات الإلكترونية، ولهم دور حاسم في تحقيق الأمن المعلوماتي.[1]

تتمثل مسؤوليات المستخدمين والعاملين في:

- الالتزام بسياسات وإجراءات الأمن المعلوماتي المحددة من قبل المؤسسة التي يعملون بها.
- استخدام كلمات مرور قوية وتغييرها بشكل دوري، وعدم مشاركتها مع أي شخص آخر.
- توخي الحذر عند التعامل مع الرسائل الإلكترونية غير المعروفة، وعدم فتح المرفقات أو النقر على الروابط المشبوهة.
- الإبلاغ الفوري عن أي نشاط مشبوه أو خرق أمني يتم اكتشافه.
- تحديث البرامج والتطبيقات بشكل مستمر، لضمان الحصول على أحدث التصحيحات الأمنية. [2]

## المطلب الثاني:

## العقوبات الجنائية المقررة لجرائم النظم المعلوماتية

إذا كانت التدابير الوقائية تهدف إلى منع وقوع الاعتداءات على النظم المعلوماتية، فإن العقوبات الجنائية تشكل الخط الدفاعي الثاني، حيث تعمل على ردع المعتدين وتأمين الزجر اللازم لكل من تسول له نفسه المساس بهذه النظم، وقد أولى المشرع الجزائري أهمية بالغة لتجريم الأفعال التي تمس بالنظم المعلوماتية، فأدرج في قانون العقوبات قسماً خاصاً تحت عنوان "جرائم المساس بالأنظمة المعالجة الآلية للمعطيات"، تضمن مجموعة من النصوص التي تحدد الأفعال المجرمة والعقوبات المقررة لها.

وتكمن أهمية العقوبات الجنائية في كونها تعبر عن الإرادة القوية للمجتمع في حماية مصالحه الجوهرية، وتؤكد على رفض المجتمع لأي سلوك يعرض أمنه المعلوماتي للخطر، حيث سيتم تناول هذا

[1] خثير مسعود، مرجع سابق، ص 140.

[2] إبراهيم بلعليات، مرجع سابق، ص 102.

الموضوع من خلال فرعين: يتناول الفرع الأول العقوبات الأصلية المقررة لجرائم النظم المعلوماتية، في حين يخصص الفرع الثاني للعقوبات التكميلية وتشديد المسؤولية الجنائية.

**الفرع الأول: العقوبات الأصلية المقررة لجرائم النظم المعلوماتية**

تُعرف العقوبات الأصلية بأنها تلك العقوبات التي ينص عليها القانون مباشرة للجريمة، وتُطبق بشكل أساسي على مرتكبها، دون حاجة إلى إضافة عقوبات أخرى، وقد حدد المشرع الجزائري في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات نوعين من العقوبات الأصلية لجرائم النظم المعلوماتية: العقوبات السالبة للحرية، والعقوبات المالية.

وتتميز هذه العقوبات بأنها متدرجة حسب خطورة الفعل الإجرامي، منها السالبة للحرية ومنها العقوبات المالية.

**1- عقوبة جريمة الدخول والبقاء غير المرخص بهما**

تنص الفقرة الأولى من المادة 394 مكرر من قانون العقوبات على: "يعاقب بالحبس من (06) ستة أشهر إلى (02) سنتين وبغرامة 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]

يتضح من هذا النص أن المشرع اعتبر جريمة الدخول أو البقاء غير المرخص بهما جنحة، وعاقب عليها بالحبس الذي يتراوح بين ستة أشهر وسنتين، وقد ساوى المشرع بين الدخول والبقاء في نفس العقوبة، كما عاقب على مجرد محاولة ارتكاب الجريمة، مما يعكس تصميمه على مكافحة هذه الظاهرة من جذورها.[2]

وتكمن الحكمة من هذه العقوبة في أن الدخول غير المصرح به إلى نظام معلوماتي، حتى لو لم يتبعه أي فعل ضار، يمثل انتهاكاً خطيراً لحرمة الملكية الخاصة وحرمة الحياة الخاصة، فمجرد الدخول يشكل تدخلاً غير مشروع في فضاء شخصي أو مؤسسي، الأمر الذي يستوجب العقاب.[3]

---

[1] المادة 394 مكرر فقرة 1 من القانون 04- 15، سالف الذكر.

[2] سليمان بارش، مرجع سابق، ص 11.

[3] عبد الرحمان خلفي، مرجع سابق، ص 192.

**2- عقوبة الصور المشددة للجريمة**

أما الفقرة الثانية من نفس المادة فتنص على: "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة".[1]

وبناءً على هذا النص، إذا ترتب على الدخول أو البقاء غير المرخص بهما نتيجة إجرامية تتمثل في حذف المعطيات أو تغييرها أو تخريب النظام، فإن العقوبة تتضاعف لتصبح الحبس من (01) سنة إلى (04) أربعة سنوات، وتجدر الإشارة إلى أن هذه الصورة المشددة تفترض تحقق نتيجة إجرامية، الأمر الذي يتطلب إثباتها لإعمال هذا الظرف المشدد.[2]

**3-عقوبات الاعتداء على النظام المعلوماتي**

قررت المادة 394 مكرر 01 عقوبة الحبس من (01) سنة إلى (03) ثلاثة سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج لكل من اعتدى على النظام المعلوماتي عن طريق الإدخال بالغش أو أزال أو عدل معطيات في نظام المعالجة الآلية.[3]

**4-عقوبة التحضير لارتكاب جريمة إلكترونية**

باستقراء المادة 394 مكرر 02 نجد أن المشرع جرم كافة الأفعال التحضيرية التي تسبق ارتكاب الجريمة المعلوماتية سوآءا من خلال تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية حتى ولو لم تنتج أثرها، كما اعتبر حيازة أو إفشاء أو نشر أو استعمال هذه المعطيات لأي غرض كان جريمة يعاقب عليها بالحبس من (01) سنة إلى (05) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج.[4]

**5-عقوبات متعلقة بالأشخاص والهيئات**

إذا استهدفت هذه الجرائم الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام يعاب الجناة بالحبس من (02) سنتين إلى (10) سنوات وبغرامة من 700.000دج إلى 2.000.000دج

---

[1] المادة 394 مكرر فقرة 2 من القانون 04- 15، سالف الذكر.

[2] بدرة عمارة، مرجع سابق، ص 444.

[3] المادة 394 مكرر 01 من القانون 04- 15، سالف الذكر.

[4] المادة 394 مكرر 02، نفس المرجع.

- إذا كان مرتكب الفعل شخص معنوي يعاقب بغرامة تعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.
- المشاركة في مجموعة في اتفاق في الاعداد لجريمة أو أكثر يعاقب عليه بنفس العقوبة المقررة للجريمة.
- يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع والمحل ومكان الاستغلال.
- يعاقب على الشروع في ارتكاب هذه الجرائم أيضا.
- يعاقب مقدمو خدمات الانترنت في هذه الجرائم بالحبس من (01) سنة إلى (03) ثلاثة سنوات أو بغرامة من 2.000.000دج إلى 10.000.000دج أو بإحدى هاتين العقوبتين. [1]

أما إذا امتدت هذه الأفعال المذكورة أعلاه إلى تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من (01) سنة إلى (03) سنوات وغرامة من 100.000دج إلى 300.000دج.[2]

**الفرع الثاني: العقوبات التكميلية المقررة لجرائم النظم المعلوماتية**

إلى جانب العقوبات الأصلية، أجاز المشرع الجزائري للقاضي أن يحكم بعقوبات تكميلية، إما بالإضافة إلى العقوبات الأصلية أو بدلاً منها في بعض الحالات، كما نص على ظروف مشددة تزيد من شدة العقاب، وعلى مسؤولية الشخص المعنوي في هذا المجال.

العقوبات التكميلية هي عقوبات إضافية يمكن للقاضي إضافتها إلى العقوبات الأصلية، وذلك حسب ظروف الجريمة وملابساتها وشخصية الجاني.

وأهم العقوبات التكميلية المقررة في مجال جرائم النظم المعلوماتية.

**1- المصادرة**

أصبحت المصادرة أداة فعالة في مكافحة الجرائم المعلوماتية، خاصة بعد تعديلات 2024، وتشمل المصادرة:

[1] المواد 394 مكرر 3 إلى المواد 394 مكرر 8 من القانون 04- 15، سالف الذكر.

[2] المادة 394 الفقرة 03، نفس المرجع.

- **مصادرة المعدات والوسائل** :أي الأجهزة والبرامج والتجهيزات التقنية التي استُخدمت في ارتكاب الجريمة، وهذا يشمل الحواسيب، الهواتف الذكية، الأقراص الصلبة، وسائط التخزين، وغيرها من الأدوات.
- **مصادرة العائدات الإجرامية** :الأموال والمكاسب التي تحققت للجاني من وراء الجريمة، فإذا استفاد المجرم مالياً من جريمته (مثل سرقة بيانات بنكية أو ابتزاز ضحاياه)، فإن هذه الأموال تكون قابلة للمصادرة.
- **مصادرة الممتلكات** :في الحالات الخطيرة، يمكن مصادرة ممتلكات المتهم إذا ثبت أنها تحققت من عائدات إجرامية.

تهدف المصادرة إلى تجريد الجاني من أدوات الجريمة وعائداتها، مما يجعله غير قادر على تكرار الفعل الإجرامي، كما تحقق ردعاً عاماً لمن تسول له نفسه اقتراف مثل هذه الجرائم. [1]

**2- المنع من مزاولة المهنة**

يمكن للقاضي أن يمنع المحكوم عليه – بشكل مؤقت أو دائم – من ممارسة مهنة أو نشاط معين، خاصة إذا كانت هذه المهنة مرتبطة بالمجال المعلوماتي الذي استُخدم لارتكاب الجريمة، ويعد هذا الإجراء من أكثر العقوبات التكميلية فعالية، خاصة إذا كان الجاني يعمل في قطاع تقني، فحرمانه من ممارسة مهنته يعتبر رادعاً كبيراً له، كما يحمي المجتمع من خطر العودة إلى ممارسته الإجرامية تحت غطاء مهني.[2]

**3- إغلاق المؤسسة أو الموقع الإلكتروني**

إذا كانت الجريمة قد ارتكبت في إطار مؤسسة أو شركة معينة، أو استُخدمت المؤسسة كغطاء لارتكاب الجريمة، فيمكن للقاضي أن يأمر بإغلاق المؤسسة، وهذا الإجراء له تأثير كبير على الجاني وزملائه والغير، ويعتبر رادعاً قوياً.[3]

---

[1] المادة 09 من الامر 66-156، المعدل والمتمم، سالف الذكر.

[2] المادة 09، نفس المرجع.

[3] المادة 18، نفس المرجع.

كما يمكن للقاضي أن يأمر بإغلاق الموقع الإلكتروني أو الصفحة الإلكترونية التي استُخدمت في ارتكاب الجريمة، وذلك لمنع استمرار النشاط الإجرامي.

تجدر الإشارة إلى أن أمر الإغلاق قد يكون بشكل مؤقت أو دائم، حسب خطورة الجريمة وجسامتها.

**4- الإقصاء من الصفقات العمومية**

يمكن للقاضي أن يقرر إقصاء المحكوم عليه من المشاركة في الصفقات العمومية لفترة زمنية محددة، وهذا الإجراء يمنع المتورطين من الاستفادة من عقود الدولة، وبالتالي يصبحون في وضع غير مؤهل للتعامل مع القطاع العام.[1]

تكمن أهمية هذا الإجراء في أنه يُبعد العناصر الفاسدة أو غير الموثوقة عن التعامل مع المال العام، مما يحمي الدولة من التعاقد مع أشخاص قد يكونون عرضة للابتزاز أو الفساد.[2]

**5- النشر القضائي**

يجوز للقاضي أن يأمر بنشر ملخص الحكم في جريدتين يوميتين أو على موقع إلكتروني معين، على نفقة المحكوم عليه، وهذا الإجراء يحقق ردعاً عاماً، حيث يتم إعلام الجمهور بالعقوبة المسلطة على الجاني.[3]

الهدف من النشر هو تحذير الآخرين من ارتكاب الجرائم المماثلة، وزعزعة استقرار المجرمين الذين يهتمون بسمعتهم.

**6- المنع من الإقامة أو الإبعاد**

في بعض الحالات الخطيرة، يمكن للقاضي أن يمنع المحكوم عليه من الإقامة في مكان معين، أو أن يأمر بإبعاده عن أراضي الدولة إذا كان أجنبياً، وهذا الإجراء يهدف إلى حماية المجتمع من خطر العودة إلى الإجرام.[4]

---

[1] المادة 09 الامر 66-156، المعدل والمتمم، سالف الذكر.

[2] رفيق شاوش، مرجع سابق، ص 588.

[3] المادة 09 الامر 66-156، المعدل والمتمم، سالف الذكر.

[4] المادة 09، نفس المرجع.

## المبحث الثاني:

## الإطار الإجرائي والتعاون في مكافحة جرائم النظم المعلوماتية

تكتسي الإجراءات المطبقة في مجال مكافحة جرائم النظم المعلوماتية أهمية بالغة، ذلك أن خصوصية هذه الجرائم تستلزم آليات إجرائية خاصة تختلف عن تلك المتبعة في الجرائم التقليدية، فالنظم المعلوماتية تتميز بطبيعتها غير المادية، والأدلة الرقمية المرتبطة بها تتسم بسرعة الزوال وسهولة العبث والتلاعب، مما يجعل عمليات جمعها وحفظها وتقديمها للمحكمة أكثر تعقيداً من الأدلة المادية التقليدية.

لقد أدرك المشرع الجزائري هذه الخصوصية، فقام بتكييف قواعد الإجراءات الجزائية لتتناسب مع طبيعة الجرائم المعلوماتية، وذلك من خلال استحداث إجراءات جديدة، منها التسرب الإلكتروني، واعتراض المراسلات، والمراقبة الإلكترونية، والحفظ والإفشاء العاجلان للمعطيات، كما أنشأ آليات للتنسيق الوطني والدولي، باعتبار أن الجرائم المعلوماتية غالباً ما تتجاوز الحدود الوطنية، مما يستلزم تعاوناً وثيقاً بين مختلف الأجهزة الأمنية والقضائية على المستويين الداخلي والدولي.

وسيتناول هذا المبحث الإطار الإجرائي والتعاون في مكافحة جرائم النظم المعلوماتية، من خلال تقسيمه إلى مطلبين رئيسيين: يتناول المطلب الأول إجراءات المتابعة والتحقيق في جرائم النظم المعلوماتية، في حين يخصص المطلب الثاني للتعاون الدولي في مكافحة هذه الجرائم.

### المطلب الأول:

### إجراءات المتابعة والتحقيق في جرائم النظم المعلوماتية

تعتبر إجراءات المتابعة والتحقيق في الجرائم المعلوماتية من أهم المواضيع التي أولاها المشرع الجزائري اهتماماً خاصاً، وذلك بالنظر إلى الطبيعة الخاصة لهذه الجرائم التي تستلزم آليات إجرائية استثنائية، وقد استحدث المشرع بموجب القانون رقم 09-04 المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جملة من الإجراءات المستحدثة التي تهدف إلى تسهيل مهام الضبطية القضائية والنيابة العامة في كشف هذه الجرائم وجمع الأدلة عليها.

ويمكن تقسيم هذه الإجراءات إلى نوعين: إجراءات تقليدية تم تكييفها مع طبيعة الجرائم المعلوماتية، وإجراءات مستحدثة ابتكرها المشرع خصيصاً لهذا النوع من الجرائم.

وفي هذا الإطار، سيتم تقسيم هذا المطلب إلى فرعين: يتناول الفرع الأول إجراءات التحري وجمع الأدلة الرقمية، في حين يخصص الفرع الثاني للجهات المختصة بالتحقيق في الجرائم المعلوماتية.

**الفرع الأول: إجراءات التحري وجمع الأدلة الرقمية**

تُعد عملية جمع الأدلة الرقمية من أخطر مراحل التحقيق في الجرائم المعلوماتية وأكثرها حساسية، وذلك لعدة اعتبارات:

– لأن الأدلة الرقمية بطبيعتها غير مادية وغير محسوسة، مما يجعل إدراكها وفهمها أصعب من الأدلة التقليدية.

– لأن هذه الأدلة سريعة الزوال ويمكن أن تفقد بمجرد إغلاق الجهاز أو انقطاع التيار الكهربائي.

–لأنها قابلة للتلاعب والتعديل بسهولة، مما يستلزم اتخاذ إجراءات صارمة للحفاظ على سلامتها وحجيتها.

وقد نظم المشرع الجزائري هذه الإجراءات في كل من قانون الإجراءات الجزائية والقانون رقم 09 –04، حيث حدد الضوابط والشروط التي يجب مراعاتها عند القيام بعمليات التفتيش والحجز الإلكتروني، وتناول موضوع حجية الدليل الإلكتروني ودور الخبرة التقنية في هذا المجال. [1]

**أولاً: التفتيش والحجز الإلكتروني**

يُعد التفتيش من أهم إجراءات التحري التي تمكّن السلطات المختصة من جمع الأدلة على الجرائم المعلوماتية، غير أن تطبيق هذا الإجراء في البيئة الرقمية يثير إشكاليات عديدة، نظراً لطبيعة الأدلة الرقمية غير المادية ووسائل تخزينها المتنوعة.

**1– التفتيش الإلكتروني وضوابطه القانونية**

أحاط المشرع الجزائري إجراء التفتيش الإلكتروني بعدة ضمانات تهدف إلى حماية حقوق وحريات الأفراد، فوفقاً لقانون الإجراءات الجزائية، "لا يجوز لضباط الشرطة القضائية أن يجروا تفتيشاً في محل مسكون دون رضاء صاحبه، إلا إذا اقتضت الضرورة ذلك، وذلك في الأحوال التي يقررها القانون".

وفي حالة الجرائم المعلوماتية، أضاف المشرع ضمانات إضافية تتمثل في:

[1] المادة 114 من القانون 25–14، سالف الذكر.

- ضرورة الحصول على إذن قضائي مسبق، إلا في حالات التلبس.
- تحديد نطاق التفتيش بدقة، بحيث يقتصر على ما هو ضروري لجمع الأدلة المتعلقة بالجريمة.
- أن يتم التفتيش بحضور صاحب الحق في النظام المعلوماتي أو من ينوب عنه، ما أمكن ذلك.
- إلزام محرري محاضر التفتيش بوصف الإجراءات التقنية التي تم اتباعها، لضمان سلامة الأدلة. [1]

**2- الحجز الإلكتروني**

الحجز الإلكتروني هو الإجراء الذي يلي التفتيش، ويقصد به الاستيلاء على الأدلة الرقمية التي تم العثور عليها، وذلك لحفظها وتقديمها كدليل في المحاكمة، ويتميز الحجز الإلكتروني عن الحجز التقليدي بأنه قد يكون على صورتين:

- **الحجز المادي** :ويتمثل في الاستيلاء على الدعامات المادية التي تحتوي على البيانات الرقمية، كالأقراص الصلبة والهواتف الذكية ووسائط التخزين.
- **الحجز المنطقي** :ويتمثل في نسخ البيانات الرقمية دون الاستيلاء على الدعامات المادية، وذلك في الحالات التي يكون فيها الحجز المادي غير ممكن أو غير مرغوب فيه. [2]

**ثانياً: حجية الدليل الإلكتروني والخبرة التقنية**

يُعد الدليل الإلكتروني من أهم أنواع الأدلة في الجرائم المعلوماتية، بل هو جوهر الإثبات في هذه الجرائم، وقد أثار هذا النوع من الأدلة جدلاً كبيراً في الفقه والقضاء، بسبب طبيعته الخاصة التي تختلف عن الأدلة التقليدية.[3]

**1- مفهوم الدليل الإلكتروني وخصائصه**

الدليل الإلكتروني هو "كل أثر رقمي ينتج عن معالجة إلكترونية للمعطيات، ويمكن استخدامه لإثبات وقوع جريمة معلوماتية أو نسبتها إلى شخص معين"، ويتميز الدليل الإلكتروني بعدة خصائص:

---

[1] المواد من 114 إلى 119 من القانون 25-14، سالف الذكر.

[2] المادة 06 من القانون 09-04، سالف الذكر.

[3] المواد 19 و20، نفس المرجع.

- **الطبيعة غير المادية** :فهو ليس ملموساً كالدليل التقليدي، مما يجعله غير قابل للإدراك الحسي المباشر.
- **سرعة الزوال** :فبعض الأدلة الرقمية، كالبيانات الموجودة في الذاكرة العشوائية(RAM) ، تفقد بمجرد انقطاع التيار الكهربائي.
- **سهولة التعديل** :حيث يمكن تعديل الدليل الإلكتروني أو تزويره بسهولة دون ترك آثار واضحة.
- **سهولة النسخ والتكرار** :يمكن نسخ الدليل الإلكتروني لعدد لا حصر له من المرات دون فقدان جودته. [1]

**2- شروط حجية الدليل الإلكتروني**

لا يختلف الدليل الإلكتروني عن أي دليل آخر من حيث أنه لا تقوم له حجة إلا إذا توافرت فيه شروط معينة، وقد حدد الفقه والقضاء هذه الشروط في:

- **شرط المشروعية** :ويقصد به أن يتم الحصول على الدليل الإلكتروني بطرق مشروعة، وفي إطار الإجراءات التي يقررها القانون، فكل دليل تم الحصول عليه بطريقة غير مشروعة يعتبر باطلاً ولا يجوز الاستناد إليه في أي إجراء قضائي، عملاً بالمبدأ القائل "البطلان يتعلق بالنظام العام.
- **شرط الصحة والسلامة** :ويقصد به أن يكون الدليل الإلكتروني صحيحاً سليماً لم يتم العبث به أو التلاعب في محتواه، ويتطلب هذا الشرط إثبات أن الدليل محفوظ في ظروف تضمن سلامته، وأن سلسلة حيازته لم تنقطع.
- **شرط الصلة بالموضوع** :ويقصد به أن يكون الدليل الإلكتروني مرتبطاً بالوقائع محل الدعوى، وأن يكون من شأنه إثباتها أو نفيها. [2]

[1] إبراهيم بلعليات ، مرجع سابق، ص ص 110-112.

[2] قطاف سليمان وبوقرين عبد الحليم، مرجع سابق، ص ص 130-135.

**3- القيمة الإثباتية للدليل الإلكتروني**

اختلف الفقه والقضاء حول القيمة الإثباتية للدليل الإلكتروني، فذهب بعضهم إلى اعتباره دليلاً كتابياً، بينما اعتبره آخرون دليلاً عينياً أو قرينياً، أما المشرع الجزائري، فقد استقر على اعتبار الدليل الإلكتروني دليلاً مستقلاً بذاته، له قوته الإثباتية التي تتفاوت حسب ظروف كل قضية.[1]

**الفرع الثاني: الجهات المختصة بالتحقيق في الجرائم المعلوماتية**

يتطلب التحقيق في الجرائم المعلوماتية جهات متخصصة تمتلك الخبرة التقنية والقدرات اللازمة للتعامل مع الأدلة الرقمية، وقد حرص المشرع الجزائري على إنشاء وحدات متخصصة داخل مصالح الضبطية القضائية، مع تعزيز دور النيابة العامة والاستعانة بالخبراء التقنيين.

**أولا: وحدات الدرك الوطني**

أدى تنامي ظاهرة الجريمة الإلكترونية إلى استحداث وحدات خاصة تمتلك تقنيات حديثة من أجل كشف وتطوير هذا النوع من الجرائم.

**1- المعهد الوطني للأدلة الجنائية وعلم الإجرام**

أنشأ هذا المعهد المتخصص التابع لمؤسسة الدرك الوطني سنة 2004، بموجب المرسوم الرئاسي 04-183 ويتكون من عدة دوائر متخصصة في مجالات عدة من بينها، الوقاية من الجرائم المتعلقة بتكنولوجية الإعلام والاتصال وذلك كونها تتمتع بعدة خصائص تؤهلها لذلك كالخبرة والتكوين والتعليم مما يجعلها مؤهلة لتقديم المساعدة التقنية والبحوث والدراسات والتحاليل في علم الجريمة.[2]

ومن أجل القيام بهذه المهام المعقدة والمنوطة بها على أحسن وجه تم تقسيم دائرة الإعلام الآلي والإلكتروني المختصة بمعالجة وتحليل وتقديم كل الأدلة الإلكترونية إلى مخابر مختصة في اقتناء المعطيات من حوامل المعلومات وضمان سلامة ونزاهة الدليل الرقمي وتتمثل هذه المخابر في:

---

[1] وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقًا للتشريع الجزائري، المجلة الجنائية القومية، المجلد 57، العدد 02، 2014، ص ص 85-86.

[2] مرسوم رئاسي 04-183 المؤرخ في 26 جوان 2004، يتضمن إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، العدد41، الصادر في 27 جوان 2004، ص18.

**مخبر الإعلام الآلي:** ويتمثل دوره في معالجة وتحليل حوامل المعطيات الرقمية (الهاتف، الشريحة، الأقراص الصلبة، ذاكرة الفلاش) كما يختص بتحديد التزوير الرقمي للبطاقات البنكية.

**مخبر الفيديـــو:** ويتمثل دوره في إعادة تمثيل مسرح الجريمة بتشكيل ثلاثي الأبعاد وتحسين نوعية الصورة والفيديو ومدى شرعيتهما.

**مخبر الصوت:** يتمثل دوره في تحديد المتكلم ومعرفته بالإضافة إلى شرعية التسجيلات الصوتية مع تحسين جودتها.[1]

**2- مركز الوقاية من جرائم المعلوماتية ومكافحتها**

كلف هذا المركز الذي بدأ في مزاولة مهامه سنة 2004 بمهمتين رئيسيتين تتمثل في:

- مهمة استباقية تتمثل بالتدقيق والوقاية
- مهمة بعدية تتعلق بردع الجرائم الماسة بالطفولة

كما يختص المركز بمعالجة الجرائم المالية والمتعلقة بالتجارة الإلكترونية والدفع الإلكتروني.[2]

**3- المصلحة المركزية للتحريات الجنائية**

تعتبر هذه المصلحة أحد المصالح المركزية التابعة لجهاز الدرك الوطني إذ تختص بالتحقيقات التقنية والعملية في الجرائم المعلوماتية المعاصرة والتي تعدت حدود المكان والزمان مما يتطلب من المحققين المختصين تقديم مقاربة تقنية أولية.[3]

**ثانيا: وحدات الأمـن الوطنـي:**

من أجل نجاعة التحقيق ومنحه دور فعال في مواجه الجرائم الإلكترونية اختصت المديرية العامة للأمن الوطني بمثل هذه التحقيقات، من خلال قسمين أساسيين يتمثل القسم الأول في المخابر والقسم الثاني في الفرق.

---

[1] رجاء أمدور، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث، تخصص قانون خاص، جامعة محمد البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، 2020-2021، ص ص 100-101.

[2] نفس المرجع، ص 101.

[3] نفس المرجع، ص 102

**1- المخابـــر**

أنشأ مخبر مركزي للشرطة العلمية بالعاصمة وآخر بوهران ومركز قسنطينة بالإضافة إلى إنجاز مخابر أخرى بورقلة وبشار وتمنغاست، كم استحدثت أقسام متخصصة في مجال تتبع الأدلة الرقمية واستغلال الأجهزة الإلكترونية على غرار أدوات التخزين الرقمية ( أجهزة التصوير، بطاقات الذاكرة، الأقراص الصلبة)، وأجهزة الكمبيوتر ولواحقها.[1]

**2- الفرق المستحدثة على مستوى كل ولاية**

توجد على مستوى كل ولاية فرقة ولائية للشرطة القضائية تختص بمكافحة الجرائم المتصلة بتكنولوجية الإعلام والاتصال وذلك نظرا لتفاقم ظاهرة الإجرام الإلكتروني المتزايد خاصة فيما يتعلق بالتأثيرات السلبية لمواقع التواصل الاجتماعي، والانفتاح على العالم الافتراضي الذي ولد انفلات أخلاقي غير مسبوق.[2]

**المطلب الثاني:**

**التعاون الدولي في مكافحة جرائـــم النظم المعلوماتية**

إن تميز الجرائم التي تستهدف النظم المعلوماتية بطابعها العابر للحدود أدى إلى تيقن المجتمع الدولي بخطورتها ووجوب الوقاية منها ومكافحتها لهذا أصبح من الضروري إيجاد أليات دولية محكمة لمواجهتها بالإضافة إلى وجوب التنسيق فيما بين الدول وتعزيز التعاون الدولي أمنيا وفنيا وقضائيا لتحقيق الأهداف المسطرة.

ومن بين هذه المساعي ما سنتناوله وفق فرعين يتمثل الفرع الأول في الاتفاقيات الدولية والأممية، والفرع الثاني في أجهزة التعاون الدولي في مجال الجرائم المعلوماتية.

[1] رجاء أمدور، مرجع سابق، ص 103.

[2] نفس المرجع، ص ص 104-105.

**الفرع الأول: الاتفاقيات الدولية والأممية**

تمثل الاتفاقيات الدولية الأداة التي يمكن أن تنتج عنها الالتزامات بين الدول ومن هذا المنطلق تم اعتماد اتفاقية بودابست بالمجلس الأوروبي، كما سنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك من أجل تعزيز التعاون بين الدول العربية في مواجهة الجرائم الإلكترونية.[1]

**أولا: الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية**

ركزت هذه الاتفاقية على الحاجة إلى التعاون الدولي في الكشف عن الجرائم المعلوماتية والتحقيق فيها ومتابعة مرتكبيها قضائيا، كما دعت إلى حماية المصالح المشروعة في استعمال وتطوير تقنية المعلومات وأقرت بالحاجة إلى حماية البيانات الشخصية.[2]

كما نظمت هذه الاتفاقية قواعد الاختصاص عند ارتكاب الجريمة داخل إقليم الدولة الطرف أو على متن سفينة ترفع علمها، أو على متن طائرة مسجلة باسمها أو من قبل مواطن يحمل جنسيتها...إلخ.[3]

**ثانيا: البروتوكول الإضافي بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر**

يمثل سوء استعمال واستخدام الانترنت بيئة خصبة لممارسة العنصرية وكراهية الأجانب، مما أدى إلى وجوب تكاتف دولي للتحقيق مع مرتكبي هذه الجرائم وملاحقتهم قضائيا، ومن ثمة تم وضع بروتوكول إضافي بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب عبر فضاء الأنترنت، ومن بين أهداف هذا البروتوكول تعزيز التعاون الدولي وتبادل الخبرات في هذا المجال بالإضافة إلى تسليم المجرمين وتقديم المساعدة القانونية في هذا الشأن.[4]

---

[1] رجاء أمدور، مرجع سابق، ص 196.

[2] نفس المرجع، ص 197.

[3] المادة 22 من الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم 185، بودابست،2001.

[4] التقرير التفسيري للبروتوكول الإضافي لاتفاقية الجريمة الإلكترونية لتجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عبر أنظمة الكمبيوتر، المنعقدة في ستارسبورغ في 28 يناير 2003، مجلس أوروبا، سلسلة المعاهدات الأوروبية، رقم 189، ص02.

**ثالثا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**

تناولت هذه الاتفاقية التعاون القانوني والقضائي، وذلك من خلال سن قواعد قانونية تتماشى مع طبيعة الجرائم المعلوماتية، كما تهدف إلى تكثيف التعاون العربي في هذا المجال قصد المحافظة على مصالح الدول العربية وأمنها، ومن بين الآليات التي تطرقت لها الاتفاقية ما يلي:

- تمديد الاختصاص في الجرائم المنصوص عليها في هذه الاتفاقية
- إمكانية تبادل المجرميـن
- تبادل المساعدة لأقصى حد ممكن
- توحيد الإجراءات المتعلقة بطلب التعاون والمساعدة المتبادلـة
- اتخاذ التدابير المؤقتة والعاجلة.[1]

**رابعا: دور الأمم المتحدة في مجال التعاون الدولي لمواجهة الجرائم المعلوماتية**

**1- المؤتمرات**

دأبت منظمة الأمم المتحدة على تنظيم مؤتمرات دورية من بينها ما يلي:

- المؤتمر السابع لمنع الجريمة ومعاملة المجرمين المنعقد في ميلانو بإيطاليا سنة 1985
- المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين المنعقد في هافانا بكوبا سنة 1990
- المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين المنعقد في القاهرة بمصر سنة 1995
- المؤتمر الحادي عشر لمنع الجريمة ومعاملة المجرمين المنعقد في بانكوك بتايلاندا سنة 2005
- المؤتمر الثاني عشر لمنع الجريمة ومعاملة المجرمين المنعقد في سالفادور بالبرازيل سنة 2010
- المؤتمر الثالث عشر لمنع الجريمة ومعاملة المجرمين المنعقد في الدوحة بقطر سنة 2015
- المؤتمر الرابع عشر لمنع الجريمة ومعاملة المجرمين المنعقد بكيوتو باليابان سنة 2020

بحيث تطرقت هذه المؤتمرات إلى تكثيف التنسيق في مجال التعاون الدولي لمحاربة الإجرام بما فيها الجرائم المعلوماتية والتي ترتكب عبر الفضاءات الرقمية.[2]

[1] رجاء أمدور، مرجع سابق، ص ص 200-201.

[2] نفس المرجع، ص ص 202-204.

**2- المنظمة العالمية للملكية الفكرية (WIPO) في مواجهة الجرائم المعلوماتية**

تعد منظمة تابعة لهيئة الأمم المتحدة يقع مقرها في جنيف تهتم بمجال حماية الملكية الفكرية بحيث تم إنشاؤها بستوكهولم في 14 يوليو 1967، وصادقت عليها الجزائر بموجب الأمر 75-02 مكرر المؤرخ في 09 جانفي 1975، ومن خلال هذا أضاف المشرع الجزائري برامج الحاسب الآلي ضمن المادة 04 من الأمر 03-05 واعتبرها من المصنفات الأدبية أو الفنية المحمية.[1]

**3- الاتحاد الدولي للاتصالات (ITU) في مواجهة الجرائم المعلوماتية**

يعد الاتحاد الدولي للاتصالات وكالة متخصصة تابعة للأمم المتحدة يقع بجنيف بسويسرا، ويهدف إلى زرع الثقة والأمان في استعمال التكنولوجيا الحديثة في مجال المعلومات والاتصالات وذلك من خلال ما يلي:

- اتخاذ التدابير القانونية لتحقيق التناسق بين الأطر القانونية الدولية.
- تعاون كافة الشركاء التابعين للأمم المتحدة من أجل توفير الأمن المعلوماتي ومكافحة الرسائل الإقتحامية.
- إتخاذ التدابير التقنية والاجرائية في مجال المعلومات والاتصالات.
- التنظيم والمشاركة في المنتديات والمؤتمرات الدوليــة بشأن مواجهة الجرائم المعلوماتية وتأمين استخدام الانترنت وحماية الأطفال منها.[2]

**الفرع الثاني: أجهزة التعاون الدولي في مجال الجرائم المعلوماتية**

لا يمكن للتعاون الدولي أن يكتمل إلا في اطار وجود اليات تنظيمية فعالة تمكن من توفير جميع المعلومات والبيانات الخاصة للجريمة ومرتكبيها خارج الحدود الوطنية، ومن بين هذه الآليات التنظيمية نجد الأجهزة الأمنية الدولية التالية:

[1] رجاء أمدور، مرجع سابق، ص207.

[2] نفس المرجع، ص ص 208-209.

**أولا: الأنتربول**

تعد المنظمة الدولية للشرطة الجنائية **(الأنتربول)** جهاز تابع لمنظمة الأمم المتحدة، يقع مقره في ليون بفرنسا، وقد تم إنشاؤه في 1923/09/07.[1]

ويضطلع هذا الجهاز بعدة أدوار في مجال مواجهة الجرائم المعلوماتية وذلك من خلال ما يلي:

- ترسيخ وتشجيع النعاون الدولي بين الأجهزة الشرطية بين الدول الأطراف لمكافحة الجريمة يشتى أنواعها وذلك بتبادل المعلومات والبيانات المتعلقة بحيثياتها بواسطة المكاتب المركزية الوطنية للشرطة الجنائية الدولية الموجودة على مستوى هذه الدول.[2]
- دعم جهود الشرطة في مواجهة الجرائم العابرة للحدود الوطنية، وتوفير الخدمات في مجال الأدلة الجنائية.
- التعاون في ملاحقة المجرمين وتسليم المطلوبين على وجه الخصوص في جرائم الاستغلال الجنسي للأطفال عبر الانترنيت والاحتيال المعلوماتي، بالإضافة الى القيام بإجراءات البحث والتحقيق في الجرائم الالكترونية.[3]

وفي إطار التعاون بين الانتربول ومجموعة الدول الثمانية الكبرى، تم اتخاذ استراتيجيات لمكافحة الجرائم المعلوماتية، وذلك من خلال استحداث مركز اتصالات امني عبر الشبكة يربط بين مصالح الشرطة في الدول الأطراف، كما توجه الى استخدام قاعدة بيانات مركزية تقوم بالتحليل والمقارنة الاوتوماتيكية للمحتويات، مع تقديم إرشادات حول الجرائم المعلوماتية وكيفيات التحقيق فيها ومكافحتها.[4]

**ثانيا: المكتب العربي للشرطة الجنائية**

قام مجلس وزراء العرب بإنشاء مكتب عربي للشرطة الجنائية من اجل تامين وتعزيز التعاون بين الدول الأعضاء من خلال أجهزتها الشرطية، وهذا فيما يخص مكافحة الجريمة ومتابعة المجرمين قانونيا

---

[1] رجاء أمدور، مرجع سابق، ص 210.

[2] محمد أحمد سليمان، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الاكاديمية للبحث القانوني، المجلد14، العدد 02، 2016، ص 53.

[3] رجاء أمدور، مرجع سابق، ص 211.

[4] عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون، دقهلية، المجلد 01، العدد 16، 2014، ص 198.

وفقا للتشريعات المعمول بها في كل دولة، مع تقديم المساعدة في دعم وتطوير أجهزة الشرطة في هذه الدول الأعضاء.[1]

**ثالثا: اليوروبول**

يمثل اليوروبول هيئة استشارية في مجال مكافحة الجرائم المعلوماتية، يقع مقره في لاهاي بهولندا ويختص بإنجاز الدراسات الخاصة بالجرائم المعلوماتية واستنتاج دوافعها، وتقديم استشراف مستقبلي حولها، كما يحظى بثقة الاتحاد الدولي للأمن المعلوماتي، وتنصب اهتماماته البحثية والتحقيقية خاصة في جرائم استغلال الأطفال في المواد الإباحية والإرهاب الالكتروني، بالإضافة الى تدعيم الأجهزة الشرطية بتقارير وادلة حول المجرمين والجرائم المعلوماتية المرتكبة.[2]

ومن بين الصلاحيات التي يتمتع بها اليوروبول ما يلي:

- مكافحة الجرائم المعلوماتية بما فيها جرائم الكمبيوتر وكافة اشكال الجرائم التي يسهل ارتكابها بواسطة التقنيات الرقمية، على ان تشمل هذه الجرائم هيكلا او منظمة إجرامية.
- توفير الخبرة والمساعدة الفنية للتحقيقات والعمليات داخل الاتحاد الأوروبي.
- توفير نظام معلومات محوسب فيما بين الدول الأعضاء لإدخال البيانات والوصول اليها وتحليلها ثم استغلالها.[3]

**رابعا: اليوروجست**

يعد اليوروجست هيئة تابعة للاتحاد الأوروبي تهدف الى تحسين كفاءة السلطات المختصة في الدول الأعضاء لمكافحة الجريمة المنظمة العابرة للحدود الوطنية بما فيها الجرائم المعلوماتية، ويسعى الى دعم التنسيق والتعاون في مجال مكافحة الجرائم الخطيرة، ومن بين مهامه أيضا نذكر ما يلي:

---

[1] نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، منشورات دار الخلدونية، الجزائر،2017، ص 150.

[2] حسين ربيعي، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، 2016/2015، ص 154.

[3] رجاء أمدور، مرجع سابق، ص ص 214-215.

- تطوير اليات مكافحة الجرائم المعلوماتية بناء على تبادل المعلومات دوريا مع محتكم الاتحاد الأوروبي، ودعم فعالية التحقيق في الجرائم المعلوماتية تمهيدا لليوروبول في مجال عمله اثناء التحقيقات.[1]
- الرفع من مستوى التنسيق اثناء التحقيقات والملاحقات القضائية بن السلطات المختصة في الدول المعنية.
- تحسين كفاءة التحقيقات بين الدول الأعضاء.
- تنفيذ طلبات التسليم من قبل السلطات الوطنية، للاستفادة من المساعدة القانونية الدولية.
- المشاركة في جهود مكافحة استغلال الأطفال في المواد الإباحية.
- مكافحة الاحتيال بالتعاون مع المكتب الأوروبي.
- مناقشة خطة العمل لمكافحة الجرائم المعلوماتية داخل فضاء الأوروبي.[2]

**خامسا: الافريبول**

خلال مؤتمر الانتربول الإقليمي الافريقي الثاني والعشرين المنعقد بوهران سنة 2013 ظهرت فكرة انشاء الافريبول بغية استغلاله في:

- المساعدة على تعزيز القدرة التحليلية للشرطة الافريقية من اجل تقييم التهديدات الاجرامية وتطوير الاستجابة اللائقة.
- تعزيز التنسيق بين قوات الشرطة المتواجدة في مهام دعم السلام.
- تطوير السياسة الشرطية الافريقية لمسايرة الجرائم المستحدثة ومواجهة الجرائم المعلوماتية بناء على تبادل الخبرات واجراء دورات تدريبية، والاستفادة من المساعدة التقنية المتبادلة في مجال المعلوماتية واستخدام التكنولوجيا والأدلة الالكترونية.[3]

[1] حسين ربيعي، مرجع سابق، ص 155.

[2] رجاء أمدور، مرجع سابق، ص ص 215-216.

[3] يوسف مناصرة، جرائم المساس بأنظمة المعالجة الالية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها)، دراسة مقارنة، دار الخلدونية، الجزائر، 2018، ص 284.

**خلاصة الفصل**

من خلال ما تم التطرق إليه يتضح أن المشرع الجزائري سعى إلى توفير حماية جنائية متكاملة للنظم المعلوماتية، وذلك عبر إقرار مجموعة من التدابير الوقائية والآليات القانونية الرامية إلى الحد من الجرائم المعلوماتية قبل وقوعها، إلى جانب فرض عقوبات جنائية تهدف إلى تحقيق الردع ومواجهة مختلف صور الاعتداء على الأنظمة والمعطيات الإلكترونية، كما حرص على وضع إطار إجرائي خاص يتلاءم مع طبيعة هذه الجرائم من خلال اعتماد وسائل حديثة للتحري وجمع الأدلة الرقمية، مع إسناد مهام المتابعة والتحقيق لجهات مختصة تمتلك الخبرة التقنية اللازمة.

كما تبين أن مكافحة الجرائم المعلوماتية لم تعد مسؤولية داخلية تقتصر على أجهزة الدولة الوطنية فقط، بل أصبحت تتطلب تعاونا وطنيا ودوليا قائما على تبادل المعلومات والمساعدة القضائية والتنسيق الأمني، خاصة في ظل الطابع العابر للحدود الذي تتميز به هذه الجرائم، وبذلك تظهر أهمية تطوير التشريعات والآليات التقنية وتعزيز التعاون الدولي لضمان فعالية الحماية الجنائية للنظم المعلوماتية ومواكبة التطورات التكنولوجية المتسارعة.

# خاتمـــــة

## خاتمـــة:

بالرغم أن الفضاء الرقمي والتكنولوجي وفر الكثير من المزايا عبر تقديم خدمات نوعية وسريعة، ووضعها في خدمة الافراد والدول وباقي الكيانات الأخرى، الا أن المخاطر التي تحفو هذا التطور في تزايد مستمر يستوجب المواكبة التشريعية والتنظيمية والتقنية اللازمة، وفقا لإجراءات تصون خصوصية الفرد وتحترمها من جهة وتضمن الوقاية من الجرائم المعلوماتية وتكافحها من جهة أخرى، سواء كان ذلك على المستوى الوطني أو في إطار التعاون الدولي.

وقد توصلنا الى مجموعة من النتائج والتوصيات يمكن تلخيصها على النحو التالي:

- **النتائج**

- إن التطور المستمر والمتتالي للجريمة المعلوماتية يجعل من الصعب تحديد تعريف جامع ومانع لها، نظرا لما تتمتع به من خصوصية مرنة في التغير والتحور.
- تظهر خطورة هذه الجرائم في امتداد اثارها من الفرد إلى المجتمع، وحتى الدول على نحو يهدد استقرارها الداخلي الاجتماعي، والاقتصادي والسياسي.
- انطلاقا من الاثار والمخاطر التي يمكن ان تشكلها الجرائم المعلوماتية عمد المشرع الجزائري الى استحداث إجراءات مكيفة تتناسب والطابع الوقائي الواجب توفره، وذلك من خلال انشاء هيئات غير قضائية ذات طابع وقائي أحيانا واستشرافي يدعم الهيئات القضائية والأمنية أحيانا أخرى.
- اللجوء إلى التعاون الدولي كحتمية أساسية تمكن المجتمع الدولي من الوقاية من الجرائم المعلوماتية باعتبارها جرائم تتعدي الحدود الوطنية.

- **المقترحات**

- الاهتمام بالجانب التشريعي لمسايرة التطور الحاصل في الاجرام عبر الفضاء الرقمي.
- تكثيف الدورات التكوينية، والاستفادة من الخبرات التقنية الأجنبية للأجهزة الأمنية والقضائية.
- توفير قواعد بيانات وطنية متطورة تجمع مختلف الهيئات الأمنية والقضائية والاستشارية فيما يخص تحليل الأدلة والبيانات الرقمية.
- نشر الوعي الجمعي لدى الافراد بخطورة الاستعمال اللاعقلاني للفضاءات الرقمية والتحسيس بمدى خطورتها على الفرد والمجتمع والدولة.

# قائمة المصادر والمراجع

## قائمة المصادر والمراجع

### أولاً: الكتب


1. إبراهيم سلطان، نظم المعلومات الإدارية، مدخل إداري، الدار الجامعية، الإسكندرية، 2000 .
2. أحمد حسين علي حسين، *نظم المعلومات المحاسبية*، مطبعة الإشعاع، الإسكندرية، 1997 .
3. أحمد رجب عبد العالي، المعاصرة في المحاسبة الإدارية، الدار الجامعية للطباعة والنشر، بيروت، 1992 .
4. الحسينة سليم إبراهيم، نظم المعلومات الإدارية، مؤسسة الوراق، عمان، الأردن، 1998 .
5. الدهراوي كمال الدين، مدخل معاصر في نظم المعلومات المحاسبية، الدار الجامعية، الإسكندرية، 2003 .
6. السيد إسماعيل، نظم المعلومات لإيجاد القرارات الإدارية، المكتب العربي الحديث، الإسكندرية، 2001
7. السيد غراب كامل وآخرون، نظم المعلومات الإدارية، جامعة الملك سعود، 1997 .
8. الطائي محمد حسين آل فرج، المدخل إلى نظم المعلومات الإدارية، دار وائل، الأردن، 2005 .
9. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.
10. بارش سليمان، شرح قانون العقوبات الجزائري: الجريمة، ديوان المطبوعات الجامعية، الجزائر، 1995 .
11. باطلي غنية، الجريمة الإلكترونية: دراسة مقارنة، الدار الجزائرية، الجزائر، 2015 .
12. بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية للنشر والتوزيع، الجزائر، 2007.
13. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017 .
14. بوسقيعة أحسن، الوجيز في القانون الجزائي العام، الطبعة 18، دارهومة، الجزائر،2019.

15. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر (أساليب وثغرات)، دار الهدى، الجزائر، 2010 .

16. خلفي عبد الرحمان، محاضرات في القانون الجنائي، دار الهدى للطباعة والنشر، الجزائر، 2012 .

17. سعد غالب ياسين، نظم المعلومات الإدارية، دار اليازوري، عمان، الأردن، 1997 .

18. سليمان عبد الله، شرح قانون العقوبات، القسم العام، الطبعة الخامسة، ديوان المطبوعات الجامعية، الجزائر، 2004 .

19. صلاح الدين عبد المنعم مبارك، اقتصاديات نظم المعلومات المحاسبية والإدارية، دار الجامعة الجديدة، الإسكندرية، 2001 .

20. عبابنة محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2004 .

21. فاضل السامرائي إيمان، وهيثم محمد الزعبي، نظم المعلومات الإدارية، دار صفاء، الأردن، 2004 .

22. قارة أمال، الحماية الجزائية المعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، 2007.

23. ممدوح إبراهيم خالد، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009 .

24. محمد البكري سونيا، وإبراهيم سلطان، نظم المعلومات الإدارية، دار النشر الجامعية الجديدة، مصر، 2002 .

25. مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها): دراسة مقارنة، دار الخلدونية، الجزائر، 2018 .

26. يسر أنور علي، شرح قانون العقوبات: النظرية العامة، دار النهضة العربية، القاهرة، 1998 .

**ثانياً: المذكرات والرسائل الجامعية**

1. أمدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث، تخصص قانون خاص، جامعة محمد البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، 2020-2021.

2. ربيعي حسين، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، 2016/2015 .

3. شنين صالح، الحماية الجزائية لبرامج الحاسب الآلي، مذكرة ماجستير في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2006-2007 .

**ثالثاً: المقالات العلمية**

1. أحمد سليمان محمد، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الاكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016.

2. بن زهرة السعيد، بلقاسم العربي، القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، دراسة في المفهوم والاختصاص، مجلة الدراسات القانونية والاقتصادية، المجلد 08، العدد 02، 2025 .

3. بن قارة مصطفى عائشة، آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم 18/07، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، 2019 .

4. حوحو رمزي، الحماية الجنائية الدولية لحقوق الإنسان، مجلة المفكر، المجلد 1، العدد 5، جامعة محمد خيضر بسكرة، 2010.

5. خراشي عادل عبد العال إبراهيم، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون، دقهلية، المجلد 01، العدد 16، 2014.

6. ذيب زكرياء، تجريم الاعتداء على نظم المعالجة الآلية للمعطيات التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، المجلد 7، العدد 2، جامعة عمار ثليجي، الأغواط، 2023 .

7. شاوش رفيق، المصلحة المحمية في الجرائم المضرة بالإدارة العامة في التشريع الجنائي المقارن، مجلة المفكر، المجلد 11، العدد 01،2016 .

8. عمارة بدرة، الحماية الجنائية للمعلومات الإلكترونية دراسة في القانون 04-15، مجلة البحوث القانونية والسياسية، جامعة الطاهر مولاي بسعيدة، المجلد 01، العدد 02، 2014.

9. لعوارم وهيبة، الدليل الرقمي في مجال الإثبات الجنائي وفقًا للتشريع الجزائري، المجلة الجنائية القومية، المجلد 57، العدد 02، 2014.

10. محمد علي سالم إسراء، الحماية الجنائية للعتبات المقدسة: دراسة مقارنة، مجلة المحقق الحلي جامعة بابل، للعلوم القانونية والسياسية، المجلد 06، العدد 01،2014.

**رابعا: الاتفاقيات الدولية**

1. الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم 185، بودابست،2001.

2. التقرير التفسيري للبروتوكول الإضافي لاتفاقية الجريمة الإلكترونية لتجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عبر أنظمة الكمبيوتر، المنعقدة في ستارسبورغ في 28 يناير 2003، مجلس أوروبا، سلسلة المعاهدات الأوروبية، رقم 189 .

**خامسا: القوانين والنصوص القانونية**

1. قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، الصادرة بتاريخ 10 نوفمبر2004.
2. قانون رقم 09-04 المؤرخ في5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 49، الصادرة في 16 عشت 2009.
3. قانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد 36، الصادرة بتاريخ 10 يونيو2018.
4. قانون رقم 24-08 المؤرخ في 26 ديسمبر 2024، يتضمن قانون المالية لسنة 2025، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، الصادر في 31 ديسمبر 2025.
5. قانون رقم 25-11 المؤرخ في 24 يوليو 2025، يعدل ويتمم القانون 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، الصادرة بتاريخ 24 يوليو 2025.
6. قانون رقم 25-14 المؤرخ في 03 غشت 2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 54، الصادرة بتاريخ 13 غشت 2025.

7. قانون رقم 26-02 المؤرخ في 17 فبراير 2026، يحدد القواعد العامة المتعلقة بخدمات الثقة للعلامات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية، العدد 14، الصادرة بتاريخ 18 فبراير 2026.
8. أمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات الجزائري، المعدل والمتمم، الجريدة الرسمية، العدد 49، الصادرة بتاريخ 11 يونيو 1966.
9. مرسوم رئاسي رقم 04-183 المؤرخ في 26 جوان 2004، يتضمن إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، العدد41، الصادرة في 27 جوان 2004.
10. مرسوم رئاسي رقم 21-439 المؤرخ في 11 نوفمبر 2021، المحدد لتشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 73، الصادرة بتاريخ 11 نوفمبر 2021.
11. التعليمة الوزارية المشتركة رقم 01/2019 المؤرخة في 15 جانفي 2019، المتعلقة بوضع مخططات أمن الأنظمة المعلوماتية في المؤسسات العمومية، وزارة البريد وتكنولوجيات الإعلام والاتصال، 2019.

**سادسا: المواقع الإلكترونية**

1. موقع أحمد عبد السلام، www.fiqh.islammessage.com
2. بوابة الإسلام، www.islamport.com
3. الموقع الرسمي لوزارة الدفاع الوطني الجزائرية،https://www.mdn.dz/
4. الموقع الرسمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، (ANPDP) https://anpdp.dz/ar/
5. الموقع الرسمي لسلطة ضبط البريد والاتصالات الالكترونية، (ARPCE)
6. https://www.arpce.dz/ar/

# الفهرس