وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم
Université Abdelhamid Ibn Badis de Mostaganem

كلية الحقوق والعلوم السياسية
قسم القانون الخاص

المرجع : .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

# جرائم الانترنت في القانون الجزائري

ميدان الحقوق والعلوم السياسية

التخصص : القانون القضائي

من إعداد الطالب:
- قحام حسام الدين

تحت إشراف الأستاذة:
- بلحمزي فهيمة

أعضاء لجنة المناقشة

| | | |
|---|---|---|
| الأستاذ(ة) | كعيبيش بومدين | رئيسا |
| الأستاذة | بلحمزي فهيمة | مشرفا مقررا |
| الأستاذ(ة) | مهيدي نوال | مناقشا |

السنة الجامعية: 2026/2025

نوقشت في : 2026/06/17

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية

مصلحة التربصات

# تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
# في إنجاز البحث

أنا الممضي أدناه , الطالب (ة) :

اللقب : حمّ حام ..... الإسم : حسام الدين .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 404492712 والصادرة بتاريخ: 2023/01/29 .....

المسجل(ة) بكلية: العلوم السياسية قسم: حقوق الخاص .....

والمكلف(ة) بإنجاز مذكرة ماستر بعنوان:

..... جريمة الاتجار بالبشر .....

.....

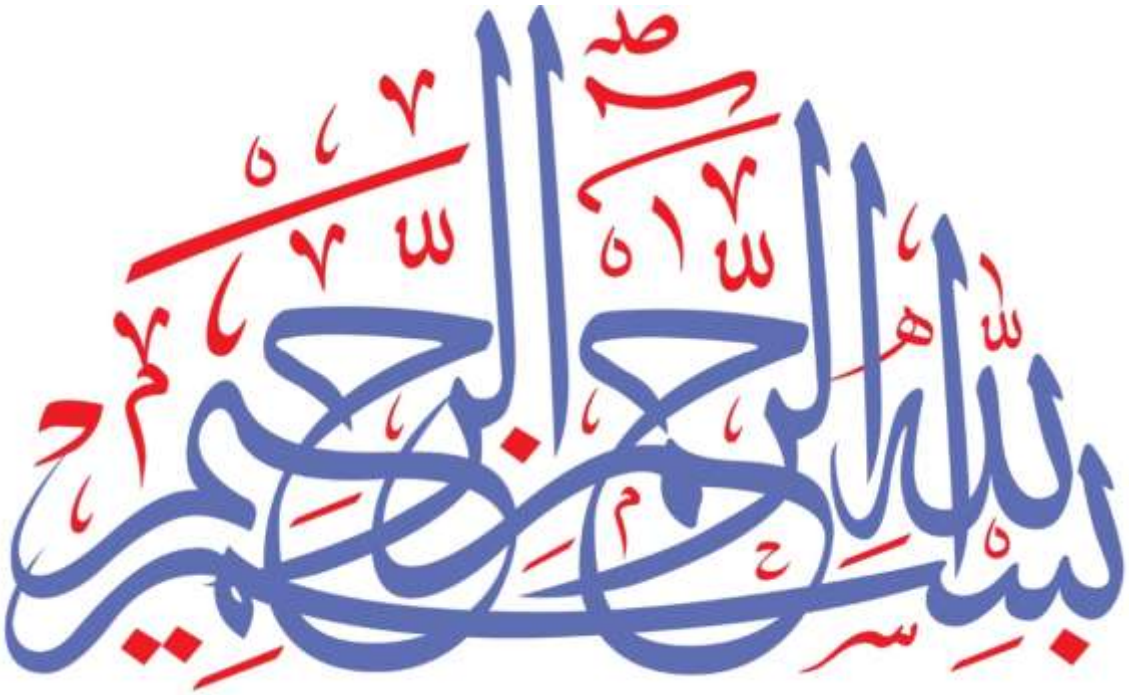
أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: .....

إمضاء المعني

الشهود
مصادقة على شرعية الإمضاء
حمّ حام حسام الدين
الصادرة في: 404492712
2023.01.29
17 JUIN 2026

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها.


بسم الله الرحمن الرحيم


وقل
رب زدني علما

# إهداء

الحمد لله الذي بنعمته تتم الصالحات، والذي وفقني وأعانني على إتمام هذا العمل المتواضع.

أهدي ثمرة جهدي وتخرجي إلى من كانا سبب وجودي وسندي في هذه الحياة، إلى من

كانا النور الذي أضاء دربي، والسند الذي منحني القوة لمواصلة الطريق...

إلى أبي الغالي، الذي علمني أن النجاح لا يأتي إلا بالصبر والاجتهاد، والذي لم

يبخل عليّ يومًا بدعمه وتوجيهه ونصائحه القيمة، فكان خير سند وخير قدوة.

إلى أمي الحبيبة، نبع الحنان والعطاء، التي سهرت الليالي من أجل راحتي، ورافقتني بدعواتها الصادقة

في كل خطوة من خطوات حياتي، فكان فضلها عليّ بعد الله عظيمًا لا يمكن أن توفيه الكلمات.

إليكما أهدي هذا العمل المتواضع عربون محبة ووفاء وتقدير، راجيًا أن أكون دائمًا مصدر

فخر واعتزاز لكما.

كما أهدي هذا العمل إلى إخوتي وأخواتي الأعزاء: سلاف، فارس، وسيرين،

الذين كانوا مصدر تشجيع ومساندة طوال مسيرتي الدراسية.

وإلى كل الأصدقاء والزملاء الذين شاركوني لحظات الدراسة والتعب، وقدموا لي الدعم والنصح.

وإلى كل من ساهم من قريب أو بعيد في إنجاز هذا العمل.

أهديكم جميعًا هذا الجهد المتواضع، راجيًا من الله أن يجعله نافعًا ومثمرًا.

**حسام الدين**

# شكر وعرفان

بسم الله الرحمن الرحيم.. الحمد لك والشكر لك يارب حمدا كثيرا مباركا فيه..
أتقدم بخالص الشكر والامتنان إلى الله عز وجل على توفيقه وعونه لإتمام هذا العمل، فقد كانت العودة إلى مقاعد الدراسة فرصة ثمينة أكدت لي أن النجاح لا يقاس بعدد مرات السقوط، بل بالإصرار على النهوض من جديد.

كما أتوجه بالشكر الجزيل إلى الأستاذة المؤطرة السيدة بلحمزي فهيمة، على ما قدمته من توجيهات قيمة ونصائح علمية ومتابعة مستمرة كان لها الأثر الكبير في إنجاز هذه المذكرة.

كما أتوجه بجزيل الشكر والتقدير إلى كل من ساندني وشجعني وآمن بقدرتي على تحقيق هذا الإنجاز، وأخص بالذكر الطاقم الإداري بصفة عامة، والسيدة صافي خيرة بصفة خاصة، لما قدمته من دعم ومساندة.

وأتقدم بخالص عبارات الشكر والامتنان إلى أساتذتي الكرام الذين أناروا لي طريق العلم والمعرفة، وكان لهم الفضل بعد الله تعالى في تكويني العلمي.

ولا يفوتني أن أتقدم بالشكر إلى جميع الأصدقاء والزملاء الذين قدموا لي الدعم والمساندة خلال فترة الدراسة.

وفي الأخير، أتوجه بالشكر إلى كل من ساهم من قريب أو بعيد في إنجاز هذا العمل، سائلًا الله تعالى أن يجزي الجميع خير الجزاء.

**حسام الدين**



# مقـــدمة

## المقـدمة

الحمد لله رب العالمين، والصلاة والسلام على أشرف المرسلين سيدنا محمد صلى الله عليه وسلم، وعلى آله وصحبه أجمعين.

يشهد العالم المعاصر ثورة رقمية غير مسبوقة نتيجة التطور المتسارع في تكنولوجيا المعلومات والاتصالات، حيث أصبحت شبكة الإنترنت من أهم الوسائل التي يعتمد عليها الأفراد والمؤسسات والدول في مختلف مجالات الحياة. فقد ساهمت هذه الشبكة في تسهيل التواصل بين الأشخاص، وتبادل المعلومات والمعارف، وإنجاز المعاملات التجارية والمالية والإدارية في وقت قياسي وبأقل تكلفة ممكنة، الأمر الذي جعلها تحتل مكانة أساسية في المجتمع الحديث.

وقد أدى الانتشار الواسع لاستخدام الإنترنت والتطبيقات الرقمية إلى تحقيق العديد من المزايا والفوائد التي انعكست إيجابًا على التنمية الاقتصادية والاجتماعية والعلمية، غير أن هذه المزايا صاحبتها مجموعة من المخاطر والتحديات الأمنية والقانونية التي أفرزت أنماطًا جديدة من الإجرام لم تكن معروفة في السابق، والتي يطلق عليها اصطلاحًا "جرائم الإنترنت" أو "الجرائم الإلكترونية".

وتعد جرائم الإنترنت من الظواهر الإجرامية الحديثة التي ارتبط ظهورها بالتقدم التكنولوجي والتطور المعلوماتي، حيث تستهدف الأنظمة المعلوماتية أو تستخدم الوسائل الإلكترونية كأداة لارتكاب الأفعال الإجرامية. وقد شهدت هذه الجرائم تطورًا ملحوظًا من حيث الأساليب والوسائل المستخدمة في ارتكابها، مما جعلها تشكل تهديدًا حقيقيًا للأفراد والمؤسسات والدول، خاصة في ظل الاعتماد المتزايد على التكنولوجيا الرقمية في مختلف الأنشطة اليومية.

وتتميز جرائم الإنترنت بخصائص تجعلها تختلف عن الجرائم التقليدية، فهي جرائم ذات طابع تقني معقد، وغالبًا ما ترتكب عن بعد دون الحاجة إلى التواجد المادي للجاني في مكان وقوع الجريمة، كما أنها تتسم بسرعة التنفيذ وسهولة إخفاء آثارها وصعوبة اكتشاف

مرتكبيها. إضافة إلى ذلك، فإن العديد منها يتجاوز الحدود الجغرافية للدول، الأمر الذي يطرح إشكالات قانونية تتعلق بالاختصاص القضائي والتعاون الدولي وآليات تسليم المجرمين وتبادل المعلومات.

وقد ساهمت التطورات التقنية الحديثة في ظهور صور متعددة لجرائم الإنترنت، من بينها جرائم الاختراق غير المشروع للأنظمة المعلوماتية، وسرقة البيانات والمعلومات، والاحتيال الإلكتروني، والتزوير الإلكتروني، وانتهاك الحياة الخاصة، والابتزاز الإلكتروني، ونشر الفيروسات والبرمجيات الخبيثة، والاعتداء على الملكية الفكرية، فضلًا عن الجرائم المرتبطة بالمحتويات غير المشروعة عبر شبكة الإنترنت.

ونظرًا للخطورة المتزايدة لهذه الجرائم وما تسببه من أضرار مادية ومعنوية جسيمة، فقد أولت مختلف التشريعات الوطنية والدولية اهتمامًا كبيرًا بمكافحتها من خلال سن قوانين خاصة وتنظيم آليات قانونية وإجرائية تمكن السلطات المختصة من تتبع مرتكبيها وملاحقتهم قضائيًا. كما تم تعزيز التعاون الدولي في هذا المجال نظرًا للطبيعة العابرة للحدود التي تتسم بها معظم الجرائم الإلكترونية.

وتبرز أهمية دراسة جرائم الإنترنت من كونها تمثل إحدى القضايا القانونية المعاصرة التي تفرض تحديات جديدة على المنظومة الجنائية التقليدية، حيث أصبح من الضروري تطوير النصوص القانونية والإجراءات القضائية بما يتوافق مع التطورات التقنية المتلاحقة. كما تكمن أهمية الموضوع في حماية الأمن المعلوماتي وصيانة الحقوق والحريات الأساسية للأفراد وضمان الثقة في البيئة الرقمية.

أما الأسباب التي دفعت إلى اختيار هذا الموضوع فتتمثل في الانتشار الواسع لجرائم الإنترنت في السنوات الأخيرة، وتزايد آثارها السلبية على مختلف فئات المجتمع، إضافة إلى الرغبة في التعرف على الإطار القانوني المنظم لهذه الجرائم ومدى فعاليته في تحقيق الحماية الجنائية المنشودة.

وتتمحور إشكالية هذه الدراسة حول السؤال الرئيسي الآتي:

هل حققت السياسة الجنائية الجزائرية التوازن بين حماية المجتمع من جرائم الأنترنت و ضمان الحقوق و الحريات الفردية في البيئة الرقمية ؟

ويتفرع عن هذه الإشكالية عدد من التساؤلات الفرعية:

- ما المقصود بجرائم الإنترنت وما أهم خصائصها؟
- ما هي أهم صور وأنواع الجرائم الإلكترونية؟
- ما هي الأركان القانونية اللازمة لقيام جرائم الإنترنت؟
- ما هي الآليات القانونية والإجرائية المقررة لمكافحة هذه الجرائم؟
- وما مدى فعالية التشريعات الوطنية والدولية في مواجهة التحديات التي تفرضها الجرائم الإلكترونية؟

وللإجابة عن هذه التساؤلات تم الاعتماد على المنهج الوصفي لتحليل المفاهيم الأساسية المتعلقة بجرائم الإنترنت، والمنهج التحليلي لدراسة النصوص القانونية المنظمة لها، مع الاستعانة بالمنهج المقارن في بعض المواضع لإبراز أوجه التشابه والاختلاف بين مختلف التشريعات.

وقد تم تقسيم هذه الدراسة إلى فصلين رئيسيين؛ خصص الفصل الأول للإطار المفاهيمي والنظري لجرائم الإنترنت من خلال دراسة تعريفها وخصائصها وأنواعها وأركانها القانونية، بينما تم تخصيص الفصل الثاني لدراسة الحماية القانونية المقررة لمكافحة هذه الجرائم، سواء من خلال القوانين العامة أو الخاصة، بالإضافة إلى بيان الإجراءات القانونية المتعلقة بالتحري والتحقيق والإثبات والتعاون الدولي.

وفي الأخير، نأمل أن تسهم هذه الدراسة في إثراء البحث العلمي في مجال الجرائم الإلكترونية، وإبراز أهم التحديات القانونية التي تفرضها الثورة الرقمية، واقتراح بعض الحلول التي من شأنها تعزيز الحماية القانونية والأمنية لمستخدمي شبكة الإنترنت.



# الفصل الأول

## الاطار النظري لجرائم الانترنت

**مـــقدمة :**

شهد العالم خلال العقود الأخيرة ثورة تكنولوجية هائلة مست مختلف جوانب الحياة، حيث أصبح استخدام الحاسوب وشبكة الإنترنت جزءًا أساسيًا من الأنشطة اليومية للأفراد والمؤسسات والدول. وقد ساهم هذا التطور في تسهيل تبادل المعلومات وتسريع المعاملات وتحقيق التواصل الفوري بين مختلف أنحاء العالم، الأمر الذي انعكس إيجابًا على مختلف المجالات الاقتصادية والاجتماعية والعلمية.

غير أن هذه التطورات التقنية لم تخل من آثار سلبية، إذ أفرزت أنماطًا جديدة من السلوك الإجرامي عرفت بجرائم الإنترنت أو الجرائم الإلكترونية، والتي استغل مرتكبوها الوسائل التكنولوجية الحديثة لارتكاب أفعال غير مشروعة تمس بالأشخاص أو الأموال أو الأنظمة المعلوماتية. وقد تميزت هذه الجرائم بخصائص خاصة جعلتها تختلف عن الجرائم التقليدية، سواء من حيث وسائل ارتكابها أو طبيعة مرتكبيها أو صعوبة اكتشافها وإثباتها.

ونظرًا لحداثة هذا النوع من الجرائم وتطوره المستمر، فقد تعددت الاجتهادات الفقهية والقانونية بشأن تحديد مفهومه وبيان خصائصه وأركانه وصوره المختلفة. كما أصبح من الضروري الإحاطة بالإطار النظري للجريمة الإلكترونية لفهم طبيعتها القانونية والوقوف على أهم التحديات التي تطرحها في المجال الجنائي.

وعليه، يهدف هذا الفصل إلى دراسة الجوانب النظرية المتعلقة بجرائم الإنترنت من خلال التطرق إلى مفهومها وخصائصها، ثم بيان أركانها القانونية وأهم أنواعها، وذلك وفق التقسيم الآتي :

**المبحث الاول : ماهية جرائم الانترنت**

أصبح الإنترنت في العصر الحديث من أهم وسائل الاتصال وتبادل المعلومات، غير أن هذا التطور التكنولوجي صاحبه ظهور مخاطر جديدة تمثلت في استغلال هذه الوسيلة لارتكاب أفعال غير مشروعة تمس بالأفراد والمؤسسات والأنظمة المعلوماتية. وقد فرضت

جرائم الإنترنت نفسها كأحد أبرز التحديات القانونية، لما تتميز به من طابع تقني يتطلب فهماً خاصاً لطرق ارتكابها وآثارها.

وتكمن خصوصية هذه الجرائم في اعتمادها على الوسائط الإلكترونية، مما يجعلها تختلف عن الجرائم التقليدية من حيث طبيعتها ووسائل تنفيذها وطرق إثباتها. لذلك كان من الضروري تحديد مفهوم جرائم الإنترنت وبيان خصائصها الأساسية لفهم الإطار القانوني الذي يحكمها. وعليه، سيتم تناول ماهية جرائم الإنترنت من خلال دراسة تعريفها وخصائصها في هذا المبحث.

**المطلب الاول : تعريف جرائم الانترنت**

ظهرت جرائم الإنترنت مع ظهور الحواسيب الإلكترونية وتطور وسائل الاتصال الحديثة، حيث كانت البدايات الأولى لهذه الجرائم مرتبطة بمحاولات اختراق الأنظمة المعلوماتية في المؤسسات الحكومية والعسكرية خلال ستينيات وسبعينيات القرن العشرين. ومع انتشار استخدام الحاسوب في مختلف المجالات الاقتصادية والاجتماعية، بدأت تظهر أشكال جديدة من الجرائم تستهدف البيانات والمعلومات المخزنة داخل الأنظمة الإلكترونية.

وفي ثمانينيات القرن الماضي، شهد العالم تطوراً ملحوظاً في استخدام شبكات الحاسوب، الأمر الذي أدى إلى ازدياد حالات الدخول غير المشروع إلى الأنظمة المعلوماتية وسرقة البيانات. كما ساهم انتشار شبكة الإنترنت في التسعينيات في توسيع نطاق هذه الجرائم، حيث أصبح المجرمون قادرين على تنفيذ أفعالهم عن بعد دون الحاجة إلى التواجد في مكان الجريمة.

ومع التطور السريع للتكنولوجيا الرقمية وظهور التجارة الإلكترونية والخدمات المصرفية عبر الإنترنت ووسائل التواصل الاجتماعي، تنوعت صور الجرائم الإلكترونية لتشمل الاحتيال الإلكتروني، وسرقة الهوية الرقمية، واختراق الحسابات الإلكترونية، ونشر البرمجيات الخبيثة، والتجسس الإلكتروني، والاعتداء على المعطيات الشخصية. وقد أدى

ذلك إلى اهتمام المشرعين بوضع قواعد قانونية خاصة لمواجهة هذه الجرائم والحد من آثارها السلبية على الأفراد والمؤسسات والدول[1].

كما شهد القرن الحادي والعشرون تطوراً نوعياً في الجرائم الإلكترونية نتيجة الاعتماد المتزايد على التقنيات الرقمية والذكاء الاصطناعي والحوسبة السحابية، مما جعل هذه الجرائم أكثر تعقيداً وصعوبة في الكشف عنها وتتبع مرتكبيها. لذلك اتجهت الدول إلى تعزيز التعاون الدولي وإبرام الاتفاقيات المتعلقة بمكافحة الجريمة الإلكترونية[2].

**الفرع الاول : التعريف الفقهي**

تعد جرائم الإنترنت من الظواهر الإجرامية الحديثة التي ظهرت نتيجة التطور المتسارع في مجال تكنولوجيا الإعلام والاتصال، حيث لم يعد النشاط الإجرامي مقتصرًا على الوسائل التقليدية، بل امتد إلى الفضاء الرقمي مستغلًا الحواسيب والشبكات الإلكترونية في ارتكاب الأفعال المجرمة قانونًا.

لم يستقر الفقه على تعريف موحد لجرائم الإنترنت، نظرًا لحداثة الظاهرة وتطورها التقني المستمر، غير أن الفقهاء حاولوا وضع تعريفات تعكس طبيعتها الخاصة وتميزها عن الجرائم التقليدية.

**التعريف الأول:**

تعد جرائم الإنترنت من الظواهر الإجرامية الحديثة التي ظهرت نتيجة التطور المتسارع في مجال تكنولوجيا الإعلام والاتصال، حيث لم يعد النشاط الإجرامي مقتصرًا على الوسائل التقليدية، بل امتد إلى الفضاء الرقمي مستغلًا الحواسيب والشبكات الإلكترونية في ارتكاب الأفعال المجرمة قانونًا.[3]

[1]– عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2013، ص 45

[2]– محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015، ص 27

[3]– محمد صبحي نجم، جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2018، ص 25

وقد عرف الفقه جرائم الإنترنت بعدة تعريفات، نظرًا لتعدد صورها وتطور أساليب ارتكابها. فيعرفها بعض الفقه بأنها: "كل سلوك غير مشروع يتم باستخدام الحاسب الآلي أو الشبكات المعلوماتية ويترتب عليه الاعتداء على الأشخاص أو الأموال أو البيانات الإلكترونية."

كما عرفت بأنها: "كل فعل عمدي يتم عبر الوسائل الإلكترونية ويستهدف المساس بسرية أو سلامة أو توافر المعلومات المخزنة أو المنقولة عبر الأنظمة المعلوماتية.

ويلاحظ من خلال هذه التعريفات أن الفقه ركز على عنصرين أساسيين هما استخدام الوسائل المعلوماتية ووقوع الاعتداء على مصلحة يحميها القانون.

ومن جانب آخر، يرى بعض الفقه أن الجريمة الإلكترونية هي الجريمة التي يكون فيها الحاسوب أو الشبكة المعلوماتية إما محلًا للجريمة أو وسيلة لارتكابها، وهو تعريف واسع يسمح بإدراج مختلف الأفعال الإجرامية

المرتبطة بالبيئة الرقمية. [1]

يعرفها بعض الفقه بأنها:

"كل سلوك غير مشروع يتم باستخدام الحاسوب أو شبكة الإنترنت ويترتب عليه اعتداء على مصلحة يحميها القانون ."[2]"

**التعريف الثاني:**

وعرّفها اتجاه فقهي آخر بأنها:

"الجرائم التي تُرتكب باستخدام أنظمة المعالجة الآلية للمعطيات أو الشبكات المعلوماتية، سواء كانت هذه الأنظمة وسيلة لارتكاب الجريمة أو محلًا لها". [3]

**التعريف الثالث:**

[1]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2016، ص 18

[2]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، دار هومة، الجزائر.

[3]– عبد القادر قادة، جرائم أنظمة المعالجة الآلية للمعطيات، دار الجامعة الجديدة، الجزائر

كما عرّفها بعض الفقه الجزائري بأنها:

"كل فعل عمدي غير مشروع يرتكب عبر نظام معلوماتي ويستهدف البيانات أو البرامج أو الشبكات الإلكترونية". [1]

كما عرّفها جانب آخر من الفقه بأنها:

"كل نشاط إجرامي تستخدم فيه التقنية الرقمية كوسيلة أو محل للجريمة". [2]

ويرى بعض الفقه أن جريمة الإنترنت قد تكون جريمة تقليدية ارتكبت بوسيلة إلكترونية، مثل النصب الإلكتروني أو التشهير عبر مواقع التواصل. [3]

**الفرع الثاني : التعريف القانوني**

لم يضع المشرّع الجزائري تعريفًا صريحًا جامعًا مانعًا لمصطلح "جرائم الإنترنت"، غير أنه تناولها من خلال نصوص قانونية متفرقة، خاصة في قانون العقوبات والقوانين الخاصة المتعلقة بتكنولوجيات الإعلام والاتصال.

**أولاً: في قانون العقوبات الجزائري**

أدرج المشرع جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن المواد 394 مكرر إلى 394 مكرر 7، حيث جرّم أفعالًا مثل الدخول غير المشروع إلى نظام معلوماتي، حذف أو تعديل المعطيات، وعرقلة سير النظام[4].

**ثانيًا: في القانون الخاص (قانون 09-04)**

استعمل المشرع مصطلح: "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، ويقصد بها الجرائم التي ترتكب باستعمال أنظمة المعلومات أو الشبكات الإلكترونية، أو التي تستهدف هذه الأنظمة والمعطيات. [1]

---

[1]– محمد حزيط، جرائم الإعلام الآلي والإنترنت في التشريع الجزائري، دار هومة، الجزائر

[2]– محمود نجيب حسني، شرح قانون العقوبات – القسم العام، دار النهضة العربية، القاهرة، 2006، ص 77.

[3]– محمد صبحي نجم، الجرائم الواقعة على نظم المعلومات، دار الثقافة للنشر، عمان، 2010، ص 19.

[4]– الأمر رقم 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات المعدل والمتمم ، المواد 394 مكرر إلى 394 مكرر7

**ثالثًا: في قانون حماية المعطيات الشخصية**

جرّم القانون الأفعال المتعلقة بالمعالجة غير المشروعة للبيانات ذات الطابع الشخصي، باعتبارها من صور الجرائم المرتبطة بالفضاء الرقمي[2].

لم يضع المشرّع الجزائري تعريفًا صريحًا لمصطلح "جريمة الإنترنت"، وإنما استعمل مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[3]."

ويقصد بها الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات، سواء بالاعتداء على سرية البيانات أو سلامتها أو توفرها. [4]

كما وسّع المشرّع نطاق الحماية ليشمل المعطيات ذات الطابع الشخصي بموجب قانون 18-07 [5].

**خلاصة التعريف القانوني**

يمكن القول إن التعريف القانوني لجرائم الإنترنت في التشريع الجزائري هو:

"كل فعل مجرّم قانونًا يُرتكب باستعمال أنظمة المعالجة الآلية للمعطيات أو شبكات الاتصال الإلكترونية، أو يستهدف هذه الأنظمة أو المعطيات، ويترتب عليه اعتداء على مصلحة يحميها القانون".

**المطلب الثاني خصائص جرائم الانترنت**

تتميز جرائم الإنترنت بخصوصية تميزها عن الجرائم التقليدية، وذلك بالنظر إلى ارتباطها الوثيق بالتطور التكنولوجي واعتمادها على الوسائل المعلوماتية الحديثة في ارتكابها. فقد أفرزت البيئة الرقمية نمطًا جديدًا من السلوك الإجرامي يتميز بالسرعة، وصعوبة الكشف

---

[1]- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي..

[3]- المادة 2 من القانون رقم 09-04، الجريدة الرسمية رقم 47 لسنة 2009.

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

[5]- المادة 3 من القانون 18-07، الجريدة الرسمية رقم 34 لسنة 2018.

عن مرتكبيه، وتجاوز الحدود الجغرافية، مما جعل مواجهتها تتطلب آليات قانونية وتقنية خاصة. كما تتسم هذه الجرائم بتنوع صورها وتعدد أهدافها، إذ قد تستهدف الأنظمة المعلوماتية أو البيانات أو الأموال أو الحقوق الشخصية. ومن ثم، فإن دراسة خصائص جرائم الإنترنت تعد أمرًا ضروريًا لفهم طبيعتها وتمييزها عن غيرها من الجرائم، وذلك من خلال التطرق إلى خصائصها التقنية والقانونية.

**الفرع الأول الخصائص التقنية**

**1- الطابع غير المادي**

جرائم الإنترنت تقع على بيانات ومعلومات رقمية غير ملموسة، مثل اختراق الحسابات أو سرقة البيانات، بخلاف الجرائم التقليدية التي تستهدف أشياء مادية.

**2- السرعة الفائقة في التنفيذ**

يمكن ارتكاب الجريمة الإلكترونية خلال ثوانٍ معدودة (مثل تحويل أموال أو نشر محتوى تشهيري)، بفضل سرعة الشبكات الرقمية.

**3- عابرة للحدود (الطابع الدولي)**

لا تعترف جرائم الإنترنت بالحدود الجغرافية، فقد يكون الجاني في دولة والضحية في دولة أخرى، مما يصعّب مسألة الاختصاص القضائي.

**4- صعوبة الاكتشاف والإثبات**

بسبب استعمال وسائل التشفير وإخفاء الهوية (VPN، حسابات وهمية)، يصعب تحديد هوية الجاني أو جمع الأدلة الرقمية.

**5- سهولة محو الأدلة**

الأدلة الرقمية يمكن حذفها أو تعديلها بسرعة، ما يجعل التحقيق يتطلب خبرة تقنية عالية.

**6- الاعتماد على الوسائل التقنية**

ترتكب باستعمال الحاسوب أو الهاتف الذكي أو الشبكات المعلوماتية كوسيلة أو محل للجريمة.

تتميز جرائم الإنترنت بأنها جرائم رقمية تعتمد على أنظمة المعالجة الآلية للمعطيات، أي أنها لا تقوم إلا بوجود وسيط تقني يتمثل في الحاسوب أو الشبكات المعلوماتية[1].

كما أنها جرائم عابرة للحدود، إذ يمكن أن يكون الجاني في دولة والضحية في دولة أخرى، ويتم تنفيذ الجريمة عبر خوادم موزعة عالميًا [2].

وتتسم كذلك بسرعة التنفيذ وإمكانية محو آثارها في وقت وجيز، مما يصعّب عملية اكتشافها وإثباتها[3].

كما أن الدليل فيها يكون دليلاً رقمياً، وهو دليل غير مادي يتطلب خبرة تقنية لاستخراجه وتحليله[4].

**الفرع الثاني الخصائص القانونية**

**1- حداثة التجريم**

جرائم الإنترنت حديثة نسبياً مقارنة بالقانون الجنائي التقليدي، مما أدى إلى ضرورة استحداث نصوص قانونية خاصة بها.

**2- تطور أساليبها المستمر**

التكنولوجيا تتطور بسرعة، وبالتالي تتغير أساليب الجريمة، مما يجعل التشريع في حالة تحديث دائم.

**3- خصوصية الإثبات**

تعتمد على الأدلة الرقمية (IP، سجلات إلكترونية، رسائل إلكترونية)، وهي تختلف عن وسائل الإثبات التقليدية.

---

[1]- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2003، ص 35

[2]- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2009، ص 52..

[3]- أحمد عبد الكريم سلامة، القانون الجنائي للمعلوماتية، دار النهضة العربية، القاهرة، 2005، ص 64..

[4]- القانون رقم 09-04 المؤرخ في 05 أوت 2009، المادة 6، الجريدة الرسمية رقم 47.

**4- صعوبة تحديد الاختصاص القضائي**

بسبب الطابع العابر للحدود، قد تتداخل اختصاصات عدة دول، مما يستدعي التعاون القضائي الدولي.

**5- خطورة آثارها**

قد تمس الأمن الوطني، الاقتصاد، الحياة الخاصة، وسمعة الأفراد، وأحيانًا تسبب خسائر مالية ضخمة في وقت قصير .

تتميز جرائم الإنترنت بأنها قد تمس عدة مصالح قانونية في آن واحد، مثل حماية الحياة الخاصة، الملكية، وأمن الدولة المعلوماتي[1].

كما أنها جرائم قد تكون وقتية أو مستمرة، فالدخول غير المشروع إلى نظام معلوماتي يُعد جريمة وقتية، بينما الاحتفاظ غير المشروع بالمعطيات قد يُعد جريمة مستمرة[2].

وتتميز كذلك بإمكانية ارتكابها من قبل شخص طبيعي أو معنوي، حيث أقر المشرع الجزائري مسؤولية الشخص المعنوي جزائياً[3].

ومن الخصائص الأساسية لجرائم الإنترنت أنها جرائم ذات طبيعة تقنية معقدة، إذ تعتمد على استخدام وسائل إلكترونية وبرامج معلوماتية تتطلب معرفة تقنية متخصصة. فمرتكب الجريمة الإلكترونية غالباً ما يمتلك قدراً من الخبرة في مجال الحاسوب والشبكات والبرمجيات، الأمر الذي يمكنه من استغلال الثغرات الأمنية أو اختراق الأنظمة المعلوماتية أو التلاعب بالبيانات الإلكترونية. وتؤدي هذه الطبيعة التقنية إلى صعوبة اكتشاف الجريمة وإثباتها مقارنة بالجرائم التقليدية، مما يستوجب الاستعانة بخبراء متخصصين في مجال الأدلة الرقمية والتحليل الجنائي المعلوماتي.

---

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

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، دار هومة، الجزائر، 2017، ص 112..

[3]- المادة 51 مكرر من قانون العقوبات الجزائري.

كما تتميز جرائم الإنترنت بأنها جرائم عابرة للحدود الوطنية، حيث لا تعترف بالحدود الجغرافية أو السياسية للدول. فالجاني قد يكون موجوداً في دولة معينة، بينما يوجد الضحية في دولة أخرى، وقد تكون الخوادم المستعملة في تنفيذ الجريمة موجودة في دولة ثالثة. ويؤدي هذا الوضع إلى إثارة العديد من الإشكالات القانونية المتعلقة بتحديد الاختصاص القضائي والقانون الواجب التطبيق، فضلاً عن صعوبات التعاون الدولي في مجال التحقيق والمتابعة القضائية[1].

ومن الخصائص المهمة أيضاً السرعة الفائقة في ارتكاب الجريمة الإلكترونية، إذ يمكن تنفيذ عملية اختراق أو تحويل أموال أو سرقة بيانات في ثوان معدودة، وهو ما يجعل التدخل السريع للجهات المختصة أمراً ضرورياً للحد من الأضرار المترتبة على الجريمة. كما أن هذه السرعة تمنح المجرم فرصة لإخفاء آثار جريمته أو نقل البيانات المسروقة إلى أماكن متعددة خلال فترة وجيزة[2].

وتتسم جرائم الإنترنت كذلك بسهولة إتلاف الأدلة أو محوها، فالأدلة الرقمية بطبيعتها قابلة للتعديل أو الحذف أو الإخفاء باستخدام برامج متخصصة، الأمر الذي يفرض على جهات التحقيق اتباع إجراءات دقيقة عند جمع الأدلة الرقمية وحفظها لضمان سلامتها وحجيتها أمام القضاء. ولهذا السبب أصبحت الخبرة التقنية تلعب دوراً محورياً في إثبات الجرائم الإلكترونية والكشف عن مرتكبيها[3].

ومن جهة أخرى، تتميز جرائم الإنترنت بانخفاض التكلفة المادية اللازمة لارتكابها مقارنة بالجرائم التقليدية، حيث يكفي في كثير من الأحيان توفر جهاز حاسوب واتصال بالإنترنت وبعض البرامج التقنية لتنفيذ أفعال إجرامية قد تلحق أضراراً جسيمة بالأفراد أو

[1]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريع المقارن، دار الفكر الجامعي، الإسكندرية، 2007، ص 27

[2]– محمد أمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص 37

[3]– محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2010، ص 30

المؤسسات أو حتى الدول. وقد ساهم هذا العامل في زيادة عدد الجرائم الإلكترونية وانتشارها على نطاق واسع.

كما أن هذه الجرائم تتصف بصعوبة اكتشاف الجاني الحقيقي، وذلك بسبب استخدام وسائل إخفاء الهوية مثل الشبكات الافتراضية الخاصة (VPN) والخوادم الوسيطة وتقنيات التشفير المختلفة. وتسمح هذه الوسائل للمجرمين بإخفاء مواقعهم الحقيقية وهوياتهم الرقمية، مما يجعل عملية تعقبهم وتقديمهم للعدالة أكثر تعقيداً.

وتتميز جرائم الإنترنت أيضاً بتعدد صورها وأشكالها، فهي لا تقتصر على نوع معين من الاعتداءات، وإنما تشمل جرائم اختراق الأنظمة المعلوماتية، والاحتيال الإلكتروني، وسرقة البيانات، وانتهاك الخصوصية، ونشر البرمجيات الخبيثة، والتزوير الإلكتروني، والابتزاز عبر الإنترنت وغيرها من الأفعال الإجرامية التي تتطور باستمرار مع تطور التكنولوجيا[1].

أما من الناحية القانونية، فإن جرائم الإنترنت تثير تحديات خاصة أمام المشرع الجنائي، إذ تتطلب تحديثاً مستمراً للنصوص القانونية لمواكبة المستجدات التقنية. فالتطور السريع في مجال تكنولوجيا المعلومات يؤدي إلى ظهور أنماط جديدة من الجرائم لم تكن معروفة سابقاً، وهو ما يفرض على المشرع التدخل باستمرار لسد الفراغ التشريعي وضمان توفير الحماية القانونية اللازمة للأفراد والمؤسسات.

وتؤدي جرائم الإنترنت إلى المساس بعدد كبير من المصالح القانونية المحمية، مثل الحق في الخصوصية وسرية المراسلات والملكية الفكرية وأمن المعاملات الإلكترونية وسلامة الأنظمة المعلوماتية. لذلك أصبحت مكافحتها تمثل ضرورة قانونية وأمنية واقتصادية في ظل الاعتماد المتزايد على التكنولوجيا الرقمية في مختلف مجالات الحياة[2].

---

[1]– محمد سعيد نمور، شرح قانون الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان ، ص 84

[2]– قانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

## المبحث الثاني : اركان و انواع جرائم الانترنت

تتميز جرائم الإنترنت بخصوصيتها القانونية والتقنية، إذ لا تقوم بمجرد استعمال الوسائل الإلكترونية، وإنما تستلزم توافر مجموعة من الأركان التي تشكل أساس قيام الجريمة، سواء تعلق الأمر بالركن الشرعي أو المادي أو المعنوي، مع مراعاة الطبيعة الخاصة للبيئة الرقمية التي ترتكب فيها هذه الأفعال. كما أن التطور المستمر في استخدام تقنيات المعلومات والاتصال أدى إلى تنوع صور الجرائم الإلكترونية وتعدد أشكالها، فمنها ما يستهدف الأنظمة والبيانات المعلوماتية، ومنها ما يمس الأموال أو الحياة الخاصة أو الأمن العام. لذلك يتناول هذا المبحث دراسة أركان جرائم الإنترنت من جهة، وأنواعها وصورها المختلفة من جهة أخرى، بهدف بيان خصوصيتها ومدى خطورتها على الأفراد والمؤسسات والمجتمع.

### المطلب الأول : أركان جرائم الانترنت

تخضع الجرائم الإلكترونية للقواعد العامة في القانون الجنائي من حيث ضرورة توافر الأركان اللازمة لقيام الجريمة، وهي الركن الشرعي والركن المادي والركن المعنوي. غير أن الطبيعة التقنية لهذه الجرائم تمنح هذه الأركان بعض الخصوصية التي تميزها عن الجرائم التقليدية

#### الفرع الاول : الركن الشرعي

#### الركن الشرعي (مبدأ الشرعية )

يقصد به ضرورة وجود نص قانوني يجرّم الفعل قبل ارتكابه، تطبيقًا لمبدأ:

"لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون."

في الجزائر، تم تجريم أفعال الاعتداء على أنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

كما نص قانون العقوبات الجزائري على جرائم المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر إلى 394 مكرر 7.

إذن لا يمكن متابعة شخص بجريمة إلكترونية إلا إذا وجد نص صريح يجرم الفعل.

يقصد بالركن الشرعي خضوع الجريمة لمبدأ الشرعية الجنائية الذي يقضي بأنه "لا جريمة ولا عقوبة إلا بنص."[1]

وقد تجسد هذا المبدأ في مجال جرائم الإنترنت من خلال إدراج نصوص خاصة ضمن قانون العقوبات، لاسيما المواد 394 مكرر إلى 394 مكرر 7 .

كما عززه المشرع بإصدار القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2].

وقد فرض التطور التكنولوجي على المشرع الجزائري إدراج نصوص خاصة لمواجهة الجرائم الإلكترونية، خاصة بعد ظهور أنماط جديدة من الاعتداءات لم تكن معروفة من قبل، مثل الدخول غير المشروع إلى الأنظمة المعلوماتية وسرقة البيانات الإلكترونية والاعتداء على المعالجة الآلية للمعطيات.

**الفرع الثاني : الركن المادي و المعنوي**

**الركن المادي**

هو السلوك الإجرامي الملموس الذي يصدر عن الجاني ويؤدي إلى نتيجة إجرامية .

الركن المادي هو المظهر الخارجي للجريمة والذي يتجسد في السلوك الإجرامي الذي يصدر عن الجاني ويؤدي إلى نتيجة إجرامية يعاقب عليها القانون.

وفي الجرائم الإلكترونية قد يتمثل الركن المادي في عدة صور منها: [3]

- الدخول غير المشروع إلى الأنظمة المعلوماتية.

---

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص 418

[2]- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]- عبد العزيز سعد، الجرائم الواقعة على نظم المعلومات، دار هومة، الجزائر، 2019، ص 73

- اعتراض البيانات الإلكترونية.
- إتلاف أو حذف المعطيات الرقمية.
- نشر الفيروسات والبرمجيات الخبيثة.
- الاستيلاء على البيانات البنكية.
- الاحتيال عبر الإنترنت.

ويتكون الركن المادي من ثلاثة عناصر :

**السلوك الإجرامي:**

مثل الدخول غير المشروع إلى نظام معلوماتي، نشر فيروسات، سرقة بيانات، قرصنة حسابات.

**النتيجة الإجرامية:**

كإتلاف البيانات، تعطيل النظام، الاستيلاء على معلومات سرية.

**العلاقة السببية:**

أي وجود رابط بين الفعل المرتكب والضرر الناتج عنه.

يتميز الركن المادي في جرائم الإنترنت بأنه غالبًا ما يتم عن بُعد ودون تلامس مادي مباشر.

يتمثل الركن المادي في السلوك الإجرامي الذي يمس نظام المعالجة الآلية للمعطيات، مثل الدخول غير المشروع أو حذف البيانات أو تغييرها[1].

كما يشمل اعتراض المعطيات أثناء انتقالها عبر الشبكات[2].

ويتحقق الركن المادي بمجرد تحقق الفعل دون اشتراط وقوع ضرر فعلي في بعض الجرائم[3].

---

[1]– المادة 394 مكرر من قانون العقوبات الجزائري.

[2]– المادة 394 مكرر 1 من قانون العقوبات الجزائري

[3]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ص 118

**الركن المعنوي**

وهو القصد الجنائي، أي الإرادة والعلم بارتكاب الفعل المجرّم.

يقصد بالركن المعنوي الحالة النفسية للجاني أثناء ارتكاب الجريمة، أي العلاقة الذهنية التي تربطه بالفعل الإجرامي.

والأصل أن الجرائم الإلكترونية من الجرائم العمدية التي تتطلب توافر القصد الجنائي[1].

وينقسم إلى:

**القصد العام:**

علم الجاني بأنه يقوم بفعل غير مشروع واتجاه إرادته إلى ارتكابه.

**القصد الخاص**

مثل نية الاحتيال، أو نية الإضرار، أو تحقيق منفعة غير مشروعة.

أغلب الجرائم الإلكترونية جرائم عمدية، لكن قد توجد صور خطأ غير عمدي في بعض الحالات (مثل الإهمال في حماية المعطيات).

الأصل أن جرائم الإنترنت جرائم عمدية تتطلب توافر القصد الجنائي العام، أي العلم بالفعل وإرادة ارتكابه[2].

ويتحقق القصد الجنائي بعلم الجاني بأنه يدخل نظاماً معلوماتياً دون وجه حق واتجاه إرادته إلى ذلك[3].

**خلاصة مختصرة**

أركان جرائم الإنترنت هي:

- الركن الشرعي (وجود نص قانوني)
- الركن المادي (سلوك + نتيجة + علاقة سببية)

---

[1]– أحسن بوسقيعة، الوجيز في القانون الجنائي العام، المرجع السابق، ص 162

[2]– المرجع: محمود نجيب حسني، شرح قانون العقوبات – القسم العام، ص 305

[3]– المادة 394 مكرر من قانون العقوبات الجزائري

**المطلب الثاني : انواع جرائم الانترنت**

تتعدد صور الجرائم الإلكترونية وتتنوع تبعًا للمصلحة المعتدى عليها، ويمكن تقسيمها إلى جرائم ماسة بالأشخاص وجرائم ماسة بالأموال والأنظمة المعلوماتية

**الفرع الاول : الجرائم الماسة بالاشخاص**

تُعد الجرائم الماسة بالأشخاص من أبرز صور جرائم الإنترنت، حيث تستهدف الحقوق الشخصية للأفراد كالشرف والاعتبار والخصوصية والحرية النفسية. وقد ساهم الانتشار الواسع لوسائل التواصل الاجتماعي والتطبيقات الرقمية في تسهيل ارتكاب هذه الجرائم، مما أدى إلى زيادة خطورتها واتساع نطاق آثارها.

**أولاً: جريمة التشهير والقذف الإلكتروني**

**1. تعريفها**

يقصد بالتشهير الإلكتروني نشر أو إذاعة معلومات أو عبارات أو صور عبر شبكة الإنترنت من شأنها المساس بسمعة شخص أو اعتباره بين أفراد المجتمع. أما القذف الإلكتروني فهو إسناد واقعة محددة إلى شخص عبر الوسائل الإلكترونية من شأنها النيل من شرفه أو اعتباره[1].

**2. صورها**

- نشر تعليقات مسيئة على مواقع التواصل الاجتماعي.
- نشر أخبار كاذبة عن شخص معين.
- إنشاء صفحات أو حسابات للإساءة إلى الضحية.
- تداول صور أو فيديوهات بقصد التشهير.

**3. أركانها**

- **الركن المادي:** نشر أو بث محتوى مسيء عبر الإنترنت.
- **الركن المعنوي:** توافر القصد الجنائي والعلم بأثر النشر.

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، 2022، ص 298.

**4. آثارها**

- المساس بسمعة الضحية.
- الإضرار بمكانته الاجتماعية والمهنية.
- حدوث أضرار نفسية ومعنوية.

**ثانياً: جريمة انتهاك الحياة الخاصة**

**1. تعريفها**

تتمثل في جمع أو تسجيل أو تخزين أو نشر المعلومات والبيانات الشخصية للأفراد دون موافقتهم أو دون سند قانوني.

**2. صورها**

- نشر الصور الشخصية دون إذن.
- تسريب المحادثات الخاصة.
- اختراق البريد الإلكتروني والحسابات الشخصية.
- نشر البيانات الشخصية على المواقع الإلكترونية.

**3. خطورتها**

تمس هذه الجريمة أحد الحقوق الأساسية للإنسان، وهو الحق في الخصوصية، كما قد تؤدي إلى الابتزاز أو الإضرار بسمعة الضحية[1].

**ثالثاً: جريمة انتحال الشخصية الإلكترونية**

**1. تعريفها**

هي قيام الجاني باستخدام بيانات أو هوية شخص آخر دون إذنه بقصد خداع الغير أو تحقيق منفعة غير مشروعة أو الإضرار بصاحب الهوية[2].

[1]– محمد سعيد نمور، الحماية الجنائية للحياة الخاصة عبر الإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2018، ص 73.

[2]– عبد الفتاح بيومي حجازي، الجرائم المستحدثة واستخدام الإنترنت في القانون الجنائي، دار الفكر الجامعي، الإسكندرية، 2016، ص 117.

**2. صورها**

- إنشاء حسابات وهمية باسم الغير.
- استخدام صور أو بيانات شخصية دون ترخيص.
- إرسال رسائل أو منشورات باسم شخص آخر.

**3. آثارها**

- الإضرار بسمعة الشخص المنتحل اسمه.
- ارتكاب جرائم أخرى تحت هوية الضحية.
- فقدان الثقة في التعاملات الإلكترونية.

**رابعاً: جريمة الابتزاز الإلكتروني**

**1. تعريفها**

الابتزاز الإلكتروني هو تهديد شخص بنشر معلومات أو صور أو تسجيلات خاصة به عبر الإنترنت أو وسائل الاتصال الإلكترونية بهدف إجباره على القيام بعمل أو الامتناع عنه أو دفع مبالغ مالية[1].

**2. صورها**

- التهديد بنشر الصور الخاصة.
- التهديد بنشر المحادثات الشخصية.
- طلب أموال مقابل عدم نشر المعلومات.

**3. خطورته**

يُعد من أخطر الجرائم الإلكترونية لما يسببه من أضرار نفسية واجتماعية ومادية للضحايا.

[1]– أحمد عبد الظاهر، الجرائم الإلكترونية وأدلة الإثبات الجنائي الإلكتروني، دار النهضة العربية، القاهرة، 2020، ص 184.

**خامساً: جريمة التهديد الإلكتروني**

**1. تعريفها**

هي توجيه رسائل أو منشورات تتضمن وعيداً بإلحاق ضرر مادي أو معنوي بشخص معين باستعمال الوسائل الإلكترونية[1].

**2. صورها**

- رسائل التهديد عبر البريد الإلكتروني.
- التهديد عبر مواقع التواصل الاجتماعي.
- التهديد بنشر معلومات أو صور خاصة.

**3. آثارها**

- إثارة الخوف والرعب لدى الضحية.
- الإضرار بالاستقرار النفسي والاجتماعي.

تشكل الجرائم الماسة بالأشخاص عبر الإنترنت اعتداءً خطيراً على الحقوق الأساسية للأفراد، خاصة الحق في الشرف والاعتبار والخصوصية والأمن النفسي. ومع تزايد استخدام الوسائط الرقمية، أصبح من الضروري تعزيز الحماية القانونية والتوعية المجتمعية لمواجهة هذه الجرائم والحد من آثارها السلبية.

**الفرع الثاني : الجرائم الماسة بالاموال و الانظمة**

**الجرائم الماسة بالأموال والأنظمة المعلوماتية**

تُعد الجرائم الماسة بالأموال والأنظمة المعلوماتية من أخطر صور جرائم الإنترنت، نظراً لما تُسببه من خسائر مالية كبيرة وأضرار تمس أمن المعلومات واستقرار المعاملات الإلكترونية. وتستهدف هذه الجرائم الأموال الإلكترونية أو الأنظمة والشبكات المعلوماتية بوسائل تقنية حديثة.

[1]– عبد الرؤوف مهدي، شرح الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2019، ص 163.

**أولاً: الجرائم الماسة بالأموال**

يقصد بها الجرائم التي تستهدف الاستيلاء على الأموال أو المنافع المالية باستخدام الوسائل الإلكترونية وتقنيات المعلومات.

**1. جريمة الاحتيال الإلكتروني**

هي استخدام وسائل إلكترونية أو معلوماتية لخداع الضحية وحمله على تسليم أمواله أو بياناته المالية[1].

**صورها:**

- انتحال صفة البنوك والمؤسسات المالية.
- إرسال رسائل وهمية للحصول على البيانات البنكية.
- إنشاء مواقع إلكترونية مزيفة مشابهة للمواقع الأصلية.
- الاحتيال عبر التجارة الإلكترونية.

**أركانها:**

- استعمال وسائل احتيالية.
- وقوع الضحية في الغلط.
- تسليم المال أو المنفعة المالية.
- القصد الجنائي.

**آثارها:**

- خسائر مالية للأفراد والمؤسسات.
- زعزعة الثقة في المعاملات الإلكترونية.

[1]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2011، ص 145.

### 2. جريمة السرقة الإلكترونية

تتمثل في الاستيلاء غير المشروع على الأموال أو البيانات ذات القيمة المالية باستخدام الحاسب الآلي أو الشبكات[1].

**صورها:**

- سرقة أرصدة الحسابات البنكية.
- تحويل الأموال إلكترونياً دون إذن.
- الاستيلاء على المحافظ الرقمية.

**خصائصها:**

- تتم عن بعد.
- يصعب اكتشاف مرتكبيها.
- تعتمد على المهارات التقنية.

### 3. جريمة تزوير وسائل الدفع الإلكترونية

يقصد بها إنشاء أو تعديل أو استعمال بطاقات الدفع أو وسائل الدفع الإلكترونية بطريقة غير مشروعة[2].

**صورها:**

- استنساخ البطاقات البنكية.
- تزوير البطاقات الائتمانية.
- تعديل البيانات المخزنة إلكترونياً.

**خطورتها:**

- تهديد الاقتصاد الرقمي.

---

[1]– محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 87.

[2]– أحمد شوقي الشلقاني، جرائم الحاسب الآلي والإنترنت، دار النهضة العربية، القاهرة، 2015، ص 201.

- الإضرار بالمؤسسات المالية.

### 4. جريمة غسل الأموال الإلكترونية

هي إخفاء المصدر غير المشروع للأموال باستخدام الوسائل الإلكترونية والشبكات الرقمية[1].

**وسائلها:**

- التحويلات البنكية الإلكترونية.
- العملات الرقمية المشفرة.
- المحافظ الإلكترونية.

**مراحلها:**

- الإيداع.
- التمويه.
- الدمج.

### ثانياً: الجرائم الماسة بالأنظمة المعلوماتية

يقصد بها الأفعال غير المشروعة التي تستهدف سلامة الأنظمة والشبكات وقواعد البيانات[2].

### 1. جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية

تعرف بأنها الولوج إلى نظام معلوماتي دون ترخيص أو تجاوز حدود الترخيص الممنوح.

**صورها:**

- اختراق المواقع الإلكترونية.
- الدخول إلى قواعد البيانات السرية.
- تجاوز كلمات المرور.

[1]– محمد حسين منصور، غسل الأموال في ظل التطور التكنولوجي، دار الجامعة الجديدة، الإسكندرية، 2016، ص 58.

[2]– عبد الرؤوف مهدي، شرح جرائم الحاسب الآلي والإنترنت، دار النهضة العربية، القاهرة، 2014، ص 121.

**أضرارها:**

- كشف المعلومات السرية.
- تعطيل الأنظمة.

### 2. جريمة إتلاف أو تغيير البيانات الإلكترونية

تتمثل في حذف أو تعديل أو تشويه البيانات المخزنة داخل النظام المعلوماتي[1].

**صورها:**

- حذف الملفات.
- تغيير محتوى قواعد البيانات.
- تشويه المعلومات الإلكترونية.

**النتائج:**

- فقدان البيانات.
- تعطيل الخدمات الإلكترونية.

### 3. جريمة نشر الفيروسات والبرمجيات الخبيثة

هي إدخال برامج ضارة إلى الأنظمة المعلوماتية بهدف الإضرار بها أو السيطرة عليها[2].

**أنواعها:**

- الفيروسات.
- الديدان الإلكترونية.
- أحصنة طروادة.
- برامج الفدية.

[1]– محمد عبد الظاهر حسين، الجوانب القانونية لجرائم الإنترنت، دار النهضة العربية، القاهرة، 2017، ص 166.

[2]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، دار الفكر الجامعي، الإسكندرية، 2012، ص 193.

**آثارها:**

- تدمير البيانات.
- تعطيل الشبكات.
- الابتزاز الإلكتروني.

### 4. جريمة تعطيل الأنظمة والشبكات

تتمثل في إعاقة أو تعطيل سير الأنظمة المعلوماتية أو الشبكات الإلكترونية[1].

**صورها:**

- هجمات حجب الخدمة (DDoS).
- تعطيل المواقع الإلكترونية.
- إغراق الخوادم بالطلبات الوهمية.

**خطورتها:**

- توقف الخدمات الحكومية والمالية.
- خسائر اقتصادية كبيرة.

### 5. جريمة الاعتداء على قواعد البيانات

هي الوصول غير المشروع إلى قواعد البيانات أو نسخها أو تعديلها أو إتلافها[2].

**صورها:**

- سرقة قواعد بيانات العملاء.
- تسريب المعلومات السرية.
- بيع البيانات الشخصية.

**الأضرار:**

- انتهاك الخصوصية.

---

[1]– محمد سعيد نمور، جرائم تقنية المعلومات، دار الثقافة للنشر والتوزيع، عمان، 2018، ص 211.

[2]– محمد حسن قاسم، الحماية الجنائية للمعطيات الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2014، ص 134.

- خسائر مالية ومعنوية.

تشكل الجرائم الماسة بالأموال والأنظمة المعلوماتية تهديداً حقيقياً للأمن الاقتصادي والمعلوماتي، إذ تستهدف الأموال الرقمية والأنظمة الإلكترونية التي أصبحت أساس المعاملات الحديثة. لذلك اتجهت التشريعات، ومنها التشريع الجزائري، إلى تجريم هذه الأفعال ووضع آليات خاصة للوقاية منها ومكافحتها، مع تعزيز التعاون الوطني والدولي لملاحقة مرتكبيها.

تختلف الجريمة الإلكترونية عن الجريمة التقليدية من حيث الوسيلة المستخدمة في ارتكابها، إذ تعتمد الجريمة التقليدية على وسائل مادية ملموسة، بينما تعتمد الجريمة الإلكترونية على الحاسوب والشبكات المعلوماتية كوسيلة أساسية لتنفيذ النشاط الإجرامي. كما أن الجريمة الإلكترونية قد تقع دون مواجهة مباشرة بين الجاني والضحية.

ومن أوجه الاختلاف أيضاً أن الجريمة التقليدية غالباً ما تكون محددة النطاق الجغرافي، بينما تتميز الجريمة الإلكترونية بطابعها العابر للحدود، حيث يمكن أن يكون الجاني في دولة والضحية في دولة أخرى والخادم الإلكتروني في دولة ثالثة[1].

كما تختلف الجريمتان من حيث الأدلة والإثبات، فالأدلة في الجرائم التقليدية تكون غالباً مادية كالبصمات وآثار الجريمة، بينما تعتمد الجرائم الإلكترونية على أدلة رقمية تحتاج إلى خبرة تقنية متخصصة لجمعها وتحليلها والمحافظة عليها.

ويظهر الاختلاف كذلك في سرعة ارتكاب الجريمة، إذ يمكن تنفيذ الجريمة الإلكترونية خلال ثوان معدودة وإحداث أضرار جسيمة تمس عدداً كبيراً من الضحايا في وقت واحد، في حين تتطلب العديد من الجرائم التقليدية وقتاً أطول وجهداً أكبر لتنفيذها[2].

[1]– أحمد عبد الكريم سلامة، جرائم الحاسب الآلي والإنترنت، دار النهضة العربية، القاهرة، 2017، ص 61.

[2]– عبد القادر البقيرات، الجرائم الإلكترونية وآليات مكافحتها، دار الخلدونية، الجزائر، 2018، ص 34.

وهذه الجرائم الماسة بالأموال والأنظمة تُعد من أهم صور الجرائم المعلوماتية، لأنها تستهدف الجانب المالي أو الأنظمة والبيانات الإلكترونية، وتؤدي إلى خسائر مادية وتعطيل للخدمات الرقمية.

**أولاً: الجرائم الماسة بالأموال**

هي الجرائم التي يكون هدف الجاني منها الحصول على منفعة مالية غير مشروعة أو إلحاق ضرر بالذمة المالية للأفراد أو المؤسسات باستعمال الوسائل الإلكترونية.

**1- الاحتيال الإلكتروني**

هو استعمال وسائل تقنية (مثل البريد الإلكتروني، المواقع المزيفة، التطبيقات) لخداع الضحية ودفعه إلى تقديم أموال أو معلومات مالية[1].

أمثلة:

رسائل مزيفة تدّعي أنها من بنك وتطلب بيانات الحساب.

إنشاء متاجر إلكترونية وهمية للحصول على أموال الزبائن.

**2- سرقة الأموال عبر الإنترنت**

تتم من خلال الاستيلاء غير المشروع على الحسابات البنكية أو المحافظ الإلكترونية أو بطاقات الدفع[2].

من صورها:

سرقة بيانات البطاقات البنكية.

تحويل الأموال دون إذن صاحب الحساب.

**3- الابتزاز المالي الإلكتروني**

يقوم المجرم بتهديد الضحية بنشر معلومات أو صور أو ملفات خاصة مقابل دفع مبلغ مالي.

---

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي المقارن.

[2]- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت.

**4- القرصنة المالية**

وتتمثل في اختراق الأنظمة المالية للشركات أو المؤسسات بهدف تحويل الأموال أو التلاعب بالسجلات المالية.

**ثانياً: الجرائم الماسة بالأنظمة المعلوماتية**

هي الجرائم التي تستهدف سلامة وسرية وتوافر الأنظمة والبرامج والبيانات الإلكترونية.

**1- جريمة الدخول غير المشروع إلى الأنظمة**

هي دخول شخص إلى نظام معلوماتي دون ترخيص، سواء بهدف الاطلاع على البيانات أو استخدامها.

مثال: اختراق قاعدة بيانات مؤسسة.

**2- تعطيل الأنظمة المعلوماتية**

تتمثل في القيام بأفعال تؤدي إلى توقف أو اضطراب عمل النظام.

مثال:

هجمات حجب الخدمة (DDoS) التي تمنع المستخدمين من الوصول إلى المواقع.

**3- تخريب أو إتلاف البيانات**

يقوم الجاني بحذف أو تغيير أو إفساد المعلومات المخزنة إلكترونياً.

**4- نشر البرمجيات الخبيثة**

مثل:

الفيروسات.

برامج التجسس.

برامج الفدية التي تقوم بتشفير الملفات وطلب مقابل مالي لفك التشفير.

**5- التجسس الإلكتروني**

يهدف إلى الحصول على معلومات سرية تخص أفراداً أو مؤسسات أو دولاً[1].

[1]- قانون العقوبات الجزائري، والأحكام المتعلقة بالجرائم الإلكترونية وحماية الأنظمة المعلوماتية.

الفرق بين الجرائم الماسة بالأموال والجرائم الماسة بالأنظمة

- الجرائم الماسة بالأموال
- الجرائم الماسة بالأنظمة

الهدف الأساسي هو تحقيق مكسب مالي أو إلحاق خسارة مالية

الهدف هو اختراق أو تعطيل أو تخريب النظام

تركز على الحسابات والأموال والمعاملات

تركز على الأجهزة والبرامج والبيانات

- مثال: سرقة حساب بنكي إلكتروني
- مثال: اختراق قاعدة بيانات

## خاتمة الفصل الأول

يتضح من خلال هذا الفصل أن الجريمة الإلكترونية تمثل أحد أخطر التحديات القانونية المعاصرة، نتيجة التطور التكنولوجي المتسارع واتساع استخدام شبكة الإنترنت. كما تبين أن هذه الجرائم تتميز بخصائص فنية وقانونية خاصة تجعل مكافحتها أكثر تعقيدًا من الجرائم التقليدية، الأمر الذي دفع المشرع الجزائري إلى تطوير منظومته القانونية لمواجهتها. كما أن تعدد صور الجرائم الإلكترونية وتنوعها يقتضي توفير آليات قانونية وإجرائية فعالة لضمان حماية الأشخاص والأموال والأنظمة المعلوماتية، وهو ما سيتم التطرق إليه في الفصل الثاني المتعلق بالآليات القانونية لمكافحة جرائم الإنترنت في الجزائر.

# الفصل الثاني

# الآليات القانونية لمكافحة جرائم الانترنت في الجزائر

**تمهـــيد :**

أدى التطور المتسارع في مجال تكنولوجيا المعلومات والاتصال إلى ظهور أنماط جديدة من السلوكيات الإجرامية التي تتم عبر الفضاء الرقمي، مما فرض على مختلف التشريعات الوطنية والدولية ضرورة إعادة النظر في الوسائل القانونية التقليدية لمواجهة هذه الجرائم. فلم تعد الجريمة مرتبطة بمكان أو زمان محددين، بل أصبحت ترتكب في بيئة إلكترونية تتجاوز الحدود الجغرافية للدول، وهو ما جعل مكافحتها تمثل تحدياً قانونياً وتقنياً كبيراً أمام المشرّع والجهات المكلفة بإنفاذ القانون.

وقد سعى المشرّع الجزائري إلى مواكبة هذه التحولات من خلال وضع منظومة قانونية تهدف إلى تجريم الأفعال التي تمس الأنظمة المعلوماتية والبيانات الإلكترونية وحقوق الأفراد والمؤسسات، إضافة إلى استحداث آليات إجرائية خاصة تسمح بالبحث والتحري وجمع الأدلة الرقمية، باعتبار أن الطبيعة التقنية لهذه الجرائم تتطلب إجراءات تختلف عن تلك المعتمدة في الجرائم التقليدية.

كما أن مواجهة جرائم الإنترنت لا تقتصر على النصوص القانونية فقط، بل تستوجب وجود هيئات متخصصة تضطلع بمهام الوقاية والكشف والتحقيق والمتابعة، إلى جانب تعزيز التعاون الوطني بين مختلف الأجهزة المختصة، وتفعيل التعاون الدولي نظراً للطابع العابر للحدود الذي تتميز به الجرائم الإلكترونية.

وعليه، سيتم من خلال هذا الفصل دراسة الإطار القانوني والمؤسساتي لمكافحة جرائم الإنترنت، وذلك من خلال التطرق في المبحث الأول إلى الجرائم الإلكترونية المنصوص عليها قانوناً والآليات القانونية لمتابعتها، مع بيان أهم النصوص التشريعية المنظمة لها، خاصة ما تعلق بأحكام قانون العقوبات وقانون الإجراءات الجزائية الجديد والإجراءات الخاصة بالتحقيق في الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال. أما المبحث الثاني فسيتناول دور الهيئات المختصة والتعاون الوطني والدولي في مكافحة جرائم الإنترنت.

## المبحث الأول: الحماية القانونية في القوانين العامة

تُعد القوانين العامة، وعلى رأسها قانون العقوبات وقانون الإجراءات الجزائية، الإطار الأساسي الذي تستند إليه الدولة في مكافحة مختلف الجرائم، بما فيها الجرائم المرتكبة عبر شبكة الإنترنت. وقد أدرك المشرع الجزائري خطورة التطور التكنولوجي وما نتج عنه من أنماط إجرامية مستحدثة تستهدف الأنظمة المعلوماتية والبيانات الإلكترونية، الأمر الذي دفعه إلى إدراج نصوص قانونية خاصة ضمن قانون العقوبات لتجريم الأفعال الماسة بأمن الأنظمة المعلوماتية والمعطيات الرقمية، مع تقرير عقوبات تتناسب مع خطورة هذه الجرائم.

### المطلب الأول: جرائم الإنترنت في قانون العقوبات

لقد ساهم قانون العقوبات الجزائري في توفير حماية جزائية للأنظمة المعلوماتية من خلال تجريم العديد من الأفعال التي تمس سرية البيانات وسلامة الأنظمة المعلوماتية وتوافرها. وتظهر هذه الحماية من خلال النصوص التي أدرجها المشرع ضمن الباب الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

#### الفرع الأول: الجرائم المنصوص عليها

أدرج المشرع الجزائري مجموعة من الجرائم الإلكترونية ضمن قانون العقوبات، وذلك بهدف حماية الأنظمة المعلوماتية من مختلف الاعتداءات التي قد تتعرض لها.

**أولاً: جريمة الدخول غير المشروع إلى نظام معلوماتي**

تُعد جريمة الدخول غير المشروع من أكثر الجرائم الإلكترونية انتشاراً، وتتحقق بمجرد ولوج شخص إلى نظام معلوماتي أو شبكة إلكترونية دون الحصول على ترخيص أو إذن مسبق من صاحب النظام. وتقوم هذه الجريمة حتى ولو لم يترتب على الدخول أي ضرر فعلي، لأن المشرع يهدف إلى حماية حرمة الأنظمة المعلوماتية ذاتها.

وتكمن خطورة هذه الجريمة في أنها تمثل المرحلة الأولى التي تسبق العديد من الجرائم الإلكترونية الأخرى، كسرقة البيانات أو تخريب الأنظمة أو التجسس الإلكتروني[1].

**ثانياً: جريمة البقاء غير المشروع داخل النظام المعلوماتي**

لا يقتصر التجريم على الدخول غير المشروع فقط، وإنما يمتد إلى البقاء داخل النظام المعلوماتي رغم زوال سبب الدخول أو اكتشاف عدم مشروعيته. ويُعد هذا السلوك اعتداءً على حق صاحب النظام في السيطرة على بياناته ومعلوماته.

**ثالثاً: جريمة حذف أو تغيير أو إتلاف البيانات الإلكترونية**

يقصد بهذه الجريمة كل فعل يؤدي إلى إزالة البيانات أو تعديلها أو تشويهها أو جعلها غير قابلة للاستعمال، سواء تعلق الأمر بملفات شخصية أو بيانات إدارية أو مالية أو تجارية.

وتزداد خطورة هذه الجريمة عندما تكون البيانات محل الاعتداء ضرورية لاستمرار نشاط مؤسسة أو إدارة عمومية[2].

**رابعاً: جريمة عرقلة سير النظام المعلوماتي**

تتحقق هذه الجريمة عندما يقوم الجاني بتعطيل أو إعاقة تشغيل النظام المعلوماتي أو الشبكة الإلكترونية، مما يؤدي إلى توقف الخدمات أو بطء أدائها أو منع المستخدمين من الاستفادة منها[3].

ومن أمثلتها الهجمات الإلكترونية التي تستهدف المواقع الحكومية أو المؤسسات الاقتصادية الكبرى.

---

[1]– المادة 394 مكرر من قانون العقوبات الجزائري.

[2]– المادة 394 مكرر 1 من قانون العقوبات الجزائري.

[3]– المادة 394 مكرر 2 من قانون العقوبات الجزائري.

**خامساً: جريمة إدخال أو تعديل المعطيات بطريقة احتيالية**

يقصد بها قيام الجاني بإدخال بيانات مزورة أو تعديل بيانات صحيحة أو حذفها بهدف تحقيق منفعة غير مشروعة أو إلحاق الضرر بالغير.

وتكثر هذه الجريمة في المجال البنكي والتجاري، حيث يتم التلاعب بالمعطيات المالية أو الحسابات الإلكترونية[1].

**سادساً: جريمة استعمال الوسائل التقنية بغرض ارتكاب الجرائم الإلكترونية**

لم يكتف المشرع بتجريم الأفعال الأصلية، بل جرم كذلك إنتاج أو حيازة أو توفير البرامج والأدوات الإلكترونية المخصصة لارتكاب الجرائم المعلوماتية، وذلك لمنع الجريمة قبل وقوعها[2].

**سابعاً: جريمة انتحال الهوية الإلكترونية**

تتمثل في استعمال اسم أو صفة أو حساب إلكتروني خاص بالغير دون إذنه بقصد التضليل أو الاحتيال أو الإضرار بالمجني عليه.

وقد أصبحت هذه الجريمة من أكثر الجرائم انتشاراً مع توسع استخدام مواقع التواصل الاجتماعي والمنصات الرقمية[3].

**الفرع الثاني: العقوبات المقررة**

حرص المشرع الجزائري على تقرير عقوبات متنوعة لجرائم الإنترنت تتناسب مع طبيعتها وخطورتها، وذلك بهدف تحقيق الردع العام والخاص.

---

[1]– المادة 394 مكرر 3 من قانون العقوبات الجزائري.

[2]– المادة 394 مكرر 7 من قانون العقوبات الجزائري.

[3]– المادة 394 مكرر 5 من قانون العقوبات الجزائري.

**أولاً: العقوبات الأصلية**

تتمثل العقوبات الأصلية في الحبس والغرامة المالية، حيث تختلف مدة الحبس وقيمة الغرامة بحسب نوع الجريمة وخطورة الفعل المرتكب.

ففي جريمة الدخول غير المشروع إلى نظام معلوماتي يعاقب الجاني بالحبس والغرامة، مع تشديد العقوبة إذا ترتب عن الفعل حذف أو تعديل المعطيات أو الإضرار بالنظام[1].

كما تتشدد العقوبات في الجرائم التي تؤدي إلى إتلاف البيانات أو عرقلة سير الأنظمة المعلوماتية أو المساس بالمصالح الحيوية للدولة[2].

**ثانياً: العقوبات التكميلية**

إضافة إلى العقوبات الأصلية، يجوز للقاضي الحكم بعقوبات تكميلية تهدف إلى منع تكرار الجريمة أو إزالة آثارها[3].

ومن أهم هذه العقوبات:

- مصادرة الأجهزة والوسائل المستعملة في ارتكاب الجريمة.
- مصادرة العائدات المتحصلة من النشاط الإجرامي.
- غلق المواقع الإلكترونية أو الحسابات المستعملة في ارتكاب الجريمة.
- الحرمان من بعض الحقوق الوطنية أو المدنية.

[1]– المادة 394 مكرر من قانون العقوبات الجزائري.

[2]– المواد 394 مكرر 1 و394 مكرر 2 و394 مكرر 6 من قانون العقوبات الجزائري.

[3]– المادة 9 مكرر من قانون العقوبات الجزائري.

**ثالثاً: مسؤولية الشخص المعنوي**

أقر المشرع الجزائري مبدأ المسؤولية الجزائية للشخص المعنوي، بحيث يمكن مساءلة الشركات والمؤسسات والجمعيات إذا ارتكبت الجرائم الإلكترونية لحسابها أو لفائدتها بواسطة ممثليها أو أجهزتها.

وتتمثل العقوبات المطبقة على الشخص المعنوي في الغرامات المالية، والمصادرة، والحل، وغلق المؤسسة أو أحد فروعها[1].

**رابعاً: تشديد العقوبة في بعض الحالات**

تشدد العقوبة إذا استهدفت الجريمة أنظمة معلوماتية تابعة للدولة أو لهيئات حساسة، أو إذا نتج عنها أضرار جسيمة تمس الأمن الوطني أو الاقتصاد الوطني أو المرافق العمومية.

ويهدف هذا التشديد إلى توفير حماية خاصة للبنى التحتية الرقمية للدولة[2].

يتضح من خلال النصوص السابقة أن المشرع الجزائري لم يكتف بتطبيق القواعد التقليدية لقانون العقوبات على الجرائم الإلكترونية، بل خصص لها أحكاماً جزائية تتلاءم مع طبيعتها التقنية. وقد ساهم ذلك في توفير حماية قانونية للأنظمة المعلوماتية والمعطيات الإلكترونية، غير أن التطور المستمر لوسائل الجريمة الإلكترونية يفرض مراجعة هذه النصوص وتحيينها بصورة دورية لضمان فعاليتها في مواجهة التهديدات الرقمية الحديثة.

**المطلب الثاني : الإجراءات الجزائية الخاصة بجرائم الانترنت**

تتميز جرائم الإنترنت بخصوصية تجعل اكتشافها وإثباتها أكثر صعوبة من الجرائم التقليدية، نظراً لاعتمادها على وسائل تقنية وأدلة رقمية قابلة للتغيير والإخفاء. لذلك

[1]– المادة 51 مكرر من قانون العقوبات الجزائري.

[2]– المادة 394 مكرر 6 من قانون العقوبات الجزائري.

استوجب الأمر وضع إجراءات جزائية خاصة تتلاءم مع طبيعتها، من خلال اعتماد وسائل بحث وتحري وتحقيق حديثة لجمع الأدلة الإلكترونية وملاحقة مرتكبيها.

وقد نظم المشرّع الجزائري هذه الإجراءات ضمن قانون الإجراءات الجزائية، خاصة المواد 65 مكرر إلى 65 مكرر 18، بهدف توفير آليات قانونية فعالة لمكافحة الجرائم المرتكبة عبر الأنظمة المعلوماتية مع ضمان احترام الحقوق والحريات.

**الفرع الأول : التحري والتحقيق**

أجاز قانون الإجراءات الجزائية وسائل خاصة في التحري، من بينها:

**تفتيش الأنظمة المعلوماتية**

يُعتبر تفتيش الأنظمة المعلوماتية من أهم الإجراءات المستحدثة في مجال مكافحة الجرائم الإلكترونية، وذلك بسبب الطبيعة الخاصة لهذا النوع من الجرائم التي تُرتكب في بيئة رقمية وتترك آثاراً إلكترونية تختلف عن الآثار المادية التقليدية. حيث تختلف مدة الحبس وقيمة الغرامة بحسب نوع الجريمة وخطورة الفعل المرتكب.

ففي جريمة الدخول غير المشروع إلى نظام معلوماتي يعاقب الجاني بالحبس والغرامة، مع تشديد العقوبة إذا ترتب عن الفعل حذف أو تعديل المعطيات أو الإضرار بالنظام[1].

كما تتشدد العقوبات في الجرائم التي تؤدي إلى إتلاف البيانات أو عرقلة سير الأنظمة المعلوماتية أو المساس بالمصالح الحيوية للدولة[2].

**ثانياً: العقوبات التكميلية**

إضافة إلى العقوبات الأصلية، يجوز للقاضي الحكم بعقوبات تكميلية تهدف إلى منع تكرار الجريمة أو إزالة آثارها.

ومن أهم هذه العقوبات[1]:

---

[1]– المادة 394 مكرر من قانون العقوبات الجزائري.

[2]– المواد 394 مكرر 1 و394 مكرر 2 و394 مكرر 6 من قانون العقوبات الجزائري.

- مصادرة الأجهزة والوسائل المستعملة في ارتكاب الجريمة.
- مصادرة العائدات المتحصلة من النشاط الإجرامي.
- غلق المواقع الإلكترونية أو الحسابات المستعملة في ارتكاب الجريمة.
- الحرمان من بعض الحقوق الوطنية أو المدنية.

**ثالثاً: مسؤولية الشخص المعنوي**

أقر المشرع الجزائري مبدأ المسؤولية الجزائية للشخص المعنوي، بحيث يمكن مساءلة الشركات والمؤسسات والجمعيات إذا ارتكبت الجرائم الإلكترونية لحسابها أو لفائدتها بواسطة ممثليها أو أجهزتها.

وتتمثل العقوبات المطبقة على الشخص المعنوي في الغرامات المالية، والمصادرة، والحل، وغلق المؤسسة أو أحد فروعها[2].

**رابعاً: تشديد العقوبة في بعض الحالات**

تشدد العقوبة إذا استهدفت الجريمة أنظمة معلوماتية تابعة للدولة أو لهيئات حساسة، أو إذا نتج عنها أضرار جسيمة تمس الأمن الوطني أو الاقتصاد الوطني أو المرافق العمومية[3].

ويهدف هذا التشديد إلى توفير حماية خاصة للبنى التحتية الرقمية للدولة.

تعد مسألة الإثبات من أهم التحديات التي تواجه السلطات المختصة في مكافحة الجرائم الإلكترونية، وذلك بسبب الطبيعة الخاصة للأدلة الرقمية التي تتميز بسهولة التعديل أو

[1]– المادة 9 مكرر من قانون العقوبات الجزائري.

[2]– المادة 51 مكرر من قانون العقوبات الجزائري.

[3]– المادة 394 مكرر 6 من قانون العقوبات الجزائري.

الحذف أو الإخفاء. فالجاني يستطيع محو آثار الجريمة خلال وقت قصير باستعمال برامج متخصصة.

كما أن الجرائم الإلكترونية تعتمد على تقنيات متطورة تسمح بإخفاء الهوية الحقيقية للجاني من خلال استخدام الشبكات الافتراضية الخاصة والخوادم الوسيطة، مما يصعب عملية تحديد المسؤول عن الفعل الإجرامي[1].

وتزداد صعوبة الإثبات عندما تتجاوز الجريمة الحدود الوطنية، حيث يتطلب الأمر تعاوناً دولياً بين السلطات القضائية والأمنية في الدول المختلفة من أجل الحصول على المعلومات والأدلة الضرورية للتحقيق.

ومن جهة أخرى، تحتاج الأدلة الرقمية إلى إجراءات تقنية دقيقة أثناء جمعها وحفظها وتحليلها حتى لا تفقد حجيتها القانونية أمام القضاء، وهو ما يستوجب الاستعانة بخبراء متخصصين في مجال الأدلة الرقمية والجرائم المعلوماتية[2].

يتضح من خلال النصوص السابقة أن المشرع الجزائري لم يكتف بتطبيق القواعد التقليدية لقانون العقوبات على الجرائم الإلكترونية، بل خصص لها أحكاماً جزائية تتلاءم مع طبيعتها التقنية . وقد ساهم ذلك في توفير حماية قانونية للأنظمة المعلوماتية والمعطيات الإلكترونية، غير أن التطور المستمر لوسائل الجريمة الإلكترونية يفرض مراجعة هذه النصوص وتحيينها بصورة دورية لضمان فعاليتها في مواجهة التهديدات الرقمية الحديثة.

في الجرائم الإلكترونية تكون غالباً على شكل ملفات رقمية أو سجلات إلكترونية أو رسائل إلكترونية أو بيانات مخزنة داخل الحواسيب والخوادم والشبكات المعلوماتية، الأمر الذي يفرض على سلطات التحقيق اتباع أساليب خاصة للبحث عنها وضبطها.

---

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، 2021، ص 198.

[2]– عبد الرزاق الشيخ علي، الجريمة المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2016، ص 102.

ويقصد بتفتيش الأنظمة المعلوماتية قيام ضباط الشرطة القضائية أو السلطات القضائية المختصة بالدخول إلى نظام معلوماتي أو جزء منه من أجل البحث عن البيانات أو البرامج أو الملفات التي لها علاقة بالجريمة محل التحقيق. ولا يقتصر التفتيش على الجهاز المادي فقط، بل يمتد إلى جميع مكوناته المنطقية والرقمية، بما في ذلك قواعد البيانات والبرمجيات ووسائط التخزين المختلفة.

وتبرز أهمية هذا الإجراء في أن الدليل الإلكتروني يتميز بسهولة إخفائه أو تعديله أو محوه خلال فترة قصيرة جداً، وهو ما يجعل سرعة التدخل أمراً ضرورياً للمحافظة على الأدلة ومنع ضياعها. كما أن الجناة غالباً ما يلجؤون إلى استخدام وسائل تقنية متطورة لإخفاء آثار جرائمهم، مثل تشفير الملفات أو حذف البيانات أو استعمال برامج إخفاء الهوية، مما يزيد من أهمية التفتيش المعلوماتي كوسيلة فعالة لكشف الحقيقة.

ويختلف التفتيش المعلوماتي عن التفتيش التقليدي من حيث الموضوع والوسائل المستعملة، فبينما يركز التفتيش التقليدي على الأشياء المادية الملموسة، ينصب التفتيش المعلوماتي على البيانات الرقمية التي قد تكون موزعة على عدة أجهزة أو مخزنة عن بعد عبر الشبكات المعلوماتية. لذلك يتطلب هذا النوع من التفتيش خبرة تقنية عالية ومعرفة متخصصة بطرق استخراج الأدلة الرقمية والمحافظة عليها.

تؤكد الدراسات الحديثة أن جرائم الإنترنت تفرض تحديات كبيرة على أجهزة التحقيق والمتابعة الجزائية، نظراً لطبيعتها التقنية غير المادية، مما يستوجب تطوير وسائل البحث والتحري التقليدية. وقد أبرزت بعض الدراسات، مثل دراسة بلعربي سليمة (2020)، ضرورة استحداث إجراءات خاصة كالتفتيش الإلكتروني والمراقبة الرقمية[1]، في حين

[1]– بلعربي سليمة، خصوصية المتابعة في الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر، المركز الجامعي مغنية، 2020.

ركزت دراسة بدودة عزيزة وعلّالي سعاد (2018) على أهمية الدليل الرقمي وضرورة تأهيل المحققين تقنياً لضمان فعالية التحقيق الجنائي في هذا النوع من الجرائم[1].

**الفرع الثاني : المتابعة والمحاكمة في جرائم الإنترنت**

**المتابعة الجزائية في جرائم الإنترنت**

تُعد مرحلة المتابعة الجزائية من أهم المراحل التي تمر بها الدعوى العمومية في جرائم الإنترنت، إذ تأتي بعد انتهاء إجراءات التحري والتحقيق وجمع الأدلة الرقمية الكافية التي تثبت وقوع الجريمة ونسبتها إلى مرتكبها. وتتمثل المتابعة الجزائية في مباشرة النيابة العامة للدعوى العمومية ضد المتهم أمام الجهات القضائية المختصة من أجل مساءلته عن الأفعال الإجرامية المنسوبة إليه[2].

وتكتسب المتابعة في الجرائم الإلكترونية أهمية خاصة بالنظر إلى الطبيعة التقنية لهذه الجرائم وما تثيره من صعوبات قانونية وعملية، لاسيما فيما يتعلق بتحديد هوية الجاني واختصاص الجهات القضائية وجمع الأدلة الرقمية وإثبات صحتها. لذلك حرص المشرع الجزائري على توفير إطار قانوني يسمح بملاحقة مرتكبي الجرائم الإلكترونية وضمان عدم إفلاتهم من العقاب.

وتباشر النيابة العامة إجراءات المتابعة بمجرد توافر أدلة كافية على وقوع الجريمة، حيث تقوم بدراسة محاضر الضبطية القضائية وتقارير الخبرة التقنية والأدلة الرقمية المحجوزة. فإذا تبين لها وجود عناصر كافية لإثبات الجريمة، فإنها تحرك الدعوى العمومية وتباشر الإجراءات القضائية اللازمة[3].

[1]– بدودة عزيزة، علّالي سعاد، التحقيق الجنائي في الجرائم الرقمية، مذكرة ماستر، جامعة غرداية، 2018.

[2]– قانون الإجراءات الجزائية الجزائري.

[3]– القانون رقم 09-04 المؤرخ في 05 أوت 2009.

وتتميز المتابعة الجزائية في الجرائم الإلكترونية بخصوصية الدليل الرقمي الذي يختلف عن الأدلة التقليدية، إذ يتطلب التأكد من سلامة الدليل وعدم تعرضه للتعديل أو التحريف منذ لحظة ضبطه إلى غاية تقديمه أمام القضاء. ولهذا تلعب الخبرة التقنية دوراً أساسياً في تدعيم المتابعة الجزائية وإثبات صحة الأدلة الرقمية[1].

كما قد تواجه النيابة العامة صعوبات مرتبطة بالطابع العابر للحدود للجرائم الإلكترونية، إذ يمكن أن يكون الجاني موجوداً في دولة والضحية في دولة أخرى والخوادم المستعملة في دولة ثالثة. وفي هذه الحالات يصبح التعاون القضائي الدولي ضرورة حتمية من أجل تبادل المعلومات وتنفيذ الإنابات القضائية وتسليم المجرمين عند الاقتضاء.

ومن جهة أخرى، تتمتع الضحية في الجرائم الإلكترونية بحق التأسس كطرف مدني للمطالبة بالتعويض عن الأضرار المادية أو المعنوية الناتجة عن الجريمة، سواء تعلق الأمر بسرقة البيانات الشخصية أو الاحتيال الإلكتروني أو الاعتداء على السمعة عبر الإنترنت[2].

**أهمية المتابعة الجزائية في جرائم الإنترنت**

تظهر أهمية المتابعة الجزائية في عدة جوانب أهمها:

- ضمان تطبيق القانون على مرتكبي الجرائم الإلكترونية.
- حماية المجتمع من مخاطر الاعتداءات المعلوماتية.
- تحقيق الردع العام والخاص.
- حماية الحقوق والحريات الرقمية للأفراد.
- تعزيز الثقة في المعاملات الإلكترونية.

[1]– محمد حزيط، قانون الإجراءات الجزائية الجزائري ، دار هومة، الجزائر.

[2]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر..

**ثانيا: المحاكمة في جرائم الإنترنت**

تُعد المحاكمة المرحلة النهائية في الدعوى العمومية، حيث يتم عرض القضية على الجهة القضائية المختصة للفصل فيها بعد دراسة الوقائع والأدلة المقدمة من طرف النيابة العامة والدفاع. وتتميز المحاكمة في الجرائم الإلكترونية بمجموعة من الخصائص المرتبطة بالطبيعة التقنية لهذه الجرائم وبخصوصية الأدلة الرقمية.

وتخضع محاكمة مرتكبي الجرائم الإلكترونية للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية الجزائري، مع مراعاة الأحكام الخاصة الواردة في التشريعات المتعلقة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

وخلال جلسات المحاكمة تقوم المحكمة بدراسة الأدلة الرقمية المقدمة في الملف، مثل الرسائل الإلكترونية وسجلات الاتصال والبيانات المستخرجة من الأجهزة الإلكترونية وتقارير الخبرة الفنية. ويخضع كل دليل للمناقشة من طرف الخصوم وفقاً لمبدأ المواجهة الذي يضمن حق الدفاع.

وتُعتبر الخبرة التقنية من أهم وسائل الإثبات أمام المحكمة، إذ يعتمد القاضي غالباً على رأي الخبراء المختصين لفهم الجوانب الفنية المتعلقة بالجريمة الإلكترونية. فالخبراء يتولون تحليل الأدلة الرقمية وتفسير نتائج الفحص التقني وتوضيح كيفية وقوع الجريمة والوسائل المستعملة في ارتكابها.

كما تثير الجرائم الإلكترونية إشكالية الاختصاص القضائي، خاصة عندما تكون الجريمة ذات طابع دولي. وفي هذه الحالة يتم تحديد الجهة القضائية المختصة وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية والاتفاقيات الدولية التي تكون الجزائر طرفاً فيها.

**ضمانات المحاكمة العادلة في جرائم الإنترنت**

رغم خصوصية الجرائم الإلكترونية، فإن المتهم يتمتع بجميع الضمانات المقررة في المحاكمة العادلة، ومن بينها:

**أولاً: قرينة البراءة**

يبقى المتهم بريئاً إلى غاية صدور حكم قضائي نهائي يثبت إدانته.

**ثانياً: حق الدفاع**

يحق للمتهم الاستعانة بمحامٍ والاطلاع على ملف الدعوى ومناقشة الأدلة المقدمة ضده.

**ثالثاً: علنية الجلسات**

تُعقد جلسات المحاكمة بصورة علنية إلا في الحالات التي يقرر فيها القانون خلاف ذلك حفاظاً على النظام العام أو الآداب العامة.

**رابعاً: الطعن في الأحكام**

يحق للمتهم وللنيابة العامة ممارسة طرق الطعن القانونية ضد الأحكام الصادرة.

**العقوبات المقررة في جرائم الإنترنت**

تختلف العقوبات بحسب طبيعة الجريمة المرتكبة، وتشمل:

- عقوبات سالبة للحرية (الحبس).
- عقوبات مالية (الغرامات).
- المصادرة.
- غلق المواقع الإلكترونية.
- حجز المعدات والأجهزة المستعملة في الجريمة.

- المنع من ممارسة بعض الأنشطة عند الاقتضاء.

وقد شدد المشرع الجزائري العقوبات في بعض الجرائم الإلكترونية الخطيرة نظراً لما تشكله من تهديد للأمن الاقتصادي والاجتماعي ولحقوق الأفراد.

**دور القضاء في مكافحة الجرائم الإلكترونية**

يؤدي القضاء دوراً محورياً في مكافحة الجرائم الإلكترونية من خلال:

- تطبيق النصوص القانونية المتعلقة بالجرائم المعلوماتية.
- حماية الحقوق الرقمية للأفراد.
- تطوير الاجتهاد القضائي في مجال الجرائم الإلكترونية.
- المساهمة في تحقيق الردع العام والخاص.
- ضمان التوازن بين مكافحة الجريمة واحترام الحريات الأساسية.

وقد نظم المشرع الجزائري هذا الإجراء من خلال القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أجاز للسلطات المختصة اتخاذ التدابير اللازمة لجمع الأدلة الرقمية مع مراعاة الضمانات القانونية المقررة لحماية الحقوق والحريات الفردية[1].

كما يقتضي التفتيش المعلوماتي احترام مجموعة من الضمانات القانونية، من بينها ضرورة وجود إذن من السلطة القضائية المختصة في الحالات التي يتطلبها القانون، واحترام مبدأ الشرعية الإجرائية، وعدم تجاوز حدود الغرض الذي تم من أجله التفتيش، بالإضافة إلى المحافظة على سرية البيانات غير المرتبطة بالجريمة[2].

[1]- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر.

ومن الناحية العملية يمر التفتيش المعلوماتي بعدة مراحل، تبدأ بتحديد الأجهزة أو الأنظمة محل التفتيش، ثم تأمينها ومنع العبث بمحتوياتها، يلي ذلك استخراج البيانات وتحليلها بواسطة خبراء مختصين، وأخيراً توثيق النتائج في محاضر رسمية يمكن الاستناد إليها أمام القضاء[1].

**اعتراض المراسلات الإلكترونية**

يُعد اعتراض المراسلات الإلكترونية من الإجراءات الحديثة التي استحدثتها التشريعات المعاصرة لمواجهة التطور المتزايد للجرائم الإلكترونية. فمع انتشار وسائل الاتصال الحديثة أصبح المجرمون يعتمدون على البريد الإلكتروني وتطبيقات التواصل الاجتماعي وبرامج المحادثة الفورية للتخطيط لجرائمهم أو تنفيذها، مما جعل من الضروري تمكين سلطات التحقيق من مراقبة هذه المراسلات في إطار قانوني محدد[2].

ويقصد باعتراض المراسلات الإلكترونية قيام السلطات المختصة بالتقاط أو تسجيل أو الاطلاع على الرسائل والاتصالات الإلكترونية المتبادلة بين الأشخاص المشتبه فيهم بهدف الكشف عن الجرائم أو جمع الأدلة المتعلقة بها. ويشمل ذلك البريد الإلكتروني والرسائل النصية والمحادثات الإلكترونية وسائر أشكال الاتصال الرقمي.

ويُعتبر هذا الإجراء استثناءً على مبدأ سرية المراسلات الذي يُعد من الحقوق الأساسية المكفولة دستورياً، لذلك أحاطه المشرع بجملة من الضمانات القانونية التي تمنع التعسف في استعماله. ومن أهم هذه الضمانات ضرورة الحصول على إذن مسبق من الجهة القضائية المختصة وتحديد مدة الاعتراض والهدف منه بدقة[3].

---

[1]– عبد العزيز سعد، الجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات، دار هومة، الجزائر.

[2]– القانون رقم 09-04 المؤرخ في 05 أوت 2009.

[3]– محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر.

وتكمن أهمية اعتراض المراسلات الإلكترونية في أنه يسمح بالكشف عن المخططات الإجرامية قبل تنفيذها أحياناً، كما يساعد على تحديد هوية المتورطين ومعرفة طبيعة العلاقة بينهم والكشف عن الأدلة التي يصعب الحصول عليها بطرق أخرى.

ويُساهم هذا الإجراء كذلك في مكافحة الجرائم المنظمة والإرهاب الإلكتروني والاحتيال المعلوماتي وجرائم اختراق الأنظمة المعلوماتية، حيث غالباً ما تتم هذه الجرائم من خلال تبادل رسائل وتعليمات عبر وسائل الاتصال الإلكترونية المختلفة[1].

غير أن اللجوء إلى اعتراض المراسلات الإلكترونية يجب أن يتم في إطار احترام التوازن بين متطلبات الأمن وحماية الحياة الخاصة للأفراد، لأن التوسع غير المبرر في استعمال هذا الإجراء قد يؤدي إلى المساس بالحقوق والحريات الأساسية.

**المراقبة الإلكترونية**

تُعد المراقبة الإلكترونية من الوسائل الحديثة التي تعتمد عليها السلطات المختصة في الكشف عن الجرائم الإلكترونية ومتابعة مرتكبيها. وقد فرض التطور السريع لتكنولوجيا المعلومات والاتصال ضرورة اعتماد هذا الإجراء بسبب الصعوبات التي تواجهها وسائل التحري التقليدية في اكتشاف الجرائم التي تُرتكب داخل الفضاء الرقمي[2].

ويقصد بالمراقبة الإلكترونية متابعة الأنشطة والاتصالات التي تتم عبر الأنظمة المعلوماتية أو شبكات الاتصال الإلكترونية بهدف جمع المعلومات والأدلة المتعلقة بالجريمة. وتشمل هذه المراقبة رصد المواقع الإلكترونية المشبوهة ومتابعة حركة البيانات والاتصالات الرقمية ومراقبة النشاط الإجرامي الذي يتم عبر الإنترنت.

---

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر..

[2]– القانون رقم 09-04 المؤرخ في 05 أوت 2009.

وتكتسي المراقبة الإلكترونية أهمية كبيرة في مجال الوقاية من الجرائم الإلكترونية، إذ تسمح بالكشف المبكر عن التهديدات والمخاطر المعلوماتية قبل تحولها إلى جرائم مكتملة الأركان. كما تساعد على التعرف على الأساليب الجديدة التي يعتمدها المجرمون في ارتكاب جرائمهم[1].

ومن بين المجالات التي تظهر فيها فعالية المراقبة الإلكترونية مكافحة القرصنة المعلوماتية والاحتيال الإلكتروني وسرقة البيانات الشخصية والاعتداء على الأنظمة المعلوماتية. كما تُستخدم لمراقبة الشبكات الإجرامية المنظمة التي تعتمد على وسائل الاتصال الحديثة في تنفيذ أنشطتها غير المشروعة[2].

إلا أن فعالية هذا الإجراء تظل مرتبطة بمدى احترام الضوابط القانونية والتقنية التي تحكمه، خاصة فيما يتعلق بحماية الحياة الخاصة وسرية البيانات الشخصية. ولذلك فإن المشرع الجزائري اشترط ممارسة هذه المراقبة تحت إشراف السلطات القضائية المختصة ووفقاً للإجراءات التي يحددها القانون.

**تتبع الاتصالات الرقمية**

يُعتبر تتبع الاتصالات الرقمية من أهم الإجراءات التقنية التي تعتمد عليها سلطات التحقيق في مجال مكافحة الجرائم الإلكترونية. ويهدف هذا الإجراء إلى تحديد مصدر الاتصالات الرقمية ومسارها والجهات المتصلة بها من أجل الوصول إلى مرتكبي الجرائم الإلكترونية وجمع الأدلة اللازمة لإدانتهم[3].

---

[1]– عبد العزيز سعد، الجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات، دار هومة، الجزائر.

[2]– محمد حزيط، الإجراءات الجزائية الجزائرية على ضوء التعديلات الحديثة، دار هومة، الجزائر.

[3]– القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ويقصد بتتبع الاتصالات الرقمية استخدام الوسائل التقنية والقانونية التي تسمح بمراقبة حركة البيانات والاتصالات عبر الشبكات الإلكترونية وتحديد الأجهزة أو الحسابات المستعملة في ارتكاب الجريمة. ويشمل ذلك تتبع عناوين بروتوكول الإنترنت (IP) وتحليل سجلات الاتصال والبيانات المرورية الخاصة بالشبكات.

وتبرز أهمية هذا الإجراء في أن المجرمين الإلكترونيين غالباً ما يحاولون إخفاء هوياتهم الحقيقية من خلال استخدام أسماء وهمية أو برامج إخفاء الهوية أو خوادم وسيطة، مما يجعل تتبع الاتصالات الرقمية الوسيلة الأساسية للكشف عن هوياتهم الحقيقية[1].

كما يُساعد هذا الإجراء على كشف الروابط بين أفراد الشبكات الإجرامية وتحديد دور كل شخص في النشاط الإجرامي، وهو ما يُساهم في بناء ملف قضائي متكامل يدعم عملية المتابعة والمحاكمة.

ويكتسب تتبع الاتصالات الرقمية أهمية خاصة في الجرائم الإلكترونية ذات الطابع الدولي، حيث قد يتم تنفيذ الجريمة من دولة معينة بينما توجد آثارها أو ضحاياها في دولة أخرى. لذلك أصبح التعاون الدولي وتبادل المعلومات بين الدول أمراً ضرورياً لنجاح عمليات التتبع والتحقيق[2].

وقد أدرك المشرع الجزائري أهمية هذا الإجراء فسمح للسلطات المختصة باللجوء إليه في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مع ضرورة احترام الضمانات القانونية التي تكفل حماية الحقوق والحريات الأساسية للأفراد.

يتضح أن فعالية مكافحة الجرائم الإلكترونية لا تتوقف على وجود نصوص قانونية تجرم هذه الأفعال فحسب، وإنما تتطلب أيضاً إجراءات فعالة للمتابعة والمحاكمة تسمح بالكشف

[1]– محمد حزيط، الإجراءات الجزائية الجزائرية على ضوء التعديلات الحديثة، دار هومة، الجزائر.

[2]– عبد العزيز سعد، الجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات، دار هومة، الجزائر.

عن الجناة ومعاقبتهم وفقاً لمبادئ العدالة وسيادة القانون. كما أن التطور المستمر للتكنولوجيا يفرض على السلطات القضائية تطوير وسائلها القانونية والتقنية لمواجهة الأشكال المستحدثة للجريمة الإلكترونية.

**المبحث الثاني : الحماية القانونية في القوانين الخاصة**

لم تقتصر مواجهة جرائم الإنترنت على القواعد العامة الواردة في قانون العقوبات وقانون الإجراءات الجزائية، بل امتدت إلى مجموعة من القوانين الخاصة التي جاءت لتنظيم المجال الرقمي وتوفير حماية قانونية أكثر تخصصًا، وذلك بالنظر إلى الطبيعة التقنية والمعقدة لهذه الجرائم. فقد أصبح الاعتماد المتزايد على تكنولوجيا الإعلام والاتصال يفرض ضرورة وضع قواعد قانونية خاصة تهدف إلى حماية الأنظمة المعلوماتية، والبيانات الشخصية، والمعاملات الإلكترونية، وضمان أمن الفضاء السيبراني.

وقد تدخل المشرّع من خلال عدة نصوص قانونية خاصة لتجريم الأفعال التي تمس بالأنظمة والشبكات المعلوماتية، أو تنتهك سرية وحرمة البيانات، أو تستعمل الوسائل الإلكترونية في ارتكاب أفعال إجرامية. كما أقر آليات قانونية للوقاية والمكافحة، من خلال تحديد التزامات مقدمي خدمات الإنترنت، وتنظيم التعاملات الإلكترونية، وحماية المستهلك الإلكتروني، وتجريم الاعتداءات الواقعة على المعطيات الشخصية.

وتبرز أهمية هذه الحماية الخاصة في كونها تستجيب لخصوصية الجريمة المعلوماتية التي تتميز بسرعة ارتكابها، وصعوبة اكتشافها، وطابعها العابر للحدود، مما يجعل القواعد التقليدية غير كافية وحدها لمواجهتها. لذلك عمل المشرّع الجزائري على تدعيم المنظومة القانونية بمجموعة من القوانين الخاصة، من بينها القوانين المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتجارة الإلكترونية، وحماية المعطيات ذات الطابع الشخصي، إضافة إلى النصوص المنظمة للأدلة الإلكترونية والإجراءات الخاصة بالبحث والتحري.

وعليه، سيتم تناول الحماية القانونية الخاصة المقررة لمواجهة جرائم الإنترنت من خلال دراسة أهم القوانين الخاصة ذات الصلة، وبيان دورها في تجريم الأفعال الإلكترونية وتوفير آليات فعالة للحد من انتشارها.

**المطلب الأول : القوانين الخاصة بجرائم الانترنت**

أفرز التطور التكنولوجي المتسارع تحديات جديدة أمام الأنظمة القانونية، حيث ظهرت جرائم مرتبطة باستعمال الوسائل الإلكترونية والأنظمة المعلوماتية، تتميز بخصوصيتها التقنية وصعوبة ضبطها بالاعتماد على القواعد القانونية التقليدية فقط. لذلك اتجهت مختلف التشريعات إلى سن قوانين خاصة تهدف إلى تجريم الأفعال التي ترتكب عبر الفضاء الرقمي، وتحديد المسؤولية الجزائية عنها، ووضع آليات قانونية فعالة لمكافحتها.

وقد أدرك المشرّع الجزائري أهمية توفير حماية قانونية خاصة لمواجهة هذا النوع من الجرائم، فعمل على إصدار نصوص تشريعية تهدف إلى حماية الأنظمة المعلوماتية والبيانات الإلكترونية، من خلال تجريم الدخول غير المشروع إلى الأنظمة، والاعتداء على المعطيات، واستعمال الوسائل الإلكترونية في ارتكاب الأفعال الإجرامية. كما عزّز هذه الحماية بإقرار إجراءات جزائية خاصة تتناسب مع طبيعة الجريمة الإلكترونية وطرق إثباتها.

وعليه، سيتم التطرق في هذا المطلب إلى أهم القوانين الخاصة المنظمة لجرائم الإنترنت، وبيان نطاق الحماية التي توفرها لمواجهة مختلف صور الإجرام الإلكتروني.

**الفرع الأول: قانون الجرائم الإلكترونية**

أدرك المشرع الجزائري خطورة الجرائم الإلكترونية وما تشكله من تهديد للأفراد والمؤسسات والدولة، لذلك أصدر القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [1]

يهدف هذا القانون إلى توفير إطار قانوني خاص لمواجهة الجرائم التي ترتكب باستعمال الأنظمة المعلوماتية والشبكات الإلكترونية، وذلك من خلال استحداث آليات قانونية وتقنية تتلاءم مع طبيعة هذه الجرائم.

ومن أهم الأحكام التي جاء بها القانون[2]:

- إنشاء منظومة وطنية للوقاية من الجرائم الإلكترونية من خلال التنسيق بين مختلف الأجهزة الأمنية والقضائية.
- السماح بإجراءات تحرٍ خاصة تتلاءم مع طبيعة البيئة الرقمية، مثل اعتراض المراسلات الإلكترونية وتتبع حركة البيانات.
- إلزام مزودي خدمات الإنترنت بالاحتفاظ ببيانات المستخدمين لفترات محددة وتقديمها للسلطات المختصة عند الحاجة القانونية.
- إنشاء هيئة وطنية متخصصة لمتابعة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتنسيق الجهود المتعلقة بمكافحتها.

وقد ساهم هذا القانون في سد الفراغ التشريعي الذي كان قائماً في مجال مكافحة الجرائم الإلكترونية، كما وفر حماية قانونية أكبر للأنظمة المعلوماتية والشبكات الرقمية.

---

[1]- القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر.

لم تقتصر مكافحة جرائم الإنترنت على النصوص الموضوعية التي تجرّم الأفعال المرتكبة عبر الوسائط الإلكترونية، بل امتدت أيضًا إلى الجانب الإجرائي من خلال استحداث قواعد خاصة للبحث والتحري وجمع الأدلة الرقمية. وقد نظم المشرّع الجزائري هذه الإجراءات ضمن قانون الإجراءات الجزائية، لا سيما المواد من 65 مكرر إلى 65 مكرر 18، التي تضمنت أحكامًا خاصة تتعلق بأساليب التحري الخاصة، واعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إضافة إلى إجراءات مراقبة الاتصالات الإلكترونية وحفظ الأدلة الرقمية، بما يسمح للجهات القضائية المختصة بمواجهة الطبيعة التقنية والمتطورة لجرائم الإنترنت[1].

وتكتسي هذه الأحكام أهمية خاصة في مجال الجرائم المعلوماتية، باعتبار أن الدليل الإلكتروني يتميز بخصوصية من حيث جمعه وحفظه وإثبات حجيته، وهو ما دفع المشرّع إلى وضع آليات إجرائية تسمح بضبط مرتكبي هذه الجرائم مع احترام الضمانات القانونية للأفراد.

ومن بين أهم الإجراءات التي نظمها قانون الإجراءات الجزائية:

المراقبة والاعتراض الإلكتروني للمراسلات والاتصالات وفق الشروط والضوابط القانونية.

تسجيل الأصوات والتقاط الصور كوسائل بحث وتحري خاصة.

تمديد اختصاصات ضباط الشرطة القضائية في مجال جمع الأدلة المتعلقة بالجرائم المرتكبة باستعمال الوسائل الإلكترونية.

حماية سرية الإجراءات وضبط استعمال التقنيات الحديثة في التحقيقات الجزائية[2].

---

[1]– قانون الإجراءات الجزائية الجزائري، المواد 65 مكرر إلى 65 مكرر 18، المتعلقة بأساليب التحري الخاصة وإجراءات البحث والتحقيق في الجرائم ذات الطبيعة الخاصة، المعدل والمتمم..

[2]– انظر: المواد 65 مكرر 5 إلى 65 مكرر 18 من قانون الإجراءات الجزائية الجزائري، المتضمنة أحكام اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وشروط اللجوء إلى هذه الإجراءات.

**الفرع الثاني: قانون حماية المعطيات الشخصية**

مع التطور المتزايد لاستخدام الوسائط الرقمية وتبادل البيانات عبر الإنترنت، أصبح من الضروري توفير حماية قانونية للمعطيات الشخصية للأفراد.

ولهذا أصدر المشرع الجزائري القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1].

ويقصد بالمعطيات الشخصية كل معلومة تسمح بتحديد هوية شخص طبيعي بصورة مباشرة أو غير مباشرة، مثل الاسم والعنوان ورقم الهاتف والبريد الإلكتروني والبيانات البيومترية.

ومن أهم المبادئ التي أقرها القانون[2]:

- مشروعية جمع البيانات ومعالجتها.
- احترام خصوصية الأفراد.
- ضرورة موافقة صاحب البيانات على معالجتها.
- ضمان سرية وأمن المعلومات الشخصية.
- حق الشخص في الاطلاع على بياناته وتصحيحها أو حذفها.

كما فرض القانون عقوبات على كل من يقوم بجمع أو معالجة أو نشر البيانات الشخصية بصورة غير مشروعة، وذلك بهدف حماية الحياة الخاصة للأفراد وتعزيز الثقة في البيئة الرقمية.

[1]- القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2]- عبد الرحمان خلفي، محاضرات في القانون الجنائي للأعمال، دار الهدى، الجزائر.

## المطلب الثاني: آليات الوقاية و المكافحة

أدى التطور المتسارع في استخدام تكنولوجيا المعلومات والاتصالات إلى تنامي ظاهرة جرائم الإنترنت، مما جعل مواجهتها تقتضي اعتماد مجموعة من الآليات الوقائية والعلاجية التي تهدف إلى الحد من انتشارها والتقليل من آثارها. فطبيعة هذه الجرائم التي تتسم بالسرعة والتعقيد وتجاوزها للحدود الإقليمية فرضت على المشرّع والجهات المختصة ضرورة وضع منظومة متكاملة تجمع بين التدابير التقنية والقانونية والمؤسساتية.

وتتمثل آليات الوقاية أساسًا في تعزيز الوعي الأمني لدى مستخدمي الشبكات، وتطوير وسائل الحماية التقنية، واعتماد سياسات أمن المعلومات داخل المؤسسات، إلى جانب سن قواعد قانونية تهدف إلى حماية الأنظمة والبيانات من الاعتداءات الإلكترونية. أما آليات المكافحة فتقوم على تفعيل دور الأجهزة المختصة في التحري والتحقيق، وتطوير وسائل البحث الجنائي الإلكتروني، وتعزيز التعاون الوطني والدولي لملاحقة مرتكبي هذه الجرائم.

وعليه، فإن مواجهة جرائم الإنترنت لا تقتصر على العقاب بعد وقوع الجريمة، وإنما تستلزم اعتماد سياسة شاملة تقوم على الوقاية المسبقة، والكشف المبكر، والمتابعة الجزائية الفعالة، بما يضمن تحقيق الأمن الرقمي وحماية الأفراد والمؤسسات من المخاطر الناتجة عن الاستعمال غير المشروع للفضاء الإلكتروني.

### الفرع الأول: دور الهيئات المتخصصة

تعتمد مكافحة الجرائم الإلكترونية على مجموعة من الهيئات المتخصصة التي تعمل على الوقاية والكشف والتصدي لهذه الجرائم. [1]

ومن أهم هذه الهيئات[2]:

[1]– القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]– محمد صبحي نجم، شرح قانون العقوبات الجزائري.

- الديوان الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المكلف بتنسيق عمليات الوقاية والتحري.
- المديرية العامة للأمن الوطني من خلال الفرق المتخصصة في مكافحة الجريمة الإلكترونية.
- قيادة الدرك الوطني عبر الوحدات المختصة في الجرائم المعلوماتية.
- الجهات القضائية المختصة التي تتولى التحقيق والمتابعة والمحاكمة.
- مصالح الخبرة التقنية والمخبرية التي تساعد في جمع وتحليل الأدلة الرقمية.

وتساهم هذه الهيئات في تعزيز الأمن السيبراني من خلال الرصد المستمر للتهديدات الإلكترونية والتدخل السريع عند وقوع الجرائم.

تُعد جرائم الإنترنت من الجرائم الحديثة التي تتميز بسرعة الانتشار وصعوبة اكتشاف مرتكبيها بسبب اعتمادها على الوسائل التقنية وإمكانية ارتكابها عبر حدود الدول. لذلك أصبحت مكافحتها تتطلب تعاون مجموعة من الهيئات الوطنية والدولية تجمع بين الجانب القانوني، الأمني، التقني والقضائي[1].

**أولاً: دور الهيئات الأمنية والشرطية المتخصصة**

تتولى الأجهزة الأمنية المتخصصة في مكافحة الجرائم الإلكترونية مهمة الكشف عن الجرائم التي ترتكب باستخدام الحواسيب وشبكات الإنترنت، ومن أهم أدوارها:

**1- البحث والتحري عن الجرائم الإلكترونية**

تقوم هذه الهيئات بجمع المعلومات الرقمية وتحليلها للكشف عن:

- عمليات الاختراق غير المشروع للأنظمة المعلوماتية.
- الاحتيال الإلكتروني وسرقة الأموال عبر الإنترنت.
- نشر البرمجيات الخبيثة والفيروسات.

[1]- مجلس أوروبا، Convention on Cybercrime (Budapest Convention)، 2001.

- الاعتداء على البيانات الشخصية.

كما تعتمد على تقنيات التحقيق الرقمي مثل تتبع الأدلة الإلكترونية وتحليل سجلات الدخول إلى الأنظمة.

**2- ضبط الأدلة الرقمية**

تعمل الشرطة الإلكترونية على ضبط وحفظ الأدلة الرقمية بطريقة قانونية تضمن قبولها أمام القضاء، مثل:

- نسخ البيانات الموجودة في الأجهزة.
- فحص البريد الإلكتروني والحسابات الرقمية وفق الإجراءات القانونية.
- تحديد مصدر الهجمات الإلكترونية.

**3- التعاون مع مزودي خدمات الإنترنت**

تتعاون الأجهزة الأمنية مع شركات الاتصالات ومقدمي خدمات الإنترنت للحصول على المعلومات التقنية التي تساعد في تحديد هوية الجناة، مثل بيانات الاتصال وعناوين الشبكات.

**ثانياً: دور السلطة القضائية**

تلعب الجهات القضائية دوراً أساسياً في مكافحة جرائم الإنترنت من خلال:

**1- تطبيق النصوص القانونية**

تقوم المحاكم والنيابات بتكييف الأفعال الإلكترونية باعتبارها جرائم ومعاقبة مرتكبيها وفق القوانين الوطنية الخاصة بالجرائم المعلوماتية.

**2- الإشراف على التحقيقات**

تراقب النيابة العامة إجراءات البحث والتحقيق، وتأذن ببعض الإجراءات التي تمس الخصوصية مثل تفتيش الأجهزة أو ضبط البيانات الإلكترونية.

**3- التعاون القضائي الدولي**

بسبب الطبيعة العابرة للحدود لجرائم الإنترنت، تحتاج السلطات القضائية إلى التعاون مع الدول الأخرى للحصول على الأدلة أو تسليم المتهمين. وتوفر اتفاقية بودابست لمكافحة الجريمة المعلوماتية إطاراً للتعاون الدولي وتبادل المساعدة القانونية[1].

**ثالثاً: دور الهيئات التقنية والأمن السيبراني**

تتمثل مهمتها الأساسية في الوقاية والحماية وليس فقط متابعة الجرائم بعد وقوعها.

ومن اختصاصاتها:

**1- حماية البنية التحتية الرقمية**

تعمل على حماية:

- شبكات المؤسسات الحكومية.
- الأنظمة المالية والمصرفية.
- قواعد البيانات الحساسة.

**2- مراقبة التهديدات الإلكترونية**

تقوم برصد الهجمات السيبرانية وتحليلها، وإصدار التحذيرات الأمنية لتقليل مخاطر الاختراق.

**3- نشر ثقافة الأمن الرقمي**

تساهم في توعية الأفراد والمؤسسات حول:

- حماية كلمات المرور.
- تجنب الروابط الاحتيالية.
- حماية البيانات الشخصية.

**رابعاً: دور المنظمات الدولية**

**1- منظمة الإنتربول (INTERPOL)**

[1]- هلالي عبد الاله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، 2007.

تساهم في مكافحة الجرائم الإلكترونية من خلال:

- تسهيل التعاون بين أجهزة الشرطة في مختلف الدول.
- تبادل المعلومات حول العصابات الإلكترونية.
- دعم التحقيقات العابرة للحدود.

**2- مجلس أوروبا واتفاقية بودابست**

تعتبر اتفاقية بودابست لعام 2001 من أهم الأدوات الدولية في مجال مكافحة الجرائم الإلكترونية، حيث تهدف إلى:

- توحيد التشريعات المتعلقة بالجرائم المعلوماتية.
- وضع قواعد للتحقيق في الجرائم الإلكترونية.
- تسهيل التعاون الدولي في مجال الأدلة الإلكترونية[1].

**3- منظمة الأمم المتحدة**

تعمل على دعم الدول في تطوير التشريعات وبناء القدرات لمواجهة الجرائم الإلكترونية، خاصة الجرائم التي تتجاوز الحدود الوطنية.

**خامساً: دور القطاع الخاص**

لا تقتصر مكافحة جرائم الإنترنت على الجهات الحكومية فقط، بل يساهم القطاع الخاص من خلال:

- شركات الاتصالات التي تساعد في تتبع مصادر الهجمات.
- شركات الأمن السيبراني التي تطور برامج الحماية.
- منصات التواصل الاجتماعي التي تعمل على إزالة المحتوى غير القانوني والإبلاغ عن الحسابات المخالفة.

إن مكافحة جرائم الإنترنت تتطلب تكاملاً بين الهيئات الأمنية والقضائية والتقنية والدولية، لأن طبيعة هذه الجرائم تجعل مواجهتها بواسطة جهة واحدة أمراً غير كافٍ. فنجاح

[1]- صالح أحمد البربري، دور الشرطة في البحث والتفتيش والضبط المتعلق بجرائم الإنترنت.

المكافحة يعتمد على تطوير القوانين، تكوين المختصين، تعزيز التعاون الدولي، واستخدام التقنيات الحديثة في كشف الجرائم وحماية المجتمع الرقمي[1].

**الفرع الثاني: التعاون الوطني والدولي**

تتميز الجرائم الإلكترونية بطابعها العابر للحدود، إذ يمكن أن يرتكب الجاني جريمته من دولة ويقع أثرها في دولة أخرى، مما يجعل التعاون الوطني والدولي ضرورة حتمية لمكافحتها. [2]

**أولاً: التعاون الوطني**

يقصد بالتعاون الوطني تنسيق الجهود بين مختلف الهيئات والأجهزة داخل الدولة لمواجهة الجرائم الإلكترونية، وذلك من خلال:

**1- تعاون الأجهزة الأمنية والقضائية**

تعمل أجهزة الشرطة والدرك والنيابة والقضاء على تبادل المعلومات حول الجرائم الإلكترونية وتتبع مرتكبيها.

إنشاء وحدات متخصصة في التحقيق الرقمي وجمع الأدلة الإلكترونية.

ملاحقة المجرمين الذين يستخدمون الشبكات المعلوماتية لارتكاب الاعتداءات.

**2- دور الهيئات التقنية**

تساهم هيئات الاتصالات ومزودو خدمات الإنترنت في كشف الأنشطة المشبوهة وحماية الشبكات.

تقديم الدعم التقني للجهات المختصة، خاصة في مجال تحليل البيانات الرقمية.

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي المقارن، دار الفكر الجامعي.

[2]- عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي.

**3- التعاون بين القطاع العام والخاص**

مشاركة الشركات التكنولوجية والبنوك والمؤسسات المالية في الإبلاغ عن الهجمات الإلكترونية.

تطوير أنظمة الحماية وتأمين قواعد البيانات والحد من تسريب المعلومات.

**4- التوعية والتكوين**

تنظيم حملات توعوية للمواطنين حول مخاطر الاحتيال الإلكتروني وسرقة البيانات.

تدريب القضاة وأعوان الأمن والخبراء على تقنيات التحقيق في الجرائم الرقمية[1].

يقوم التعاون الوطني على التنسيق بين :

- الأجهزة الأمنية
- السلطات القضائية.
- مزودي خدمات الإنترنت.
- الهيئات الحكومية المختصة بالأمن السيبراني.
- المؤسسات الاقتصادية والمالية.

ويهدف هذا التعاون إلى تبادل المعلومات والخبرات وتسريع إجراءات التحري والتحقيق.

**ثانياً: التعاون الدولي[2]**

نظراً لأن الجرائم الإلكترونية تتجاوز حدود الدول، أصبح التعاون الدولي ضرورة أساسية، ويتمثل في:

[1]- اتفاقية بودابست بشأن الجريمة الإلكترونية، مجلس أوروبا، 2001.

[2]- محمد أمين البشري، التحقيق في الجرائم المعلوماتية، جامعة نايف العربية للعلوم الأمنية.

**1- تبادل المعلومات والخبرات**

- تتعاون الدول في تبادل المعلومات حول أساليب ارتكاب الجرائم الإلكترونية وهوية المجرمين.
- تبادل الخبرات التقنية والقانونية لمواجهة التطور المستمر لهذه الجرائم.

**2- المساعدة القضائية الدولية**

- يتم ذلك من خلال طلبات التعاون بين السلطات القضائية لجمع الأدلة أو استجواب الأشخاص أو تنفيذ عمليات البحث والحجز الإلكتروني.
- تسهيل إجراءات تسليم المجرمين عند ارتكاب جرائم عابرة للحدود.

**3- الاتفاقيات الدولية**

- تعد اتفاقية بودابست بشأن الجريمة الإلكترونية من أبرز الأدوات الدولية التي تهدف إلى توحيد القواعد القانونية وتعزيز التعاون بين الدول في مجال مكافحة الجرائم الإلكترونية.
- تشجع على اعتماد تشريعات وطنية متقاربة وتسهيل التعاون بين أجهزة إنفاذ القانون.

**4- دور المنظمات الدولية**

تساهم منظمات مثل الإنتربول والأمم المتحدة في دعم الدول من خلال التدريب، وتبادل المعلومات، وتطوير آليات مكافحة الجرائم الإلكترونية[1].

يشمل :

- تبادل المعلومات بين الدول.
- الإنابات القضائية الدولية.
- تسليم المجرمين.

[1]- الأمم المتحدة، تقارير مكتب الأمم المتحدة المعني بالمخدرات والجريمة حول الجرائم السيبرانية.

- المساعدة القضائية المتبادلة.
- المشاركة في المؤتمرات والاتفاقيات الدولية المتعلقة بالأمن السيبراني.

ويكتسي هذا التعاون أهمية كبيرة نظراً للطبيعة العالمية لشبكة الإنترنت وصعوبة ملاحقة مرتكبي الجرائم الإلكترونية دون تنسيق دولي فعال.

أصبحت حماية البيانات الشخصية من أهم المواضيع القانونية المرتبطة بالتحول الرقمي، وذلك بسبب تزايد عمليات جمع ومعالجة المعلومات الشخصية للأفراد عبر الوسائل الإلكترونية. ويقصد بالبيانات الشخصية كل معلومة تسمح بتحديد هوية شخص طبيعي بشكل مباشر أو غير مباشر.

وقد أولى المشرع الجزائري أهمية كبيرة لهذا الموضوع من خلال إصدار القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي يهدف إلى ضمان احترام الحياة الخاصة للأفراد وحماية حقوقهم الأساسية[1].

ويقوم نظام حماية البيانات الشخصية على مجموعة من المبادئ الأساسية، من بينها مبدأ المشروعية في جمع البيانات، ومبدأ تحديد الغرض من المعالجة، ومبدأ المحافظة على سرية المعلومات، ومبدأ الحصول على موافقة الشخص المعني عند الاقتضاء.

كما منح القانون للأفراد مجموعة من الحقوق، من بينها الحق في الاطلاع على البيانات الخاصة بهم، والحق في تصحيحها أو حذفها، والحق في الاعتراض على بعض عمليات المعالجة. وفي المقابل، فرض التزامات قانونية على الجهات التي تقوم بمعالجة البيانات، ورتب عقوبات على مخالفة هذه الالتزامات.

[1]- القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وتساهم هذه الحماية القانونية في تعزيز الثقة في المعاملات الإلكترونية وتشجيع استخدام الخدمات الرقمية مع ضمان احترام الخصوصية الفردية[1].

[1]– محمد صخري، الحماية القانونية للبيانات الشخصية في التشريع الجزائري، مجلة الدراسات القانونية، العدد 12، 2020، ص 88.

## خاتمة الفصل الثاني

يتضح من خلال هذا الفصل أن المشرع الجزائري تبنى منظومة قانونية متكاملة لمواجهة الجرائم الإلكترونية، من خلال النصوص العامة الواردة في قانون العقوبات وقانون الإجراءات الجزائية، إضافة إلى القوانين الخاصة وعلى رأسها القانون رقم 09-04 والقانون رقم 18-07. كما عزز هذه الحماية بإنشاء آليات مؤسساتية متخصصة وتفعيل التعاون الوطني والدولي، غير أن التطور المستمر للجرائم الإلكترونية يفرض مواصلة تحديث التشريعات وتطوير الوسائل التقنية والبشرية لضمان فعالية أكبر في الوقاية والمكافحة .



# خاتـــمة

**خـاتمة :**

من خلال هذه الدراسة التي تناولت موضوع جرائم الإنترنت، يتضح أن التطور التكنولوجي الذي عرفه العالم خلال العقود الأخيرة قد أحدث تغيرات جذرية في مختلف المجالات، وأسهم في تسهيل حياة الأفراد وتطوير أساليب العمل والتواصل وتبادل المعلومات. إلا أن هذا التطور ذاته أفرز صورًا جديدة من السلوك الإجرامي استغلت الإمكانيات الهائلة التي توفرها التكنولوجيا الحديثة، مما أدى إلى ظهور جرائم الإنترنت باعتبارها من أخطر الجرائم المستحدثة في العصر الرقمي.

وقد بينت الدراسة أن جرائم الإنترنت تمثل مجموعة من الأفعال غير المشروعة التي ترتكب باستخدام الأنظمة المعلوماتية أو تستهدفها بشكل مباشر، وهي تتميز بجملة من الخصائص التي تجعلها تختلف عن الجرائم التقليدية، من أهمها الطابع التقني، وسهولة ارتكابها، وصعوبة اكتشافها، والطابع العابر للحدود، فضلًا عن إمكانية إحداث أضرار جسيمة خلال فترة زمنية قصيرة.

كما تبين أن صور جرائم الإنترنت متعددة ومتجددة باستمرار، وتشمل جرائم الاختراق الإلكتروني، والاحتيال عبر الإنترنت، وسرقة البيانات والمعلومات، والابتزاز الإلكتروني، والتزوير الإلكتروني، وانتهاك الخصوصية، ونشر البرمجيات الخبيثة، وغيرها من الجرائم التي تمس الأفراد والمؤسسات والدول على حد سواء.

وقد أظهرت الدراسة كذلك أن التشريعات الحديثة لم تعد قادرة على الاكتفاء بالقواعد التقليدية لمواجهة هذا النوع من الجرائم، بل أصبح من الضروري استحداث نصوص قانونية خاصة تتلاءم مع طبيعة البيئة الرقمية. ولهذا سعت العديد من الدول، ومنها الجزائر، إلى سن تشريعات متخصصة وتجريم مختلف الأفعال الماسة بالأنظمة المعلوماتية والبيانات الرقمية، مع وضع إجراءات خاصة للتحري والتحقيق والإثبات الإلكتروني.

ورغم هذه الجهود التشريعية، فإن مكافحة جرائم الإنترنت ما زالت تواجه العديد من التحديات، من بينها التطور المستمر للوسائل التقنية المستخدمة من قبل المجرمين، وصعوبة تتبعهم وتحديد هوياتهم الحقيقية، ونقص الكفاءات التقنية المتخصصة، فضلًا عن الإشكالات المرتبطة بالاختصاص القضائي الدولي وتضارب القوانين بين الدول.

ومن خلال ما سبق يمكن استخلاص النتائج التالية:

أولًا: أصبحت جرائم الإنترنت من أخطر أشكال الإجرام المعاصر نظرًا لارتباطها بالتطور التكنولوجي المستمر.

ثانيًا: تتميز الجرائم الإلكترونية بخصائص فريدة تجعل اكتشافها وإثباتها أكثر صعوبة مقارنة بالجرائم التقليدية.

ثالثًا: تشكل الأدلة الرقمية عنصرًا أساسيًا في إثبات الجرائم الإلكترونية، مما يستدعي تطوير وسائل جمعها وحفظها وتحليلها.

رابعًا: ساهم المشرع الجزائري في تعزيز الحماية القانونية من خلال سن قوانين خاصة تتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

خامسًا: يبقى التعاون الدولي ضرورة حتمية لمواجهة الجرائم الإلكترونية نظرًا لطبيعتها العابرة للحدود.

وانطلاقًا من النتائج المتوصل إليها، يمكن تقديم التوصيات الآتية:

- مواصلة تحديث التشريعات المتعلقة بالجرائم الإلكترونية لمواكبة المستجدات التقنية.
- تعزيز التكوين المتخصص للقضاة وأعضاء النيابة العامة وضباط الشرطة القضائية في مجال الأدلة الرقمية.
- دعم المخابر الجنائية الرقمية وتزويدها بالوسائل التقنية الحديثة.
- نشر الثقافة الرقمية والوعي الأمني بين مختلف فئات المجتمع.

- تشجيع التعاون بين المؤسسات الحكومية والقطاع الخاص في مجال الأمن السيبراني.
- تعزيز آليات التعاون الدولي وتبادل المعلومات والخبرات بين الدول.
- تطوير برامج الحماية المعلوماتية داخل المؤسسات العامة والخاصة.



# قائمة المراجع

**القــوانين :**

1- قانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

2- القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

3- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

4- اتفاقية بودابست بشأن الجريمة الإلكترونية، مجلس أوروبا، 2001.

5- الأمم المتحدة، تقارير مكتب الأمم المتحدة المعني بالمخدرات والجريمة حول الجرائم السيبرانية.

**الكتب العامة:**

1- أحمد شوقي الشقاقي، جرائم الحاسب الآلي والإنترنت، دار النهضة العربية، القاهرة، 2015.

2- أحمد عبد الكريم سلامة، جرائم الحاسب الآلي والإنترنت، دار النهضة العربية، القاهرة، 2017.

3- أحمد الطاهر عبد الطاهر، الجوانب القانونية لجرائم الإنترنت، دار النهضة العربية، القاهرة، 2017.

4- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، 2021.

5- محمد صبحي نجم، جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2018.

6- محمد سعيد نمور، جرائم تقنية المعلومات، دار الثقافة للنشر والتوزيع، عمان، 2018.

7- محمد حزيط، قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر.

8- عبد العزيز سعد، الجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات، دار هومة، الجزائر.

9- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريع المقارن، دار الفكر الجامعي، الإسكندرية، 2007.

10- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2016.

11- عبد القادر البقيرات، الجرائم الإلكترونية وآليات مكافحتها، دار الخلدونية، الجزائر، 2018.

12- عبد الرؤوف مهدي، شرح الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2019.

13- عبد العزيز سعد، الجرائم الواقعة على نظم المعلومات، دار هومة، الجزائر، 2019.

**الكتب المتخصصة :**

1- عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2013.

2- عبد الرزاق الشيخ علي، الجريمة المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2016.

3- عبد الفتاح بيومي حجازي، الجرائم المستحدثة واستخدام الإنترنت في القانون الجنائي، دار الفكر الجامعي، الإسكندرية، 2016.

4- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2011.

5- أحمد الطاهر عبد الطاهر، الجرائم الإلكترونية وأدلة الإثبات الجنائي الإلكتروني، دار النهضة العربية، القاهرة، 2020.

6- محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

7- محمد حسين منصور، غسل الأموال في ظل التطور التكنولوجي، دار الجامعة الجديدة، الإسكندرية، 2016.

8- حسن قاسم، الحماية الجنائية للمعطيات الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2014.

9- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2010 و2015.

10- محمد سعيد نمور، الحماية الجنائية للحياة الخاصة عبر الإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2018.

11- محمد صحراوي، الحماية القانونية للبيانات الشخصية في التشريع الجزائري، مجلة الدراسات القانونية، العدد 12، 2020.

12- محمد سعيد نمور، شرح قانون الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان.

13- محمد أمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.

## مذكـــرات التخرج :

1- بلعربي سليمة، خصوصية المتابعة في الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر، المركز الجامعي مغنية، 2020.

2- بدودة عزيزة، علّالي سعاد، التحقيق الجنائي في الجرائم الرقمية، مذكرة ماستر، جامعة غرداية، 2018.

## مراجع أجنبيـة :

1- Bouberguig, A., Automated data processing systems offences in Algerian Penal Code, Journal of Legal Studies, (2018).

# الفـــهـــــرس

إهداء

شكر وعرفان

مقدمة .....أ

**الفصل الأول : الاطار النظري لجرائم الانترنت.....4**

المبحث الأول : ماهية جرائم الانترنت.....4

المطلب الأول : تعريف جرائم الانترنت.....5

الفرع الأول: التعريف الفقهي .....6

الفرع الثاني : التعريف القانوني.....8

المطلب الثاني : خصائص جرائم الانترنت.....9

الفرع الأول : الخصائص التقنية.....10

الفرع الثاني: الخصائص القانونية.....11

المبحث الثاني : أركان و أنواع جرائم الانترنت.....15

المطلب الأول : أركان جرائم الانترنت.....15

الفرع الأول : الركن الشرعي.....15

الفرع الثاني: الركن المادي و المعنوي .....16

المطلب الثاني : انواع جرائم الانترنت.....19

الفرع الأول : الجرائم الماسة بالأشخاص .....19

الفرع الثاني: الجرائم الماسة بالاموال و الانظمة.....22

**الفصل الثاني : الآليات القانونية لمكافحة جرائم الانترنت في الجزائر .....34**

المبحث الأول : الحماية القانونية في القوانين العامة .....35

المطلب الأول : جرائم الإنترنت في قانون العقوبات .....35

الفرع الأول : الجرائم المنصوص عليها .....35

الفرع الثاني: العقوبات المقررة .....37

المطلب الثاني : الإجراءات الجزائية الخاصة بجرائم الانترنت .....39

الفرع الأول : التحري والتحقيق .....40

الفرع الثاني: المتابعة والمحاكمة في جرائم الإنترنت.....44

المبحث الثاني : الحماية القانونية في القوانين الخاصة .....53

المطلب الأول : القوانين الخاصة بجرائم الانترنت .....54

الفرع الأول : قانون الجرائم الإلكترونية .....55

الفرع الثاني: قانون حماية المعطيات الشخصية.....57

المطلب الثاني : آليات الوقاية والمكافحة.....58

الفرع الأول : دور الهيئات المتخصصة .....58

الفرع الثاني: التعاون الوطني والدولي .....63

خاتمة.....70

قائمة المراجع.....74

الفهرس.....77

الملخص .....79

# مـلخص مذكرة الماستر

تعد جرائم الإنترنت من أخطر الظواهر الإجرامية المعاصرة التي أفرزتها الثورة الرقمية والتطور المتسارع في تكنولوجيا المعلومات والاتصالات، حيث أصبحت مختلف الأنشطة الإنسانية مرتبطة بالأنظمة المعلوماتية والشبكات الإلكترونية، الأمر الذي أدى إلى ظهور أنماط إجرامية جديدة تختلف عن الجرائم التقليدية من حيث الوسائل والأساليب وآثارها القانونية والاقتصادية والاجتماعية. وقد فرض هذا الواقع تحديات كبيرة على المشرع وأجهزة العدالة الجنائية، مما استوجب وضع قواعد قانونية وإجرائية خاصة لمواجهتها.

تهدف هذه الدراسة إلى إبراز مفهوم جرائم الإنترنت وخصائصها وأهم صورها، من خلال التعرض للتعريفات الفقهية والقانونية لهذه الجرائم، وبيان خصائصها التقنية والقانونية التي تميزها عن غيرها من الجرائم. كما تتناول الدراسة أهم أنواع جرائم الإنترنت، لاسيما الجرائم الماسة بالأشخاص كالاعتداء على الحياة الخاصة والتشهير الإلكتروني والابتزاز الإلكتروني، والجرائم الماسة بالأموال كالاحتيال الإلكتروني وسرقة البيانات والأموال، إضافة إلى الجرائم الماسة بالأنظمة المعلوماتية كالدخول غير المشروع وإتلاف البيانات ونشر البرمجيات الخبيثة.

كما تبحث الدراسة في الحماية القانونية المقررة لمكافحة جرائم الإنترنت من خلال النصوص العامة الواردة في قانون العقوبات، والنصوص الخاصة التي استحدثها المشرع لمواجهة الجرائم الإلكترونية، مع التطرق إلى التشريعات المتعلقة بحماية المعطيات الشخصية. كذلك تتناول الدراسة آليات التحري والتحقيق في الجرائم الإلكترونية، بما في ذلك تفتيش الأنظمة المعلوماتية، واعتراض المراسلات الإلكترونية، والمراقبة الإلكترونية، وتتبع الاتصالات الرقمية، ودور الهيئات المختصة في الوقاية والمكافحة.

وقد خلصت الدراسة إلى أن مكافحة جرائم الإنترنت تتطلب منظومة قانونية متكاملة تجمع بين النصوص الموضوعية والإجرائية، مع ضرورة مواكبة التشريعات للتطور التقني المستمر، وتعزيز التعاون الوطني والدولي، وتوفير الكفاءات البشرية والوسائل التقنية اللازمة للكشف عن الجرائم الإلكترونية وإثباتها وملاحقة مرتكبيها، بما يحقق التوازن بين حماية المجتمع وصون الحقوق والحريات الأساسية للأفراد.



**الكلمات المفتاحية :**

جرائم الإنترنت، الجريمة الإلكترونية، الأنظمة المعلوماتية، الأدلة الرقمية، التحري الإلكتروني، الأمن السيبراني، الحماية القانونية، المعطيات الشخصية

# Abstract of Master's Thesis

Cybercrime has become one of the most serious contemporary criminal phenomena resulting from the digital revolution and the rapid development of information and communication technologies. The increasing reliance on information systems and electronic networks in various aspects of life has led to the emergence of new forms of criminal activity that differ from traditional crimes in terms of methods, means, and consequences. This situation has created significant challenges for legislators and criminal justice authorities, requiring the adoption of specific legal and procedural mechanisms to address such offenses.

This study aims to examine the concept of cybercrime, its characteristics, and its main forms. It analyzes both doctrinal and legal definitions of cybercrime and highlights its technical and legal features. The study further explores the different categories of cybercrime, including crimes against persons such as violations of privacy, cyber defamation, and online blackmail; crimes against property such as electronic fraud, theft of data and funds; and crimes against information systems such as unauthorized access, data destruction, and the dissemination of malicious software.

The research also focuses on the legal protection mechanisms established to combat cybercrime through both general criminal law provisions and special legislation enacted to address cyber offenses. In addition, it examines laws related to personal data protection and discusses modern investigative measures, including computer system searches, interception of electronic communications, electronic surveillance, and digital communication tracking. The study further highlights the role of specialized institutions and the importance of preventive and repressive measures at both national and international levels.

The study concludes that combating cybercrime requires a comprehensive legal framework that combines substantive and procedural rules, continuous adaptation of legislation to technological developments, enhanced national and international cooperation, and the provision of adequate technical resources and specialized expertise. Such measures are essential to ensure effective prevention, detection, investigation, and prosecution of cybercriminal activities while safeguarding fundamental rights and freedoms

**key words:**
Cybercrime, Electronic Crime, Information Systems, Digital Evidence, Electronic Investigation, Cybersecurity, Legal Protection, Personal Data Protection