كلية الحقوق والعلوم السياسية لونيسي علي _بليدة 02_



القرصنة الالكترونية في التشريع الجزائري

أطروحة مكملة لنيل شهادة الدكتوراه في القانون.

تخصص: قانون جنائي

إعداد الباحثة: **إشراف الأستاذة:**

عناصر خيرة **أ.د روابح إلهام شهرزاد**

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
برحماني محفوظ	أستاذ التعليم العالي	البليدة	رئيسا
روابح إلهام شهرزاد	أستاذ التعليم العالي	البليدة	مشرفا ومقررا
رزاقي نبيلة	أستاذ التعليم العالي	البليدة	مناقشا
يعقر طاهر	أستاذ التعليم العالي	خميس مليانة	مناقشا
علياتي محمد	أستاذ التعليم العالي	المدية	مناقشا
جوهر قوادري صامت	أستاذ التعليم العالي	الشلف	مناقشا

السنة الجامعية:2026/2025

بِسْمِ اللهِ الرحمن
الرَّحِيمِ

(إِنَّا عَرَضْنَا الْأَمَانَةَ عَلَى السَّمَاوَاتِ
وَالْأَرْضِ وَالْجِبَالِ فَأَبَيْنَ أَنْ يَحْمِلْنَهَا
وَأَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْإِنْسَانُ)

سورة الأحزاب الآية 72

الإهداء :

إلى وطني الذي أسندت إليه كياني، وملاذي الذي يملأ فضاءاتي وأحزاني ومشاتلي التي غرستني حبا طيبة وحنانا أمـــي الغالية حفظها الله وأسعدها.

إلى الجبل الشامخ، وكتابي المفتوح، والقلاع الحصينة أبـــي حفظه الله

إلى زوجي الذي قاسمني الهموم والابتلاءات، وكان حلي وترحالي

إلى أطيافي الجميلة التي تملأ دنياي غبطة وسرورا.

لأنك كنت جزءا من هذه الرحلة بصمتك وألمك، شاركتني البيت فكنت جزءا من معاناتي وقوتي، ولأن وجودك علمني الصبر أكثر مما علمتني الكتب، أهديك هذا العمل أخي الغالي

إخوتي وأخواتي وأحبابي

شكر وعرفـان

الحمد لله الذي رفع السماء وعلم ادم الأسماء وانزع بحكمته الداء ومن عدله وفضله جعل لكل داء دواء، الذي ميزنا بالعلوم وقضى ألا يستوي الذين يعلمون والذين لا يعلمون،

الحمد لله الذي خلق الإنسان في أحسن تقويم وجعل له عقلا وحباه بالتكريم، سبحانه رفع شأن العلم فاقسم بالقلم وامتن على الإنسان فعلمه ما لم يكن يعلم، بعث لنا خير خلقه وصفوة رسله رحمة وملاذا رسوله المصطفى ونبيه المرتضى معلم الحكمة وهادي الأمة صلى الله عليه وعلى اله الأبرار.

ثم إنه لا يشكر الله من لا يشكر الناس، وبهذه اللحظة التي أعتبرها منعطف حياتي، فإني أتقدم بجزيل الشكر والعرفان إلى أسرة جامعة البليدة 2 _ كلية الحقوق والعلوم السياسية، إدارة وأساتذة وموظفين، على الدعم الأكاديمي والمحفز الذي أتيح لي

كما أتوجه بجزيل الشكر والعرفان للأستاذة المشرفة الأستاذة روابح إلهام شهرزاد بخالص الامتنان، التي كانت سيفي وقلمي ويرجع لها فضل تقدمي في هذا العمل العلمي، التي أمدتني بالكثير من الإرشادات والتوجيهات وتذليل الكثير من الصعوبات فجزاها الله كل خير، كما أني أعترف أن جهدي هذا هو جهد المقل وحسبي أني وضعت لبنة تضاف لباقي اللبنات، ولا أحسب أنني قدمت الكثير لكنها استضاءة ومحاولة مني الخوض في هذا المجال الصعب، وقد أخذ مني الجهد والوقت لإخراجه في هذه الأطروحة.

كما لا يفوتني تقديم جزيل الشكر إلى لجنة المناقشة على جهدهم في مراجعة هذا العمل وتقديم التوجيهات والنصائح، إليكم جميعا أيها الغوالي أهدي أطروحتي.

قائمة المختصرات

باللغة العربية

ج: جزء

ج ر: الجريدة الرسمية

ص: صفحة

ق.م.ج: القانون المدني الجزائري

ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري

ق.ت: القانون التجاري

ق.ع: قانون العقوبات

ق.ح.ح.م: قانون حماية حقوق المؤلف

ع: عدد

س: سنة

ط: طبعة

م: مجلد

ق.ع.ف: قانون العقوبات الفرنسي

م.ق: المجلة القضائية

باللغة الفرنسية:

ART : Article

EDIT : Edition

N° : Numéro

P : Page .Op.cit. : OpuceCitatum

مقـــدمـة

مقدمة

منذ أن خلق الله الإنسان على كوكب الأرض كانت رحلته تكمن في البحث عن التقدم والتطور، ففي البدء كانت حياته بسيطة إذ كان يعيش الحياة القاسية المريرة، فكان لابد من الاعتماد على نفسه في تحصيل قوته اليومي، ومع مرور الزمن تغيرت نظراته للحياة فكان لابد من تطوير مهاراته وقدراته التي وهبها الله له، فبانت ثقافات أخرى مركونة مع شعوب أخرى، فمن الاعتماد على أدوات بسيطة أنية كالصيد، البحث عن رمق العيش، فالوصول إلى اكتشاف الأدوات الاحتجاجية وصنعها من المعدن الأرضي، وصولا للثورة الصناعية المذهلة التي كانت بدايتها في القرن الثامن عشر، حيث شهد العالم تطورا متسارعا في مختلف المجالات، ولاسيما في المجال العلمي والتكنولوجي، حيث أخترع الهاتف والتلغراف وهو وسيلة التواصل بين الشعوب وبعضها البعض، إلا أن تطور أكثر حين ظهرت الشبكة العنكبوتية التي دخلت على المجتمع فانقلب على عقبيه، فكان الحاسوب الذي زاد من تسريع الحركة التواصلية وصولا للقرن الواحد والعشرون الذي شهد تطورا مذهلا في كل المجالات، فظهرت الهواتف الذكية، والذكاء الاصطناعي، وهذا العصر بالذات يشهد تقدما مذهلا وقد سماه العلماء بعصر التكنولوجيا، أين صارت التكنولوجيا جزءا لا يتجزأ من حياتنا اليومية التي لا نستطيع الاستغناء عنها، وسهلت التواصل، ونشرت الثقافة، واختصرت الوقت والمسافة بين الشعوب.

وفي ظل التطور السريع للتكنولوجيا، خاصة في مجال الإعلام والاتصال وتزايد الذكاء الاصطناعي مما أدى إلى ظهور وسائل حديثة للحصول على المعلومات وتبادلها، فقد أصبح استخدام الحاسب الآلي وشبكات الاتصال، وعلى رأسها شبكة الإنترنيت، وسيلة أساسية لنقل المعلومات بسرعة وسهولة، الأمر الذي جعل تداولها عبر الشبكات أمرا مألوفا في مختلف مجالات الحياة، لا سيما في ميدان التعاملات الرقمية.

غير أن هذا التطور الكبير في تقنيات الاتصالات السلكية واللاسلكية، وما صاحبه من انفتاح وتوسع في استخدام الإنترنيت، أدى في المقابل إلى بروز مخاطر وأساليب جديدة تمثلت في ظهور أنماط حديثة من الجرائم، كالاختراق، الاختلاس، والتدمير والسطو الالكتروني، والتشهير الإلكتروني باستعمال منصات رقمية وغيرها من الجرائم ترتكب من مكان إلى أخر، ومن شخص إلى أخر وهو ما يعرف بالجرائم المعلوماتية.

وتشمل هذه الجرائم العديد من الأفعال غير المشروعة مثل عملية الاختراق للحاسوب غير القانونية وغير الشرعية بهدف سرقة المعلومات، أو حتى الأموال، وتدمير البيانات، وغيرها من الاعتداءات التي

تستهدف الأنظمة المعلوماتية وبيانات الأفراد والمؤسسات وهذا ما يشكل تهديدا حقيقيا لأمن المعلومات وخصوصية الأفراد والمؤسسات.

كما أن هذا النوع من الجرائم يمثل أحد أبرز التحديات التي تواجه المجتمعات المعاصرة، لما يشكله من خطر على أمن المعلومات وخصوصية الأفراد وسلامة المعاملات الإلكترونية، فنظرا لتزايد هذه الجرائم وتطور أساليب ارتكابها تزامنا مع التطور التقني، سارعت مختلف دول العالم إلى وضع أطر قانونية وتشريعية لمكافحتها والأفعال المرتبطة بالاعتداء على الأنظمة المعلوماتية ضمن القوانين المتعلقة بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، كما تضمن قانون العقوبات أحكاما خاصة بتجريم الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات .

وفي هذا السياق، سعى المشرع الجزائري لمواجهة هذه الظاهرة، مواكبا التطور التكنولوجي من خلال تدخلاته التشريعية، فوضع بعض النصوص التشريعية والإجراءات الخاصة لمواجهة الجرائم المرتبطة بالإنترنيت من أبرزها القانون رقم 04_15 سنة 2004 المتعلق بأنظمة المعالجة الآلية للمعطيات ، تلاه لاحقا القانون 09_04 المتعلق بجرائم تكنولوجيا الاعلام والاتصال ، ضمن جرائم الإنترنيت التي تعد أفعالا تستهدف أنظمة المعلومات التي يحميها قانون العقوبات، وكون هاته النصوص التشريعية جاءت على فترات متباعدة زمنيا إلا أنها سعت إلى رفع التحديات في مواجهة هذا النوع من السلوكيات غير المشروعة، إما التي يتم تنفيذها باستخدام الإنترنت كوسيلة، أو تلك التي تكون شبكة الإنترنيت أو أنظمتها هي المستهدفة على حد سواء، غير أن هذه الإجراءات في الواقع العملي لا تزال محل تساؤل، خاصة في ظل نقص الإحصائيات الدقيقة وغياب معطيات واضحة حول حجم الاستعمال غير المشروع لشبكة الانترنيت.

كما أنه من المهم الإشارة إلا أنه رغم المساعي الحميدة والجهود التشريعية التي بذلتها الجزائر من خلال سن القوانين مسايرة بذلك التطور التكنولوجي لم تحدد مدى فعاليتها على أرض الواقع فهي لا تزال محل نقاش وتساؤل كونها مرتبطة بمدى توفر الإمكانيات التقنية والبشرية المتخصصة لدى جهات التحقيق والمتابعة القضائية، إضافة إلى ضرورة تعزيز التكوين المتخصص في مجال الجرائم وتوفير الأجهزة والبرمجيات المتخصصة، مع تطوير مهارات الأجهزة الأمنية في مواجهة عالم القرصنة الإلكترونية، حماية للفضاء الرقمي للمواطنين وتأمين حقوقهم.

أهمية الدراسة

نظرًا إلى أن موضوع الجرائم الإلكترونية قد حظي باهتمام واسع في البحوث والدراسات القانونية، فإن دراسة القرصنة الإلكترونية، باعتبارها إحدى صور هذه الجرائم، تظل ذات أهمية خاصة، بالنظر إلى التطور المستمر في الأدوات والتقنيات المعلوماتية المستعملة في ارتكابها. وقد أدى هذا التطور إلى تعدد صور الجرائم المرتبطة بها وتجدد أساليب ارتكابها، بما يثير جملة من الإشكالات القانونية والإجرائية، ويبرز أهمية البحث في مختلف المشكلات التي يطرحها هذا الموضوع.

فعلى الصعيد العلمي فإن الأهمية من هذه الدراسة هو الرغبة في تسليط الضوء على ظاهرة إجرامية يزداد انتشارها يوما بعد يوم تزامنا مع الانتشار الهائل لمستعملي الكمبيوتر وشبكة الإنترنيت وهو ما تفطن له المشرع الجزائري أين صادق على اتفاقية الأمم المتحدة لمكافحتها سنة 2002، كما أدرج بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، أحكاما خاصة لمواجهة الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات، وذلك من خلال استحداث القسم السابع مكرر ضمن الباب المتعلق بالجرائم ضد الأموال، والمتضمن المواد 394 مكرر إلى 394 مكرر 7. ثم عرفت هذه المنظومة الجزائية تعديلات لاحقة بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم لقانون العقوبات، بما يستوجب الرجوع إلى الصيغة التشريعية النافذة عند بيان الأحكام الجزائية المتعلقة بالقرصنة الإلكترونية. حتى يتصدى لهذه الجريمة متخذا سبيل التشريعات الأجنبية.

أما **من الناحية العملية:** فان التطور الرقمي المتسارع أدى إلى ظهور ظاهرة القرصنة الإلكترونية على الصعيدين الدولي والوطني، فأصبح ضرورة ملحة، البحث فيها بغرض إيجاد حلول جذرية للعديد من المشكلات العملية ولعل أبرزها المتعلقة بالإثبات عن طريق الأدلة المتحصل عليها من الوسائل الإلكترونية (حواسيب خوادم، بيانات رقمية، .....إلخ) في إطار نظرية الإثبات الجنائي ، على اعتبار أن هذا الأخير هو المشكلة الأكثر تعقيدا ، فلا يفر مرتكبوها من العقاب، وفي ذات الوقت لا يحدث اعتداء على الحريات الفردية للأفراد وتنتهك حرمات حياتهم الخاصة وعلى هذا الأساس سيحاول هذا البحث أن يحدد الأسس التي تحقق التكافؤ بين التشريع الجنائي الموضوعي والتشريع الإجرائي وهذا بغرض تسليط الضوء على خصوصية هذا النوع من الجرائم، على مستوى مختلف الأنظمة القانونية بصفة عامة و التشريع الجزائري بصفة خاصة الذي تبني تجريم هذه الأفعال في القانون 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها .

أما عن **أسباب اختياري** لموضوع القرصنة الإلكترونية في التشريع الجزائري فهي عديدة يمكن تقسيمها إلى أسباب موضوعية وأخرى ذاتية

فالأسباب الموضوعية لاختيار الموضوع تكمن في الأهمية العلمية والعملية التي يكتسيها، بالنظر إلى ما تثيره جرائم القرصنة الإلكترونية من إشكالات قانونية وإجرائية متجددة، لا سيما مع التطور المستمر لوسائل ارتكابها وتنوع صور الاعتداء على الأنظمة المعلوماتية، وما يترتب عن ذلك من صعوبات في تحديد الأفعال المجرّمة وتكييفها القانوني وإثباتها، فضلًا عن مدى ملاءمة القواعد الإجرائية الجزائية لمتطلبات البحث والتحري والإثبات في البيئة الرقمية.

ويضاف إلى ذلك محدودية الدراسات القانونية المحلية المتخصصة التي تناولت هذه الجريمة بصورة مستقلة ومتكاملة، رغم تنامي صورها واتساع نطاق آثارها على الأفراد والمؤسسات، الأمر الذي يبرر الحاجة إلى دراسة الإطار القانوني والإجرائي الذي أقره المشرع الجزائري لمواجهتها.

أما **الأسباب الذاتية** فهي رغبة الباحثة لاكتشاف هذا المجال من خلال دراسة الآليات القانونية والإجرائية لملاحقة الجرائم الإلكترونية ومعرفة كيفية تطبيق القوانين المتعلقة بالقانون الرقمي، لتقديم إضافة في البحث العلمي التخصصي حتى يكن مرجعا للباحثين في هذا المجال، ولعل من أهم الدوافع التي جعلتني اختار موضوع البحث هذا هو الإلمام والإحاطة بمختلف جوانب الموضوع وعناصره من خلال الاعتماد على تقصي النصوص القانونية في التشريع الوطني والاتفاقيات الدولية بغرض تقديم إضافة علمية تسهم في رفع مستوى الوعي المجتمعي بمخاطر القرصنة، وتعزيز الأمن الرقمي للأفراد والمؤسسات، كما يقدم للجامعات مراجع تحليلية وتقويمية حول الإطار القانوني للقرصنة الإلكترونية ومنه إثراء المناهج الدراسية وورشات العمل الأكاديمية ، كذلك يسهم البحث في دعم المؤسسات التربوية والتعليمية لتطوير برامج توعية وحماية الطلاب والكوادر من مخاطر القرصنة الالكترونية، كما أن رغبتي الخاصة في البحث ترتكز على اهتمامي الشخصي بهذا المجال لما يكتسبه من مستجدات وإشكالات يؤدي البحث فيها إلى الوصول إلى نتائج موضوعية ذات قيمة تطبيقية .

إشكالية الدراسة:

في ظل التطور الرقمي السريع الذي فرض إدخال تعديلات على قانون العقوبات واستحداث نصوص قانونية خاصة لتجريم الأفعال التي تمس أنظمة المعالجة الرقمية فانه يمكن تحديد الإشكالية الرئيسية لهذه الدراسة من خلال تحليل النصوص القانونية التي وضعها المشرع الجزائري، وخصوصا القانون 09_04

المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مما يتبادر في ذهننا تساؤلات جوهرية حول كفاية النصوص القانونية للحد من الجرائم، أم أن هناك حاجة ملحة لمواكبة التجارب الدولية وذلك باستحداث قوانين خاصة بكل نوع من أنواع الجرائم الالكترونية بما فيها القرصنة الالكترونية.

بناء على ما سبق ذكره، تبرز لنا الإشكالية في السؤال الرئيسي

كيف واكب المشرّع الجزائري جريمة القرصنة الإلكترونية في ظل التطور المتسارع لتكنولوجيات الإعلام والاتصال، وذلك من خلال تجريم مختلف صور الاعتداء على الأنظمة والمعطيات المعلوماتية، وتنظيم إجراءات البحث والتحري والإثبات المتعلقة بها؟ وإلى أي مدى اتسمت النصوص القانونية ذات الصلة بالدقة في تحديد الطبيعة القانونية لكل فعل إجرامي على حدة، بما ينسجم مع خصوصية الجرائم المرتكبة في البيئة الرقمية؟

وللتطرق وتوضيح هذه الإشكالية تم طرح عدة تساؤلات فرعية منها:

***ما المقصود بالقرصنة الإلكترونية في التشريع الجزائري وما نطاق تجريمها؟**

***هل النصوص القانونية التي اعتمدها المشرع الجزائري كافية لتجريم القرصنة الإلكترونية؟**

***ما هي وسائل الإثبات المعتمدة في الجرائم الإلكترونية أمام القضاء الجزائري؟**

***ما هي الوسائل المتبعة لمكافحة هاته الجريمة؟**

كما أنه من خلال دراسة القوانين التشريعية الجزائرية برزت بعض الإشكاليات الجزئية الجديدة التي ولدتها ظاهرة المعلوماتية وتطبيقاتها المتعددة خاصة في نطاق القانون الجنائي.

ومن بينها مدى ملاءمة تطبيق المفاهيم القانونية التقليدية، التي نشأت في بيئة مادية ملموسة، للتطبيق على الفضاء الرقمي الذي يتميز باللامادية والسرعة والعالمية، فالمفاهيم الكلاسيكية في القانون الجنائي، كفكرة المال المادي، والسرقة قد تواجه صعوبات عند إسقاطها على الأفعال التي تستهدف المعطيات والأنظمة المعلوماتية ومنه يتبادر إلى ذهننا التساؤل حول إمكانية الاكتفاء بتكييف هذه المفاهيم التقليدية لتشمل الاعتداءات المعلوماتية، أو أصبح من الضروري البحث عن بدائل قانونية أخرى، كالاستعانة باليات الحماية التي توفرها نصوص الملكية الفكرية، أم نحن بحاجة إلي نصوص جزائية خاصة تراعي خصوصية الجريمة المعلوماتية.

صعوبات الدراسة

بالرغم من الصعوبات العديدة التي صادفتني هي الصعوبات المرتبطة بمطبيعة الموضوع، والمراجع ذات الصلة سواء من بحوث أو دراسات وخاصة منها المتعلقة بالتشريع الجزائري والسبب يعود إلى أن القرصنة الإلكترونية أمر مستحدث وبالتالي يحتاج لمزيد من البحث والدراسة في هذا المجال بالإضافة إلى قلة الأحكام والسوابق القضائية، كل ذلك فرض بذل مجهودات مضاعفة لتتبع المعلومات وتحليلها بدقة، من أجل بناء تصور شامل يوفق بين الجانب النظري والممارسة العملية، والوصول إلى نتائج علمية دقيقة تستجيب لمتطلبات الدراسة الأكاديمية في هذا المجال، ومن أبرز الصعوبات التي اعترضت البحث، صعوبة الوصول إلى الحالات والتطبيقات القضائية بسبب طبيعتها الحساسة إذ غالبا ما تكون محاطة بالسرية، الأمر الذي جعل من الضروري البحث في الدراسات المغايرة والسابقة للباحثين من الشرق الأوسط، ويمكن القول أن هذه الصعوبات، رغم حدتها كانت دافعا أساسيا نحو مزيد من التعمق العلمي والابتكار في منهجية البحث.

الدراسات السابقة:

نظرا لحداثة الموضوع من خلال بحثنا فيه لاحظنا أن الباحث الجزائري يدرس القرصنة الإلكترونية في إطار الجرائم الإلكترونية ومن بين الدراسات السابقة نجد:

حسين طاهري، عالج موضوع **جرائم القرصنة الإلكترونية، دراسة تحليلية** مقارنة مرفقة بالاجتهاد القضائي المقارن في مجال الجرائم المعلوماتية والقرصنة الالكترونية، دار الخلدونية، الطبعة الأولى، 2023 ، حيث سلط الضوء على طبيعة هذه الجرائم القانونية، وآثارها على منظومة القانون الجنائي، وصعوبة تكييفها في التشريعات الوطنية، كما قارن بين الاجتهادات القضائية في بعض النظم القانونية للتوصل إلى فهم أعمق للظاهرة، وركزت الدراسة على أهمية حماية المعطيات الإلكترونية، لما لهذا من مخاطر على اقتصاديات الدول ومنها الأمن القومي وسيادتها وتأثيرها على العمليات المالية والمصرفية والتجارة الالكترونية فضلا عن أضرارها على المجتمع والمنظومة الأخلاقية وعلى صغار السن والشباب.

خالد أحسن احمد لطفي، جرائم الإنترنيت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2018 الذي يشرح من خلال كتابه معنى الجرائم الإلكترونية محددا الفرق بينها وبين الجرائم التقليدية، ليتطرق الى القرصنة الإلكترونية في صورة الاختراق يحدد من هم المخترقون وطرق الاختراق، كما يبين الفرق بين جرائم القرصنة الإلكترونية والابتزاز الالكتروني، فالكتاب عبارة عن دراسة قانونية مقارنة يشرح طبيعتها وأساليبها والعقوبات القانونية وطرق الوقاية منها.

فيصل بدري، مكافحة الجريمة المعلوماتية، في القانون الدولي والداخلي، **أطروحة دكتوراه علوم تخصص قانون عام**، جامعة الجزائر 1-بن يوسف بن خدة-2017، **2018**، يتناول الجريمة المعلوماتية على المستويين الدولي والوطني وسبل مكافحتها من خلال إبراز الجهود الدولية والوطنية في مواجهة الجرائم المعلوماتية كنوع جديد ومستحدث، مع إبراز الصعوبات والتحديات التي تقف أمام فعالياتها.

غنية باطلي، الجريمة الإلكترونية دراسة مقارنة، الدار الجزائرية 2015، تناولت الباحثة الجريمة الإلكترونية مرتكزة على التشريع الجزائري، في تكييفه لجريمة الدخول والخروج، والمعالجة الآلية للمعطيات من خلال القوانين **15/04** والقانون **09-04** المتعلق بتكنولوجيا الإعلام والاتصال، مبرزة أركان كل جريمة والعقوبات المقررة لها.

تركز الدراسة على استعراض الأحكام القانونية والتنظيمية ذات الصلة، وتحليل مدى توافقها مع المعايير والتوجيهات الدولية في هذا المجال، ويؤكد الباحث على الحاجة إلى تطير نظام قانوني خاص بجريمة القرصنة الإلكترونية، يواكب التحولات العالمية يستجيب لمتطلبات التنمية المستدامة في الجزائر، كما تسعى الدراسة إلى توضيح الرؤية القانونية الحالية، من خلال تحليل النصوص التشريعية والتنظيمية، تقديم تصور لإصلاح هذا النظام بما يضمن تكامله مع المعايير الدولية، ومراعاة الخصوصيات الوطنية.

تقسيمات الدراسة:

على غرار الإشكالية التي طرحتها في سياق المقدمة ارتأيت معالجة هذا الموضوع من الناحية الموضوعية والإجرائية، عن طريق الإجابة على العديد من الإشكاليات بموجب خطة محورية لمضمون الأطروحة موزعة على مقدمة، وبابين وخاتمة، معتمدة على القوانين والمراسيم واجتهادات المحكمة العليا مع استخراج الأسس القانونية التي تحكم الجريمة عبر مختلف مراحلها، وفق التقسيم التالي:

الباب الأول: الإطار القانوني والموضوعي للقرصنة الإلكترونية ضمن الجرائم المعلوماتية

يصف بعض الفقه الجرائم الالكترونية بالجرائم العابرة للحدود، فالانتشار الكبير لهذا النوع من الجرائم أدى إلى المساس بالأمن والسيادة والاقتصاد على الصعيدين الوطني والدولي ونتج عنه ميلاد خطوات هامة للقضاء على جرائم تقنية المعلومات من خلال استخدام الوسائل الإلكترونية درئا للتجاوزات من قوانين وإجراءات، وعليه قسمت هذا الباب إلى فصلين تناولت في الأول الإطار القانوني للقرصنة الإلكترونية أما في الثاني فتناولت الآليات والنظام الجزائي والإجرائي لمكافحتها.

كما تضمن المبحث الأول للفصل الأول الإطار المفاهيمي للقرصنة، أما المبحث الثاني تضمن صور وطرق وأساليب القرصنة الإلكترونية، في حين تضمن الفصل الثاني الطبيعة القانونية والتكييف القانوني للقرصنة الالكترونية في المبحث الأول وذلك من خلال دراسة أركان الجريمة ثم تطرقت في المبحث الثاني إلى المسؤولية الجزائية والعقوبات المقررة لهذه الجريمة.

الباب الثاني: النظام الإجرائي لمكافحة جريمة القرصنة الإلكترونية

نظرا لما قد يترتب عن هذه الأفعال من أضرار تمس الأفراد والمؤسسات، تدخل المشرع لتجريم هذه الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك من خلال استحداث نصوص قانونية تهدف إلى حماية الأنظمة المعلوماتية وضمان أمن البيانات المتداولة.

أما في الباب الثاني تم التطرق إلى إجراءات سير الدعاوى المتعلقة بجريمة القرصنة الإلكترونية أين ركزت أساسا على القواعد والإجراءات القانونية التي تحكم متابعة هذه الجرائم منذ اكتشافها إلى غاية صدور الحكم وتنفيذه، بدءا من اكتشاف الجريمة بموجب شكوى، أو تبليغ، أو تحريات إلى دور النيابة العامة في تحريك الدعوى العمومية ، وخصوصية ذلك ثم انتقلنا إلى إجراءات البحث والتحري التي بينا دور الضبطية القضائية في جرائم القرصنة والوسائل التقنية المستعملة في التحري (تتبع ip ، فحص الأنظمة) والإشكالات المرتبطة بالاختصاص الإقليمي كونها من الجرائم العابرة للحدود، كما بينا من خلال الفصول المدرجة، فتضمن الفصل الأول إجراءات البحث والتحري أمام الشرطة القضائية ثم المتابعة من خلال المبحث الأول، ووسائل الإثبات في جرائم القرصنة الالكترونية والتي تركز على الأدلة الرقمية وحجية الدليل الالكتروني أمام القضاء في المبحث الثاني وتم التطرق أيضا إلى إجراءات المتابعة والتحقيق القضائي مبرزين دور قاضي التحقيق وإجراءات التفتيش والحجز الالكتروني وأوامر المراقبة والتتبع وأخيرا المحاكمة في جرائم القرصنة الالكترونية من سير المحاكمة وتقييم القاضي للأدلة الرقمية والصعوبات العملية (كتعقيد التقنية، ونقص الخبرة).

منهج الدراسة:

اعتمدت دراسة هذه الإشكالية على كل من المنهج التحليلي والوصفي الذي يظهر جليا من خلال تحليل مختلف النصوص القانونية المنظمة لهذا النوع من الجرائم والآثار القانونية المترتبة عن ارتكابها والحلول القانونية في حال ثبوت اقترافها وذلك استنادا إلى النصوص والتشريعات المنصوص عليها في قانون العقوبات للتصدي لهذا النوع من الجرائم والإجراءات المنصوص عليها في قانون الإجراءات الجزائرية والقوانين المكملة له.

لأمحص في خاتمة لجملة النتائج التي توصلنا إليها من خلال قراءة للنصوص التشريعية خاصة المستحدثة والمواكبة للعصر منها: القانون 09-04 المتعلق بالقواعد الخاصة الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وهو أبرز قانون نظم الجرائم المعلوماتية وعاقب على الدخول غير المشروع(القرصنة) وكذا القانون 04_15 المتضمن قانون العقوبات الجزائري (المواد 394 مكرر وما بعدها).

الباب الأول

الإطار المفاهيمي لجريمة القرصنة الإلكترونية

لقد أتاح الانتشار الواسع لاستخدام الحاسوب والأنظمة المعلوماتية وشبكات الاتصال الحديثة القدرة الهائلة على تبادل البيانات والوصول إلى المعلومة والتعرف عليها في وقت وجيز، وهو ما أبرز الدور الإيجابي للتطور التكنولوجي في هذا المجال، إلا انه بالرغم من المنافع التي يؤديها الحاسب الآلي التي جعلت من الحياة اليومية سهلة ومتطورة في مختلف الميادين الاقتصادية والإدارية، غير أن ذلك غير كافي كون المسألة لم تعد مسألة استخدام الحاسوب وشبكة الانترنيت فقط بل أصبحت مرتبطة بمدى القدرة على التحكم في مخاطره والحد من أضراره لما له من مساوئ وسلبيات كثيرة ومتنوعة، تمثلت في بروز أنماط جديدة من السلوكيات غير المشروعة المرتبطة باستغلال الوسائل المعلوماتية وذلك عن طريق الولوج غير المصرح به إلى الشبكات بغرض الحصول على المعلومات والتلاعب بها أو استغلالها بطرق غير قانونية الأمر الذي جعل بعض الباحثين يرون أن خطورة هذه السلبيات تفوق في بعض المرات الفوائد التي يحققها استخدام التكنولوجيا خاصة إذا ما تعلق الأمر بأمن المعلومات وخصوصية الأفراد واستقرار المؤسسات التي أصبحت في وقتنا الحالي تشكل تحديا حقيقيا ، الغرض منه ليس حماية الحاسوب والشبكات فقط عن طريق استخدام برامج الحماية، بل يجب فهم طريقة تفكير المخترقين وأساليبهم، لأن ذلك يساعد على اكتشاف نقاط الضعف في الأنظمة قبل أن يستغلها المهاجمون، وهنا تبرز الحاجة إلى وضع آليات قانونية وتقنية فعالة لتنظيم استخدام الشبكات بغرض تحقيق التوازن بين إيجابيات التكنولوجيا الحديثة والحد من أثار السلبية الناتجة عنها، ومن دون هذا الفهم الشامل يصبح من الصعب تحديد درجات الأمان الحقيقي للأنظمة والبيانات المخزنة فيها

فكون القرصنة الإلكترونية من الظواهر الإجرامية والموضوعات الحديثة المطروحة للنقاش في المحافل العلمية والدولية والإقليمية التي فرضت نفسها بقوة بسبب التطور المتسارع لتكنولوجيا الاتصالات أصبح من الضروري التوصل إلى فهم مشترك لهذه الظاهرة، وخصائصها بوصفها غالبا أفعال قد يرتكبها فرد واحد يمتلك مهارات تقنية عالية أو مجموعة من القراصنة يعملون بصورة منظمة عن طريق اختراق الأنظمة المعلوماتية والدخول بطريقة غير شرعية ومن دون ترخيص صاحبه وحتى دون علمه بغرض إلحاق أضرار كسرقة المعطيات أو إتلافها أو تعطيلها أو حذفها أو تغييرها بسوء نية لتحقيق الربح

وفي نفس السياق فان القرصنة الإلكترونية تعد إحدى صور الجريمة الالكترونية، لكنها تختلف عنها من حيث التعقيد والطبيعة، باعتبار أن القرصنة تتطلب أدوات وتقنيات متقدمة أكثر، فهي تركز على الاختراق غير القانوني للأنظمة المعلوماتية وسرقة البيانات والتلاعب بها، على عكس الجريمة الإلكترونية في شكلها العام التي قد تشمل أفعالا متنوعة مثل الاحتيال والتشهير

وعليه تم تقسيم هذا الباب إلى فصلين، حيث تم التطرق في الفصل الأول إلى الإطار المفاهيمي لجريمة القرصنة الإلكترونية، وفي الفصل الثاني إلى الطبيعة والتكييف القانوني للجريمة وكذا المسؤولية والعقوبات المترتبة عليها.

الفصل الأول

الإطار المفاهيمي للقرصنة الإلكترونية

نظرا لزيادة احتياج الأفراد لاستعمال الحاسب الآلي وشبكة المعلومات التي أصبحت جزءا لا يتجزأ من حياة الأفراد والمؤسسات على حد سواء، خاصة في ظل التطور السريع جدا للتكنولوجيا ، وانتشار استخدامها في مختلف المجالات لما توفره من وسائل وإمكانيات هائلة لمعالجة المعلومات وتخزينها وتبادلها بسرعة وفاعلية، الأمر الذي أدى إلى ظهور سلوكيات جديدة متعلقة بالولوج إلى هذه الأنظمة أو التعامل معها بطرق مختلفة، منها ما هو تقني أو تجريبي، ومنها ما هو مرتبط بأهداف غير مشروعة ومن أبرز هاته السلوكيات ما يعرف بالقرصنة الإلكترونية التي هي عمليات تهدف إلى الوصول إلى الأنظمة المعلوماتية المخزنة فيها بطرق غير مصرح بها ، غير أن طبيعة هذه الظاهرة متعددة الأبعاد، كونها تشمل أشكالا مختلفة من الاختراق أو التسلل بحسب الوسائل المستعملة والغرض من وراءها[1].

إن ظهور عدد كبير من المواقع الإلكترونية التي توفر مختلف أنواع البرمجيات والتطبيقات الرقمية، سواء كانت برامج ترفيهية مثل الألعاب، أو أنظمة تشغيل، أو برامج خدمية متنوعة، أين تتاح هذه البرمجيات للمستخدمين بطرق متعددة، فتُعرض مجانًا أو بمقابل مالي يتم دفعه عبر وسائل الدفع الإلكتروني، كالبطاقات الائتمانية، الأمر الذي جعل عملية الحصول علي هذه البرمجيات أمرًا في غاية السهولة ولا يتطلب سوى خطوات بسيطة عبر الشبكة[2].غير أن هذا التطور التقني، رغم ما يحمله من مزايا في نشر المعرفة الرقمية وتسهيل الوصول إلى المنتجات المعلوماتية، أفرز في المقابل ظواهر سلبية من أخطرها القرصنة الإلكترونية للبرمجيات، التي تمثل اعتداءً على الأنظمة المعلوماتية وحقوق الملكية الفكرية وتلحق أضرارًا اقتصادية كبيرة بقطاع صناعة البرمجيات. فقد أسهم انتشار الاختراق والنسخ غير المشروع للبرامج عبر الإنترنت في تكبد الشركات المنتجة خسائر مالية معتبرة، كما انعكس ذلك على سوق العمل من خلال فقدان عدد كبير من الوظائف في هذا المجال، فضلاً عن تراجع العائدات الضريبية للدول نتيجة تداول هذه البرمجيات القانونية[3]

وفي المقابل، يحاول بعض القائمين على مواقع الإنترنت تبرير نشاطهم بدعوى إتاحة البرمجيات لعدد أكبر من المستخدمين، خاصة في ظل ارتفاع أسعار النسخ الأصلية، الأمر الذي يجعل اقتناءها صعبًا

[1] عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل للنشر والتوزيع، الأردن، عمان ،2005، ص 18-19

[2] طارق إبراهيم الدوسقي عطية، الأمن المعلوماتي النظام القانون للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية،2009، ص 12-13.

[3] طارق إبراهيم الدسوقي عطية، المرجع نفسه، ص 126-127.

بالنسبة لفئات واسعة من المستخدمين، ولا سيما الطلبة[1]، كما يتباهى بعض القراصنة بقدراتهم التقنية في تجاوز أنظمة حماية النسخ المدمجة في البرامج ونشرها عبر الشبكة، للتباهي بها فقط[2]. ومع تزايد الاعتماد على نظم المعلومات في مختلف المجالات الاقتصادية والإدارية، لم تعد هذه الأفعال مجرد اعتداءات بسيطة، بل أصبحت تمثل أحد صور الجرائم المعلوماتية التي قد تمس المصالح الاقتصادية والأمن المعلوماتي للدول[3].

ومن ثم، يقتضي الأمر الوقوف على الإطار المفاهيمي لهذه الظاهرة، من خلال تحديد مفهوم القرصنة الإلكترونية وبيان خصائصها وأشكالها المختلفة، وهو ما يشكل مدخلًا أساسيًا لفهم طبيعة هذه الجريمة وآليات مواجهتها في التشريعات الجنائية الحديثة.

وبناء على ذلك، فان تحديد طبيعة القرصنة الإلكترونية أو تصنيفها القانوني لا يتحدد إلا بعد فهم ماهيتها وخصائصها وعناصرها الأساسية التي تميزها عن غيرها من الأفعال المتعلقة بالأنظمة المعلوماتية، تمهيدا لمناقشة صورها القانونية وطرق التعامل معها وفقا للتشريع الجزائري من خلال الوقوف على أهم النصوص التنظيمية والتشريعية ذات الصلة، وعليه سيتم تقسيم هذا الفصل إلى مبحثين كالتالي:

المبحث الأول: مفهوم القرصنة الإلكترونية

المبحث الثاني: الطبيعة والتكييف القانوني للقرصنة الإلكترونية

المبحث الأول: مفهوم القرصنة الإلكترونية

أدت التطورات الحديثة في تكنولوجيا المعلومات والاتصالات إلى الخروج من عصر الحرب التقليدية التي تتميز بالقتال والصواريخ والدبّابات إلى حرب أكثر عصرنه وحداثة وتتمثل في الحرب الالكترونية، فأصبحت المعلومات المتداولة عبر جهاز الحاسوب من علامات العصر الحديث والتي لا يمكننا الاستغناء

[1] نسيسة فاطمة الزهراء، **الجريمة الإلكترونية وأثرها على الفرد والمجتمع**، دراسة سوسيولوجية، الفا للوثائق، الجزائر، 2020، ص 114.

[2] بشرى حسين الحمداني، **القرصنة الإلكترونية أسلحة الحرب الحديثة**، دار أسامة للنشر والتوزيع، عمان، الأردن، 2014، ص 19.

[3] عبد الله عبد الكريم عبد الله، **جرائم المعلومات والانترنت (الجرائم الإلكترونية) منشورات الحلبي الحقوقية**، بيروت، 2007، ص 7.

عليها نظرا لكونها تسهّل متطلبات الحياة، وتعمل على تطوير أساليب العصرنة في حفظ هاته المعلومات أو تخزينها ونقلها وتوفيرها.[1]

غير أن هذا الاعتماد المتزايد على الأنظمة المعلوماتية أحدث نوعا جديدا من الممارسات غير المشروعة وهي ما تُعرف بالقرصنة الالكترونية، بما تشمله من اختراقات للأنظمة الحاسبة أو تجسس الكتروني لأخطر المواقع بدءا من الدول المتقدمة كأمريكا وأوروبا ثم الدول العربية.

إن ظاهرة الاختراق للأجهزة الالكترونية أضحت منتشرة في فترة وجيزة مما يجعلها صعبة الاكتشاف عن منتسبيها الذين يمكنهم التنصت والتجسس وترقب خصوصيات أي شخص عن طريق استخدام فيروسات تصيب الجهاز الآلي.

يقصد بالقرصنة السيبيرانية مختلف الأفعال غير المشروعة التي تستهدف الأنظمة المعلوماتية أو المنتجات الرقمية، وذلك من خلال التحايل على نظم المعالجة الآلية للبيانات أو تجاوز التدابير التقنية المقررة لحمايتها، وتشمل هذه الأفعال جملة من الممارسات غير القانونية، مثل الدخول غير المصرح به إلى الأنظمة المعلوماتية، أو استغلال البرامج الحاسوبية بطرق مخالفة للقانون، أو نسخها أو إعادة إنتاجها أو توزيعها دون إذن من أصحاب الحقوق،[2] كما تمتد هذه الممارسات إلى استخدام البرمجيات المقرصنة، أو تعطيل وسائل الحماية التقنية المصممة لحماية البرامج والبيانات، أو تقليد المنتجات البرمجية ومحاكاتها بهدف الانتفاع بها دون الحصول على الترخيص أو التفويض القانوني اللازم.
وتؤدي هذه الأفعال في الغالب إلى المساس بحقوق الملكية الفكرية، والإضرار بالمصالح الاقتصادية للدول والمؤسسات والأفراد، فضلاً عما قد يترتب عليها من تهديد لأمن الأنظمة المعلوماتية وسلامة البيانات المتداولة عبر الفضاء الرقمي.

لذلك تُعد القرصنة السيبرانية من أخطر صور الاعتداء على البيئة الرقمية المعاصرة، لما تنطوي عليه من انتهاك لحقوق الاستغلال المشروع للبرمجيات والمنتجات الرقمية[3] .

---

[1] بشرى حسين الحمداني، **مرجع سابق**، ص 10.

[2] عبد الفتاح بيومي حجازي، **النظام القانوني لحماية الحكومة من جرائم الإنترنيت**، دار الفكر الجامعي، الإسكندرية، ص20.

[3] شريفة كلاع، **الأمن السيبيراني وأشكال التهديد**، تحديات عالمية، الفا للوثائق، قسنطينة، الجزائر، 2023، ص 117.

وعلى هذا الأساس كان لزاما أن نتطرق إلى مفهوم القرصنة الالكترونية والتمييز بينها وبين المصطلحات المشابهة، وهو ما نتناوله في هذا المبحث الذي من خلاله سعيت إلى تبيان المقصود من جريمة القرصنة الالكترونية، وعليه سوف يتم تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: مفهوم القرصنة الإلكترونية

تعتبر القرصنة الإلكترونية من المسائل الأكثر حداثة لارتباطها بالتطور التكنولوجي ومنه فان تحديد مفهومها يعتبر الخطوة الأولى للتعرف على هذه الجرائم المتصلة بالفضاء الرقمي، غير أن تحديد مفهومها غير موحد فهو يختلف حسب الفقهاء والتشريعات، إذ يختلف من فقه إلى أخر ومن نظام قانوني إلى أخر ويرجع سبب ذلك اختلاف التصورات حول طبيعة هذه الأفعال ونطاقها، فهناك اتجاه يرى مفهوم القرصنة الإلكترونية من الجانب الضيق ويعتبرها كل فعل يتمثل في الدخول غير المشروع إلى الأنظمة المعلوماتية أو اختراقها، بينما يتجه اتجاه أخر إلى توسيع نطاقها ليشمل مختلف الأفعال غير المشروعة المرتكبة بواسطة الحاسب الآلي أو عبر الشبكات المعلوماتية، كالاعتداء على المعطيات أو تعطيل الأنظمة أو الاستيلاء على المعلومات وقرصنة البرمجيات[1] وهذا الاختلاف في التعريفات يجعل مفهوم القرصنة الإلكترونية نسبيا يتحدد انطلاقا من الزاوية التي ينظر من خلالها الفقيه أو المشرع إلى هذه الظاهرة الإجرامية [2].

وقبل التطرق إلى تحديد مفهوم القرصنة الإلكترونية في مختلف التشريعات منها التشريع الجزائري الذي هو محل دراستنا كان لزاما التعرف على نشأة القرصنة الإلكترونية

الفرع الأول: تاريخ وتطور القرصنة الإلكترونية

إن القرصنة الالكترونية لم تكن وليدة اللّحظة فقد تطورت نشأتها عبر مراحل، فأصبحت فضاءً يستحوذ على اهتمام الشباب ومختلف الفئات العلمية والتعليمية، ومع ازدياد انتشار أساليب الاختراق الإلكتروني، تحول الفضاء الرقمي إلى ميدان للصراعات، إما عن طريق التجسس والاختراق أو التخريب أو التلاعب بقواعد البيانات أين تصل خطورتها في بعض الأحيان إلى تهديد الأمن القومي لبعض الدول[3]، ومنه يمكن تقسيم تاريخ نشأة القرصنة الإلكترونية إلى ثلاث مراحل ويمكن تلخيصها فيما يلي:

أولا: مرحلة النشأة من سنة 1971 إلى سنة 1989

[1] طارق إبراهيم الدوسقي عطية، **مرجع سابق**، ص 127.

[2] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص25.

[3] أشرف السعيد أحمد، **مرجع سابق**، ص 12.

عند بداية ظهور السمات الأولى والبوادر التقنية لجهاز الكومبيوتر من طرف شركة IBN، والتي أطلقت عليه اسم الكومبيوتر الشخصي، نظرا لصغر حجمه، كانت البداية الأولى لظهور ما يعرف ب"الهاكرز" ، دفعت الرغبة المُلحة لمعرفة طريقة عمل هذه الأجهزة وطريقة تخريبها بالعمل الحقيقي وبذل الجهود لاكتساب مهارات في جانب المعلوماتية حيث ظهرت مجموعة من الهاكر يعملون على تخريب أجهزة المؤسسات التجارية حتى أنها عرضت فيلم سنة 1983، بعنوان حرب الألعاب والذي سلط الضوء على عمل الهاكر وجاءت فيه رسالة تنبيه لخطورة النتائج التي قد تترتب عن أفعالهم[1]، كما ظهر في أواخر هذه المرحلة نوع آخر من المخترقين يُعرفون باسم الكراكرز، أين أسس " ليكس لوثر" سنة 1984 مجموعة من الهاكرز والهواة الذين يرتكبون جرائم القرصنة على أجهزة الآخرين، أطلق عليها اسم (LOD) تحت قيادة (MOD) والذي اعتبر أذكى الهاكرز في تلك الفترة. [2]وقد كان هدف مجموعة من الهاكرز والهواة الذين يقومون بالقرصنة العبث بأجهزة الغير، ثم ظهرت بنفس الفترة مجموعة أخرى أسسها "فيبر" تتنافس مع المجموعة الأولى.[3]

ثانيا: مرحلة الانتشار 1990 إلى 1994

وفي مطلع سنة 1990، بدأت المجموعتان بحرب كبيرة أًطلق عليها حرب الهاكرز العظمى، وكان فيها كل طرف يحاول اختراق أجهزة الآخر فيما استمرت الحرب بين الفريقين مدة الأربع سنوات لتنتهي بإلقاء القبض على "فيبر" ليظهر بعدها شخصيات أخرى في الرحلة التالية.[4]

كما تميزت هاته المرحلة بتوسع النشاط مع الشبكات الأولى وانتقاله إلى عمليات شبه منظمة، أين انتشرت الحواسيب الشخصية وتحول النشاط من فردي إلى شبه منظم، عن طريق تبادل المجموعات واستغلال الثغرات للحصول على معلومات أو تعطيل أنظمة.

ثالثا: مرحلة الاحتراف ما بعد1994

---

[1] أحمد حسين خميس، **الهاكرز، طرق الاختراق وأساليب الحماية**، المركز المصري لتبسيط العلوم، الإسكندرية، 2001، ص 07.

[2] عبد الصبور عبد القوي على المصري، **الجريمة الالكترونية**، دار العلوم، القاهرة، 2008، ص56.

[3] حاتم عبد الرحمان منصور الشحات، **الإجرام المعلوماتي**، دار النهضة العربية، القاهرة، 2002 ص 22.

[4] حسين طاهري، **جرائم القرصنة الإلكترونية**، دراسة تحليلية مقارنة مرفقة بالاجتهاد القضائي المقارن في مجال الجرائم المعلوماتية والقرصنة الالكترونية، دار الخلدونية، الجزائر، 2023، ص 14.

بدأت في هذه المرحلة عمليات القبض على أحد كبار الهاكرز في التاريخ المدعو "كيفن متينيك" ونقلت وكالات الأنباء في العالم خبر اعتقاله وكان الخبر سببا في تغيُّر وجهات النظر بحيث أصبح يظهر بصورة البطل ليعطي للمشاهد صورة واضحة عن الهاكر.[1]

وأعلنت في الآونة الأخيرة شركة «Google» أن نظام البريد الالكتروني الذي اعتمدته على موقعها على شبكة الانترنيت «Gmail» قد تعرض لعملية قرصنة لآلاف الحسابات في خدمة بريد " هوت مايل".

ومن أبرز القضايا في تاريخ القرصنة الالكترونية نجد قضية اختراق مجموعة " سيتي جروب" الأمريكية، والذي أسفر عن سرقة عشرات الملايين من الدولارات، وحسب ما أقره مكتب التحقيقات الفيديرالي «FBI»، فإن القراصنة كانوا على اتصال بعصابة روسية على الإنترنت وتم كشف الهجوم عن بنك سيتي التابع للمجموعة.[2]

من جانب آخر فإن التشريع الفرنسي والولايات المتحدة الأمريكية منذ بداية 1996 قد تنبها إلى جدِّية الآثار التي تحدثها القرصنة الالكترونية والخطورة التي يواجهها ضحايا الهاكرز، وفي هذا الصدد تم إصدار عدد من الأحكام التي تدين مرتكبيها، وقد جاءت القرارات القضائية استنادا للعديد من الأحكام والأسس القانونية منها: قواعد قانون العلامة التجارية وأحكامه أيضا قانون الملكية الفكرية والقواعد التي تتضمنها القوانين الخاصة التي سُنت بصورة خاصة للتصدي لهذه الظاهرة[3].

في ديسمبر 2006 اضطرت وكالة ناسا إلى حجب رسائل البريد الإلكتروني المرفقة بمرفقات قبل إطلاق المركبات الفضائية وذلك تحسبا لاحتمال تعرضها للاختراق وذكرت مجلة بيزنس ويك الأمريكية أن خطط إطلاق المركبات الفضائية الأمريكية الأخيرة قد سربت إلى مخترقين أجانب مجهولين وغير معروفين.

في عام 2007 تعرضت شبكات حاسوب الحكومة الأستونية لهجوم من نوع الحرمان من الخدمة نفذه مجهولون وذلك بعد جدل مع روسيا بشأن إزالة نصب تذكاري أسفر الهجوم عن تعطل بعض الخدمات الحكومية الإلكترونية والخدمة المصرفية عبر الأنترنت وفي نفس العام، تم اختراق حساب بريد إلكتروني

---

[1] أشرف السعيد أحمد، **القرصنة الإلكترونية**، مطابع الشرطة لنشر والتوزيع، **مصر**، **2013** ص15.

[2] إسماعيل محمود الرزاز، **الحماية القانونية من الهجمات والجرائم السيبيرانية**، مركز المحمود لتوزيع الكتب القانونية، مصر 2023، 25-26.

3 نسيمة سحواذ، **الجريمة الإلكترونية مشكلة عالمية**، مجلة الشرطة للمديرية العامة للأمن الوطني، العدد 129 ديسمبر 2015، ص 139.

غير سري لوزير الدفاع الأمريكي من قبل مجهولين ضمن سلسلة واسعة من الهجمات التي استهدفت شبكات حاسوب البنتاغون.

في أكتوبر 2009 تم اكتشاف فيروس ستكسنت "stuxet[1]" وهو برنامج خبيث يتمثل في دودة إلكترونية متقدمة صممت لتعطيل أنظمة التحكم الصناعية من إنتاج شركة سيمنز " (siemen ا) المستخدمة في إيران وأندونيسيا ودول أخرى أثار هذا الاكتشاف تكهنات حول كونه سلاحا إلكترونيا حكوميا استهدف به برنامج إيران النووي.

وفي عام 2010 قامت جماعة تسمي نفسها" بالجيش السيبراني الإيراني" Cyber Army Iranian بتعطيل خدمة البحث في محرك بايدو الصيني الشهير حيث جرى تحويل المستخدمين إلى رسالة سياسية ذات طابع إيراني وكانت هذه الجماعة نفسها قد استهدفت موقع تويتر عام 2009 واخترقته لنشر رسالة مشابهة.

وفي يناير 2011 أعلنت الحكومة الكندية على أنها تعرضت لهجوم إلكتروني واسع استهدف عدة مؤسسات من بينها وكالة البحث والتطوير الدفاعي الكندية وقد أجبرت هذه الهجمات كلا من وزارة الدفاع المالية ومجلس الخزانة الكندي على قطع اتصالهما بالإنترنت كإجراء وقائي[2].

وفي أكتوبر 2012 أعلنت شركة أمن المعلومات الروسية " كاسبيرسكي "عن اكتشاف هجوم إلكتروني عالمي أطلق عليه اسم " أكتوبر الأحمر" وأوضحت الشركة أن هذا الهجوم كان جاريا منذ عام 2007 على الأقل ويهدف إلى جمع معلومات حساسة من السفارات، شركات الأبحاث المؤسسات العسكرية شركات الطاقة وغيرها كما أشارت إلى أن أبرز أهدافه تركزت في دول أوروبا الشرقية، دول الاتحاد السوفياتي السابق، آسيا الوسطى، إضافة إلى بعض دول أوروبا الغربية وشمال أمريكا.

في أبريل 2013 تسببت مجموعة أنونيموس بهجوم إلكتروني على مواقع إسرائيلية دعما للأسرى والقضية الفلسطينية شملت القائمة مواقع البورصة الإسرائيلية وموقع مكتب رئيس الوزراء ووزارة الدفاع،

[1]Zetter, Kim .count down to Zero Day: Stuxnet and the launch of the World's First Digital Weapon .New York: Crown Publishing Group, 2014.

[2] خالد حسن أحمد لطفي، **جرائم الانترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني** دار الفكر الجامعي، الطبعة الأولى، الإسكندرية سنة 2018، ص69.

إضافة إلى موقع جهاز الأمن الرسمي لمكتب الإحصاء ووزارة التربية والتعليم، إلى جانب عشرات مواقع أخرى وآلاف الحسابات الإسرائيلية على فيسبوك وتويتر [1].

في يناير 2014 أقرت خدمة الاتصال المرئي سكايب بتعرضها لهجوم إلكتروني مؤكدة في الوقت نفسه أن بيانات المستخدمين لم تتأثر، فجاء هذا الاعتراف بعد يوم واحد من إعلان الجيش السوري الإلكتروني، الموالي للرئيس بشار الأسد، أنه تمكن من اختراق حسابات سكايب على منصات التواصل الاجتماعي، وفي أغسطس من نفس السنة اعترف مفتش من وحدة الجرائم الإلكترونية الأمريكية بأن قراصنة أجانب تمكنوا خلال السنوات الثلاث السابقة من اختراق حواسيب تابعة للهيئة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل.

اختراق حسابات 500 مليون مستخدم لشركة "Yahoo" في سبتمبر 2016 أعلنت شركة Yahoo أن بيانات مالا يقل عن 500 مليون حساب مستخدم قد تعرضت للاختراق، في حادثة وصفت بأنها واحدة من أكبر عمليات القرصنة الإلكترونية في التاريخ[2]، وأوضحت الشركة في بيانها أنها تعتقد بأن الهجوم كان مدعوما من قبل إحدى الدول، ما يشير إلى أن منفذيه عملوا الحساب حكومة معينة، كما أضافت أن عملية الاختراق تعود إلى أواخر عام 2014.

تبين من خلال المراحل الثلاث لنشأة القرصنة الإلكترونية وتطورها بدءا من محاولات فردية بسيطة إلى هجمات منظمة ومعقدة أين شهدت مع انتشار شبكة الإنترنيت على نطاق أوسع تصاعدا في حجم ونوع الهجمات فلم تعد تقتصر على الفضول التقني أو التجارب الفردية، و إنما اتخذت أشكالا أكثر تنظيما مثل اختراق الأنظمة الإلكترونية وسرقة البيانات وتعطيلها، أين ظهرت مجموعات متخصصة في هذا المجال تدير هذه العمليات وتتقن كيفية استغلال الثغرات التقنية للوصول إلى أهدافها المنشودة ، قد تكون مادية اقتصادية أو سياسية أو حتى إجرامية، و لم يكتفي المخترقون بهذا القدر من السلوكيات السيئة بل مع تطور وسائل الاختراق بسبب التقدم السريع في التقنيات الرقمية وانتشار الهواتف الذكية والخدمات الإلكترونية، أصبحت القرصنة الإلكترونية تشكل تهديدا حقيقيا على الأمن القومي والاقتصادي، وهو ما جعل العديد من

---

[1] عبد الكريم بلعزوق، "**دراسة في ماهية الإجرام الإلكتروني ومجرم الإنترنت**"، مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريرج، الموسوم بعنوان، الإجرام السيبراني المفاهيم والتحديات، 11، 12أفريل 2017 ص 4.

[2] خالد حسن أحمد لطفي، **مرجع سابق**، ص70.

الدول تسعى إلى تعزيز منظومة الأمن السيبراني وسن تشريعات قانونية خاصة لمكافحة الجريمة وهو ما جعل دراسة تاريخها وتحليل مراحلها أمرا ضروريا لفهم التهديدات المستقبلية وإعداد استراتيجيات الحماية [1].

الفرع الثاني: تعريف القرصنة الالكترونية

القرصنة الإلكترونية أو ما يعرف باللغة الإنجليزية (Hacking) الدخول إلى الأنظمة المعلوماتية بطريقة غير شرعية وغير مرخص بها للقيام بأفعال غير مشروعة مثل التجسس والسرقة أو التخريب أو التدمير ....الخ عن طريق إضافة أو إنقاص أو نسخ أو مسح أو إضافة ، نظرا لاختلاف مفهوم القرصنة الإلكترونية سابقا أين كانت تجسد صفة المستخدم العبقري وتبين قدرته على الابتكار على عكس عملية القرصنة اليوم التي أصبحت في غاية التعقيد والصعوبة، وهذا راجع إلى التطور السريع الذي شهدته تكنولوجيا المعلومات، وعلى هذا الأساس فان القرصنة الإلكترونية هي في الواقع امتداد بمفهوم القرصنة التقليدية ، إلا أنها تختلف عنها في الوسائل والبيئة التي ترتكب فيها، كونها تنتقل من المجال المادي إلى المجال الافتراضي الذي يتميز بالسرعة والسهولة في ارتكاب تلك الأفعال [2]،

ومن هذا المنطلق فإننا نتطرق إلى تحديد مفهوم للقرصنة الإلكترونية من خلال هذا الفرع.

أولا: التعريف اللغوي والفقهي للقرصنة الإلكترونية

القرصنة بشكل عام هو القدرة على الوصول لهدف معين والدخول على الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصيات الآخرين وإلحاق الضرر بهم[3]. فغالبا ما تتم عملية الاختراق من خلال استغلال الثغرات الموجودة في النظام، والتي تكون في كثير من الأحيان في المنافذ الخاصة بالجهاز أين يمكن تشبيهها ببوابات مفتوحة على شبكة الإنترنت، تتيح للمخترق أو القرصان إمكانية التسلل إلى النظام والدخول إليه بطريقة غير شرعية[4].

ويطلق على الفاعل في هذا المجال عدة تسميات تختلف باختلاف طبيعة الفعل المرتكب، من أهم المصطلحات المتداولة "المخترق" و "الكراكر" إذ تستخدم للدلالة على الشخص الذي لا يكتفي بمجرد الولوج

[1] NathanW.Fisk: Digital piracy, New York, NY: Chelsea house, c2011, p 32.

[2] أشرف السعيد أحمد، **مرجع سابق**، ص 12

[3] بشرى حسين الحمداني، **مرجع سابق**، ص 13

[4] محمد أمين الشهاوي، **الجرائم المعلوماتية**، دار النهضة العربية، القاهرة، 2010، ص 41.

غير المشروع إلى الأنظمة، بل يتعداه إلى إحداث أضرار بها، كحذف الملفات أو نشر البرمجيات الخبيثة مثل الفيروسات وأحصنة طروادة أو زرع برامج تحسيسية[1]،

انطلاقا من ذلك، يقتضي الأمر بداية تحديد مفهوم "القرصنة الإلكترونية" باعتبارها مصطلحا مركبا، من خلال الوقوف على مدلوله اللغوي في كل من المعاجم العربية والمعاجم الأجنبية، تمهيدا لضبط معناه الاصطلاحي والقانوني للتطرق إلى التعريفات التي تثيرها القرصنة الإلكترونية.

أ: تعريف القرصنة الإلكترونية في المعاجم العربية

يرجع أصل مصطلح القرصنة إلى كلمة قرصان البحر وظاهرة قراصنة البحر الذين كانوا منذ العصور القديمة، يقومون بعملية السطو في وسط البحر، بغرض الاستلاء على السفن والبضائع بالقوة، إلى أن تطور استعمال هذا المصطلح عبر مرور الزمن فأصبح يطلق على كل فعل استيلاء غير مشروع على ممتلكات الغير، كما جاء في تعريف معجم اللغة العربية المعاصر[2]، وفق التصريف الآتي "قرصنَ، يُقرصن، قرصنةً، أي قام بأعمال سلب بحري وتحويل اتجاه السفينة لغرض تحقيق أهداف إما اقتصادية أو سياسية، ثم امتد استعمال المصطلح في العصر الحديث ليشمل مجالات تخرج عن إطار البحر، وخاصة في ميدان التكنولوجيا والمعلومات، حيث أصبح يدل على الاستغلال غير المشروع للمصنفات الفكرية أو البرامج المعلوماتية أو الأعمال الأدبية والفنية، و قرصنة حقوق المؤلفين التي تتطلب ترخيص من أصحابها.[3]

ب: تعريف القرصنة في القواميس الأجنبية:

جاء في تعريف قاموس أكسفورد " oxford" البريطاني " Oxford Advanced Learner's Dictionary مصطلح القرصنة :**(Piracy)** بأنه القيام بمهاجمة السفن في البحار وسلبها بالقوة، كما أن هذا المصطلح يستخدم في العصر الحديث للدلالة على قيام القرصان بنسخ أعمال الآخرين وبيعها بدون ترخيص منهم[4]، كما أن البعض من القواميس الفرنسية يُرجع مفهوم القرصنة إلى أنها مشتقة من كلمة

---

[1] عبد الله سليمان، **شرح قانون العقوبات الجزائري**، القسم الخاص، ديوان المطبوعات الجامعية، الجزائر، 2012، ص 233.

[2] أحمد مختار عمر، **المعجم العربي المعاصر**، عالم الكتب، القاهرة مصر سنة 2004، ص 125: " لقرصان: هو الشخص الذي يقوم بالاستيلاء على أموال أو ممتلكات الغير بالقوة أو بطرق غير مشروعة، وقد استعمل المصطلح حديثا للدلالة على من يقوم باختراق الأنظمة المعلوماتية أو الاستيلاء على البيانات بوسائل غير قانونية".

[3] مصطفى الفؤاد، القرصنة وأمن البحر الأحمر، دار أمجد للنشر والتوزيع، الطبعة الأولى، عمّان، 2020، ص 22.

[4] محمد بن أبي بكر الرازي، "مختار الصحاح"، **المكتبة العصرية**، بيروت ،2018، ص251

Hors-la-loi، والتي تعني الخارج عن القانون أي كل من يقوم بحملة بحرية مسلحة دون رخصة معتمدة من حكومة معينة، يظهر من خلال القاموس الفرنسي

(le Petit la rousse) القرصنة **(Piraterie)** ويقصد بها أعمال السلب والنهب التي يرتكبها القراصنة في البحار ضد السفن التجارية، كما يستعل هذا المصطلح كذلك للدلالة على النسخ غير المشروع للأعمال الفكرية أو الفنية المحمية قانونا [1].

فيظهر جليا من هذا المنطق أن القرصنة في القواميس الأجنبية مثلها مثل القواميس العربية قد تطورت من مفهومها التقليدي إلى مفهومها الواسع أين حددت مفهوم القرصنة في أعمال الاعتداء والسلب، إثم توسع استعمالها ليشمل مجالات أخرى من بينها القرصنة الإلكترونية.

ج: التعريف الفقهي للقرصنة الإلكترونية

في هذا الإطار، يلاحظ أن الفقه لم يستقر على مصطلح موحد لوصف الاعتداءات التي تستهدف النظام الآلي لمعالجة المعطيات، فتختلف التسميات باختلاف الزوايا التي نظر من جهتها إلى هذه الجرائم تبعا لاختلاف الترجمة المعتمدة للمصطلح الأجنبي، حيث ينظر من خلالها إلى هذه الظاهرة، فبين من استعمل مصطلحي جرائم الكمبيوتر أو الحاسب الآلي رأى أخر حتمية استعمال تعابير أكثر شمولية وأكثر توسع، محاولة منه استيعاب صور متعددة من الأفعال الإجرامية أين نجد مصطلح قرصنة أو قرصان أو اخترق أو تسلل وهذا التوسع في مصطلح القرصنة الإلكترونية من معناه اللغوي التقليدي الضيق إلى معناه الحديث الواسع ليشمل الجانب القانوني أيضا فيركز على الأفعال غير المشروعة الموجهة ضد الأنظمة المعلوماتية والبيانات الرقمية، وبذلك يكون الانتقال من المفهوم اللغوي إلى المفهوم القانوني خطوة ضرورية لفهم القرصنة الإلكترونية ، إذ يركز القانون على تحديد الأفعال المجرمة ومسؤولية مرتكبيها وعقوباتها[2] .

كما يتجه بعض الفقهاء إلى اعتبار أن الجريمة الإلكترونية تتحقق أساسا عند المساس بالكيان المنطقي للمعلوماتية أي بالبرمجيات والمعطيات، دون غيرها من المكونات المادية، فيعلل أصحاب هذا الاتجاه بأن العناصر المادية يمكن أن تخضع لأحكام القانون الجنائي التقليدي في حين أن خصوصية الجريمة

---

[1] Le petit la rousse Illustré, Dictionnaire de la langue française, la rousse, Paris, 2012,p804, mot « piraterie » .

[2] محمد حماد مرهج الهيتي، **الجريمة المعلوماتية دراسة مقارنة في التشريع الإماراتي السعودي والبحريني والقطري والعماني**، دار الكتب القانونية _ دار شتات للنشر والبرمجيات مصر _ الإمارات، ص 49-50.

الإلكترونية تبرر من خلال الاعتداء، إذ أن الاستلاء على شريط ممغنط أو قرص أو حتى على الحاسوب ذاته، لا يندرج ضمن نطاق الجريمة الإلكترونية فهو يعد سرقة عادية وليس جريمة إلكترونية أما إذا قام باختراق النظام أو تعديل البيانات فهنا تتحقق الجريمة الإلكترونية [1]إلا أن هذا الرأي ينتقد باعتبار أن التجريم يهدف إلى توفير الحماية الكاملة للنظام المعلوماتي بمكوناته المادية والمنطقية وحتى ما ينتجه من بيانات أو معلومات[2].

إن تعدد التعاريف واختلافها يعود بالأساس إلى تباين وجهات النظر لفقهاء القانون الجنائي في التشريعات المقارنة بشأن الوصف أو التسمية القانونية لهذه الجريمة فلم يضع المشرع، في غالب التشريعات المقارنة تعريفا جامعا مانعا لمفهوم القرصنة الإلكترونية، وانما اتجه الى تجريم الأفعال المادية التي تشكل صورا للاعتداء على الأنظمة المعلوماتية أو البيانات، بحسب طبيعة السلوك المرتكب، ومن ثم فان تحديد مفهوم القرصنة الالكترونية ظل الى حد كبير مجالا للاجتهاد الفقهي، الأمر الذي أدى الى تعدد التعارف واختلاف المصطلحات للمستعملة للدلالة عليها[3].

1: المفهوم الاصطلاحي للقرصنة الإلكترونية في التشريعات المقارنة

تناولت التشريعات المقارنة القرصنة الإلكترونية ضمن الأفعال الإجرامية المرتبطة بالاعتداء على الأنظمة والمعطيات المعلوماتية، وإن اختلفت في أسلوب تنظيمها وتحديد الأفعال المجرّمة. كما أسهمت اتفاقية بودابست بشأن الجريمة المعلوماتية في وضع إطار قانوني لمواجهة عدد من الأفعال المرتكبة ضد الأنظمة والمعطيات المعلوماتية، لاسيما الدخول غير المشروع إلى النظام المعلوماتي والاعتداء على سلامة المعطيات والأنظمة.

ولا تتجه أغلب التشريعات المقارنة إلى وضع تعريف اصطلاحي مستقل للقرصنة الإلكترونية،وإنما تحدد الأفعال التي تندرج ضمنها من خلال تجريم صور السلوك المرتبط بالدخول أو البقاء غير المشروع في الأنظمة المعلوماتية، أو الوصول إلى المعطيات دون ترخيص، أو الاعتداء على سلامة الأنظمة

[1] عبد الفتاح بيومي حجازي، **(دراسة قانونية مقارنة)**، دارا لفكر الجامعي، الإسكندرية، مصر،2005 ص 46.

[2] Michel Vivan , Cybercriminalité et droit pénal Presses Universitaires de France, Paris, 2001,p 37

[3] عماد محمد سلامة، مرجع سابق ،2005، ص 161

والمعطيات. ومن ثم، يمكن الوقوف على مفهوم القرصنة الإلكترونية من خلال الأفعال التي أسبغ عليها المشرّع صفة التجريم، بدلًا من البحث عن تعريف تشريعي موحد لها.

وفي هذا السياق، عُبّر عن القرصنة الإلكترونية في بعض الأدبيات والتعريفات الصادرة عن الهيئات والمنظمات المتخصصة بأنها تقوم على الوصول إلى أنظمة أو أهداف معلوماتية بطرق غير مشروعة، غالبًا من خلال استغلال الثغرات الموجودة في وسائل الحماية التقنية. ويكشف هذا التصور عن الجانب التقني للقرصنة، في حين يتولى التشريع تحديد صور السلوك التي تستوجب التجريم والعقاب[1].

وعليه، فإن دراسة موقف التشريعات المقارنة من القرصنة الإلكترونية تقتضي بيان الكيفية التي عالجت بها كل منظومة قانونية الأفعال المكوّنة لها، من خلال النصوص المتعلقة بالدخول غير المشروع إلى الأنظمة المعلوماتية والاعتداء على المعطيات والأنظمة، مع إبراز أوجه الاتفاق والاختلاف بينها.

كما عرفها الفقه الفرنسي على أنها الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح، ففي الغالب ترتكب الجريمة الإلكترونية ليس بغرض تحقيق الربح وإنما بواقع الانتقام والسخرية من المنافسين إلى غير ذلك[2].

ومنه فان القرصنة الالكترونية كما يطلق عليها Hacking وعلى المخترق مصطلح Hacker تعرف على أنها " عملية السطو والاحتجاز غير المشروع، وهي قيام شخص أو عدة أشخاص متمكنين في اختراق برامج الحاسوب بالتحكم في كيفية توصيتها وإدارتها، أين يشترط فيهم الذكاء والمستوى العالي حتى يتمكنوا من الولوج إلى الحاسوب والسطو على البيانات ومنه الانتقال إلى أجهزة مرتبطة به.

ويعرف البعض القرصنة الالكترونية على أنها: «اختراق لأجهزة الحاسوب أو المواقع تتم عبر شبكة الانترنت" غالبا ذلك يرجع إلى أن نسبة كبيرة منها مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية يمكن أن يرتبط بها أكثر من حاسوب، ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين من اختراق برامج الحاسوب وطرق إدارتها أي أنهم مبرمجون ذوي مستوى من الخبرة يستطيعون اختراق حاسوب معين

[1] عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، رسالة قدم ت استكمالا للحصول على الماجستير في القانون العام، جامعة الشرق الأوسط، الأردن 2014، ص12.

[2] حسين طاهري، **الجرائم الإلكترونية**، دار النهضة الخلدونية، الجزائر ،2022، ص 06.

للتعرف على محتوياته ومن خلالها تتم عملية الاختراق للتعرف على محتوياته كما يمكن أيضا اختراق باقي الأجهزة المرتبطة به في الشبكة ذاتها.[1]

ومن الناحية القانونية، تخول التشريعات وحتى الأعراف التجارية للمتضرر من عملية الاختراق، وهو صاحب المصنف الأصلي رفع دعوى أمام القضاء المدني لوقف الضرر الناتج عن الاستغلال غير مشروع باعتباره اعتداء على حقوق التأليف وحقوق المؤلف، بما يعكس أهمية ضبط القرصنة الإلكترونية في الإطار القانوني لحماية الملكة الفكرية.[2]

يوجد اختلاف حول مفهوم القرصنة الالكترونية بين علماء الإجرام فيعرفها بعضهم على أنها الاستيلاء على شيء مملوك للغير بطريقة احتيالية قصد تملكه. ليمتد هذا المصطلح ويشمل أشكالا متعددة من السلوكيات غير المشروعة، مثل السرقة والاحتيال والنصب ومنه الرابط المشترك لهذه الأفعال هو القدرة على الوصول لهدف معين باستخدام كل الطرق غير المشروعة تكون غالبا عبر استغلال ثغرات في نظام الحماية الخاص بالأنظمة المعلوماتية وإلحاق الضرر بالمتضررين[3]

2: المفهوم الجامع للقرصنة الإلكترونية (تعريف خبراء المعلوماتية)

قام كل من Alterman و Bloch مؤلفان لمقال فرنسي بعنوان الاحتيال المعلوماتي والغش المعلوماتي بإدراج تعريف منظمة التعاون الاقتصادي والتنمية الاقتصادية فادرج الغش المعلوماتي ضمن مفهوم الجريمة الإلكترونية، حيث نص التعريف على ما يلي:

تُعتبر جريمة معلوماتية كل سلوك غير مشروع، أو مخالف للأخلاق، أو غير مرخص به، يتعلق بالمعالجة الالية للبيانات أو بنقلها، ويقصد بها أي تصرف مخالف للقانون أو غير مرخص، أو لا ينسجم مع قواعد السلوك L'éthique وله صلة بالمعالجة الإلكترونية للبيانات أو تبادلها أو نقلها ، وتندرج القرصنة الإلكترونية ضمن هذا التعريف إذ تمثل نوعا محددا من الأفعال غير القانونية التي تخترق النظام الرقمي

[1] مريم بالطة، آسيا برغيت، **الأمن المعلوماتي في مواجهة القرصنة الالكترونية**، "مجلة السلام للعلوم الإنسانية والاجتماعية "30-10-2022، ص14.

[2] حسين طاهري، **جرائم القرصنة الالكترونية، مرجع سابق**، ص 60.

[3] فراس جمال شاكر، السبيرانية وتحولات القوة في النظام الدولي، دار أمجد للنشر والتوزيع، دار أمجد للنشر والتوزيع، عمان، 2022، ص 186.

مباشرة، مثل اختراق الأنظمة أو الشبكات أو سرقة أو تعديل البيانات ومنه يمكن القول أن القرصنة الإلكترونية هي شكل من أشكال الغش الإلكتروني إلا أن تركيزها يكمن في الوصول إلى الأنظمة التقنية[1].

لقد أدرج واضعو هذا المفهوم البعد المعنوي والأخلاقي ضمن تعريف الجريمة الإلكترونية غير أن الخبراء يرون أن هذا التوجه يفتقر إلى الطابع العملي، ويميلون بدلا من ذلك إلى المنهج الأنجلوسكسوني القائم على أسلوب الجرد حيث تعد قائمة محددة بالأفعال غير المشروعة التي تندرج ضمن نطاق الجريمة الإلكترونية، مثل اختراق الأنظمة، سرقة البيانات، أو تعديلها بدون ترخيص، فيكون هذا الأسلوب أكثر دقة ووضوح[2]

ومنه تعد القرصنة الإلكترونية من صور الاعتداء على أنظمة المعالجة الآلية للبيانات، وقد تشكل في الوقت ذاته وسيلة لارتكاب جرائم أخرى، متى استُعمل الدخول غير المشروع إلى النظام للوصول إلى بيانات أو أموال أو منافع غير مشروعة. ومثال ذلك أن يقوم شخص بالدخول غير المشروع إلى نظام معلوماتي تابع لمؤسسة مصرفية، ثم يستعمل ما مكنه منه هذا الدخول في تحويل أموال إلى حساب يسيطر عليه، فتكون القرصنة في هذه الحالة وسيلة لارتكاب اعتداء آخر على المال.

وانطلاقا من ذلك، تدخل المشرع الفرنسي لتوفير حماية جنائية لأنظمة المعالجة الآلية للبيانات، من خلال تجريم عدد من الأفعال التي من شأنها المساس بأمن هذه الأنظمة وسلامتها، وذلك ضمن الفصل الثالث المعنون بـ «الاعتداءات على أنظمة المعالجة الآلية للبيانات» من الباب الثاني من الكتاب الثالث[3] من قانون العقوبات الفرنسي، ولا سيما الأفعال المنصوص عليها في المواد 323-1 وما يليها

وفي هذا الإطار، نصت المادة 323-1 من قانون العقوبات الفرنسي، في صيغتها السابقة لتعديلها بموجب القانون رقم 2023-22 المؤرخ في 24 يناير 2023، على تجريم فعل الدخول أو البقاء بصورة احتيالية في كل أو جزء من نظام المعالجة الآلية للبيانات، حيث كانت تقرر عقوبة الحبس لمدة سنتين وغرامة قدرها 60.000 يورو[4]

[1] غنية باطلي، الجريمة الإلكترونية، دراسة مقارنة، الدار الجزائرية، الجزائري، 2015، ص 20.

[2] غنية باطلي، نفس المرجع ص 20-21.

[3] Code pénal français, Livre III, Titre II, Chapitre III, « Des atteintes aux systèmes de traitement automatisé de données », articles 323-1 à 323-8 Légifrance

[4] غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، الدار الجزائرية، الجزائري، 2015، ص 20.

كما كانت المادة ذاتها تشدد العقوبة عندما يترتب عن الدخول أو البقاء بصورة احتيالية حذف البيانات الموجودة داخل النظام أو تعديلها أو إحداث تغيير في طريقة عمله، إذ كانت العقوبة في هذه الحالة تصل إلى ثلاث سنوات حبسا وغرامة قدرها 100.000 يورو يتضح من تحليل هذه المادة

،وفي تحليل نص المادة في صيغتها السابقة، أن المشرع الفرنسي كان يميز بين صورتين للاعتداء على نظام المعالجة الآلية للبيانات؛ تتمثل الصورة الأولى في مجرد الدخول أو البقاء بصورة احتيالية في كل أو جزء من النظام، دون اشتراط تحقق نتيجة مادية لاحقة، في حين تتمثل الصورة الثانية في أن يترتب عن هذا الدخول أو البقاء حذف البيانات الموجودة داخل النظام أو تعديلها أو إحداث تغيير في طريقة عمله، وهو ما كان يؤدي إلى تشديد العقوبة[1].

وبذلك، لم تقتصر الحماية الجنائية المقررة بموجب المادة 323-1 على منع الدخول أو البقاء بصورة غير مشروعة في النظام المعلوماتي، وإنما امتدت كذلك إلى البيانات التي يحتوي عليها وإلى طريقة عمل النظام، إذ إن تحقق إحدى النتائج المتمثلة في حذف البيانات أو تعديلها أو إحداث تغيير في طريقة عمل النظام يؤدي إلى تشديد العقوبة[2].

ويستفاد من ذلك أن محل الحماية الجنائية في هذه المادة يتحدد أساسا في نظام المعالجة الآلية للبيانات باعتباره البيئة التقنية التي تتم فيها معالجة البيانات، مع امتداد الحماية إلى البيانات ووظائف النظام ويرى بعض الفقه أن المفهوم الأنسب لاستعمال مصطلح حماية النظام المعلوماتي لا يقتصر على العناصر المادية للحاسوب أو البرامج فقط بل يشمل أيضا المعلومات والبيانات المخزنة في ذاكرته وبصياغة أخرى يقصد بالمحتوى **Le contenu** النظام المعلوماتي ذاته، بينما تعد منتجات النظام تلك المعلومات التي يتم حفظها أو استخدامها لاحقا، إذن فإن حماية النظام في حد ذاته لا يثير أي إشكال قانوني أو صعوبة مرتبطة بحق الملكية أو قابليته للتملك ما دام ينظر إلى النظام باعتباره مجموعا واقعياfait universel

[1] Article 323-1 du Code pénal — rédaction en vigueur depuis le 26 janvier 2023

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

[2] نفس المرجع، ص 21

يتكون من عناصر أساسية تعد بمثابة وسائل أو أدوات مخصصة لمعالجة المعطيات وهي عبارة عن أموال مادية قابلة كأي منقول مادي للتملك(كمبيوتر وتوابعه)، أما البرامج فهي تعد نتاجا فكريا يحظى بالحماية وفقا لقانون حقوق المؤلف، ويكفي أن نعتبر أن اجتماع هذه العناصر المختلفة في إطار واحد متكامل هي نظام المعالجة الآلية للبيانات يجعل هذا الأخير قابلا لأن يكون محلا للتملك بوصفه مجموعا واقعيا[1].

أما بالنسبة للتشريعات الأمريكية والكندية فقد اتسم موقفها بشيء من الغموض أمام صعوبة هذه الإشكالية إذ تبنت تصورا مختلطا فهي لم تركز على حماية النظام المعلوماتي لذاته، بل اعتبرته وسيلة أساسية لضمان حماية منتجاته ومن ثم فإن قيام التجريم لديهما يفترض توافر الاعتداء في آن واحد على المنتجات وعلى النظام نفسه[2].

أدى هذا التوسع إلى اعتماد المصطلحات المتقاربة في بعض الكتابات، حيث أصبحت الجرائم لا تقتصر على النسخ المادي [3]، فاستخدام هذا المصطلح يسمح بالدلالة على صور متعددة من الاعتداءات غير المشروعة، إذ يشمل جرائم الحاسوب بمختلف صورها، إلى جانب ما يعرف أحيانا بالجرائم المعلوماتية أو الغش المعلوماتي أو الاعتداء على معطيات الحاسوب الآلي وجرائم الإنترنت، وهذا الاتساع في المفهوم يجمع تحت مظلته العديد من الأفعال الضارة بالأفراد والمجتمع، كسهولة استنساخ البيانات أو المعلومات الرقمية كالبرمجيات أو الموسيقى وأفلام الفيديو التي تعتبر قرصنة، إضافة إلى قرصنة مخلفات الملكية الفكرية كتزييف أعمال مؤلف ما والتصميم، والنموذج والعلامة التجارية ، وقرصنة الأعمال العلمية والأكاديمية التي تقوم على سرقة الأفكار بمجرد نسخ وثائق موجودة في الويب[4]، الأمر الذي يدفع المشرع إلى تعزيز الحماية الجنائية في هذا المجال حتى لا يتمكن المجرمون من التحايل وتحقيق أغراضهم غير المشروعة باستغلال ما يتيحه التقدم العلمي من إمكانات لم تكن متصورة عند وضع النصوص القانونية.

يفترض في المصطلحات القانونية أن تتسم بالمرونة والرؤية المستقبلية بحيث تراعي ما قد يطرأ من تطورات في ميدان الاعترافات والتقنيات الالكترونية فهل كان يخطر ببالنا أن تظهر أدوات إلكترونية متطورة كالتي نشهدها اليوم مثل الهواتف المحمولة التي تكاد تضاهي في قدراتها الحواسيب بما توفره من إمكانيات

---

[1] أمال قارة **الحماية الجزائية للمعلوماتية في التشريع الجزائري** دار هومة للنشر الجزائر، 2007، ص 21.

[2] غنية باطلي **مرجع سابق**، ص22-23.

[3] **المبادئ الأولية لحقوق المؤلف**، منشورات اليونيسكو، 1981، ص 62

[4] محمد علي محمد التوني، **استراتيجية مكافحة الهجمات السيبيرانية**، دار الفكر الجامعي، مصر ،2022، ص 246.

في الاتصال المحلى والدولي، وإرسال الرسائل النصية والبريد الالكتروني والصور والتعليقات، إضافة إلى إمكانية الوصول إلى شبكة الانترنت عبر هذه الأجهزة الصغيرة الحجم، فهل من المنطقي إخضاعها فقط لقوانين الاتصالات أو إساءة استخدام الهاتف مع ما تتمتع به من قدرات هائلة تجعلها في مرتبة قريبة من الحاسوب الآلي.

إلى جانب ذلك اعتمد مجلس أوروبا مصطلح الاتفاقية المتعلقة بالجريمة الالكترونية المعروفة باسم اتفاقية بودابست لعام 2001، والتي تلزم الدول الأعضاء باتخاذ التدابير اللازمة لردع جميع الأفعال الموجهة ضد سلامة وسرية وتوافر أنظمة الحاسوب والشبكات وبياناتها، وكذلك مواجهة مختلف صور إساءة استخدام تلك الأنظمة والشبكة والمعلومات[1].

من خلال نصوص هذه الاتفاقية يتبين أنها تتناول صورا متعددة من الأفعال غير المشروعة، مثل الدخول غير المصرح به إلى الأنظمة والتعامل غير المشروع مع بياناتها فضلا عن إساءة استخدام الأجهزة، وهي مسائل ستتناولها لاحقا بالتفصيل[2].

غير أن التعدد الاصطلاحي لا يعكس مجرد اختلاف لغوي أو ترجمي فحسب، بل يكشف عن إشكالية أعمق تتعلق بتحديد النطاق الحقيقي لهذه الجرائم، فهل يكفي أن يكون النظام الآلي محلا للاعتداء، سواء في جانبه المادي أو غير المادي، حتى تندرج الواقعة ضمن هذا النوع من الجرائم؟ أم أن الأمر يتطلب وجود عنصر معين، كالبيانات او المعطيات أو الوظيفة المعلوماتية للنظام، وهو الأمر الذي يجرنا إلى ضرورة التمييز بين الاعتداءات التي تمس الكيان المادي للجهاز وتلك التي تمس مكوناته غير المادية، على أساس أن هذا التحديد هو الذي سيسمح بضبط المفهوم القانوني الدقيق لهذه الجرائم[3].

وعلى الرغم من تعدد المصطلحات المستعملة في هذا المجال يبقى مصطلح الجريمة الإلكترونية الأدق تعبيرا ذلك أن البرامج والمعطيات سواء أثناء وجودها داخل النظام أو خلال معالجتها أو انتقالها، ليست سوى نبضات أو إشارات إلكترونية تترجم يتم تخزينها على وسائط معينة، ونقلها مع إعادة إنتاجها، وكون لهذه البيانات قيمة ملموسة، فإنها لا تعد من قبيل الأشياء المعنية مثل الحقوق الفكرية أو الآراء

---

[1] بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي الداخلي**، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر 01، الجزائر 2017-2018، ص28

[2] غنية باطلي، **مرجع سابق**، ص 24-25

[3] محمد حماد مرهج الهيتي، **مرجع سابق**، ص 50.

والأفكار بل تعتبر من الأشياء المادية والمحسوسة في العالم الخارجي يتم التعامل معها قانونيا كممتلكات. ، ويمكن القول باختصار أن القرصنة الالكترونية هي أي فعل إجرامي يستهدف أو يتعلق بالمعطيات المعالجة بلغة الآلة (معلومات أو برامج) أو بالنظام المعلوماتي ككل وتنفذ عادة باستخدام الحاسوب أو أي جهاز إلكتروني ذو إمكانيات مماثلة[1].

3: موقف الشريعة الإسلامية من القرصنة الإلكترونية.

تميز الإسلام بكونه دين الطمأنينة والاستقرار في شؤون الدنيا والآخرة، فيقوم على مبدأ صيانة الإنسان وحمايته من كل صور الاعتداء التي تمسه في دينه أو نفسه أو عقله أو ماله أو شرفه لهذا وضعت الشريعة الإسلامية جملة من الأحكام والسائل الكفيلة للمحافظة على هذه القيم ومنع انتهاكها [2]كما ذكرنا سابقا أن القرصنة الإلكترونية هي عملية اختراق أجهزة الحاسوب غير شبكة الإنترنت ومن مخاطر القرصنة الإلكترونية أنها تمكن المهاجمين من الدخول إلى الملفات الشخصية وسرقة المعلومات والبيانات ثم نشرها أو تحريفها، كما تقضي إلى تداول الأكاذيب والشائعات وتزوير الحقائق، وقد تنصب أفعال أو أقوال أو صور لأشخاص غير أصحابها ومن أخطر عواقب القرصنة هو التجسس على الأفراد وكشف أسرارهم وانتهاك أعراضهم وكشف عوراتهم وهو من أعظم الكبائر وأخطر الجرائم فقد نهى الله تعالى عن التجسس عموما فقال الله تعالى" **ولا تجسسوا**"[3].

أيضا ورد في حديث رسول الله صلى الله عليه وسلم" ولا تجسسوا، ولا تنافسوا، ولا تحاسدوا ولا تباغضوا ولا تدابروا وكونوا عباد الله إخوانا"[4]. فالقرصنة بهذا الشكل محرمة شرعا وتزداد خطورتها إذا خدمت أعداء الإسلام حتى تعادل في الإثم الحرابة لما تخلفه من فساد أمني واجتماعي وانتهاك الأعراض لذلك يجب معاقبة مرتكبيها بعقوبات رادعة يقرها ولي الأمر لما لها من أضرار كبيرة وخطيرة على المجتمع.

---

[1]أمال قارة، **مرجع سابق**، ص21.19

[2]خينش دليلة، **الجريمة الإلكترونية والأمن الاجتماعي**، ديوان المطبوعات الجامعية، الجزائر ،2023، ص 53

[3] سورة الحجرات الآية 12.

[4]مسلمين الحجاج أبو الحسين القشيري النيسابوري، صحيح مسلم، **كتاب البر والصلة والآداب، باب تحريم الظن والتجسس والتنافس والتناجي ونحوها**، دار إحياء التراث العربي، بيروت، بدون سنة، حديث رقم 2563، ج 4، 1986

وجريمة القرصنة على هذا النحو أضر وأخطر من الحرابة والله تعالى يقول:" إنما جزاء الذين يحاربون الله ورسوله ويسعون في الأرض فسادا أن يقتلوا أو يصلبوا أو تقطع أيديهم وأرجلهم من خلاف أو ينفوا من الأرض ذلك لهم جزي في الدنيا ولهم في الآخرة عذاب عظيم"[1].

"وتوعد الله سبحانه المستهزئين بأعراض المسلمين بالعذاب الشديد في الدنيا والآخرة، قال الله تعالى ﴿إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ ۚ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ﴾"[2].

ثانيا: مفهوم القرصنة الالكترونية في التشريع الجزائري

تعتبر الجزائر من بين الدول التي مسها التطور التكنولوجي في مجال المعلوماتية ومنه انتشار القرصنة الالكترونية، باعتبارها من المظاهر الإجرامية الحديثة نتيجة الاستخدام المتزايد لشبكة الإنترنيت، فهي في الأصل تمثل اعتداءً على أمن المعلمات، وقد نصت عليها المادة 394 مكرر من قانون العقوبات الجزائري التي يعتبرها مساسا بأنظمة المعالجة الآلية للمعطيات[3].

وفي هذا الإطار فإن درجة خطورة القرصنة لا تقل شأنا عن الدول الأخرى لاسيما في مجال التجارة الالكترونية التي أصبحت إحدى الركائز الأساسية للاقتصاد الرقمي في العصر الراهن، وأشارت احدى الدراسات الميدانية التي أجريت ما قبل 2014، أن القرصنة الالكترونية قليلة في الجزائر لكونها محصورة على فئة الشباب فقط ما جعل الدولة تسن القوانين المتعلقة بالإعلام والاتصال كخطوة أولى للحد من هذا النوع من الجرائم.

كما أن المشرع الجزائري لم يضع تعريفا صريحا لمصطلح القرصنة الإلكترونية، غير أنه عالج الأفعال المكونة لها من خلال تجريم مجموعة من السلوكيات التي ترتبط بالاعتداء على هذه أنظمة المعالجة الالية للمعطيات، وقد تدخل المشرع الجزائري مبكرا لتوفير حماية جنائية لأنظمة المعالجة الالية للمعطيات، وذلك بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، حيث أدرج ضمنه القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الالية للمعطيات"، متضمنا مجموعة من النصوص التي جرمت افعالا مختلفة

[1] سورة المائدة الآية 33.

[2] سورة النور الآية 19.

[3] الأمر رقم 66_156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم، المادة 394 مكرر

تمثل اعتداءًا على هذه الأنظمة أو على المعطيات التي تتضمنها، ورتبت عليها عقوبات جزائية بحسب طبيعة الفعل.

وقد واصل المشرع الجزائري تطوير التشريع المتعلق بالحماية الجنائية في هذا المجال من خلال التعديلات اللاحقة التي طرأت على قانون العقوبات، ولا سيما القانون رقم 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156[1].

الى جانب ارسائه اطارا تشريعيا خاصا بموجب القانون 09-04 المؤرخ في أوت2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها سعيا منه مواكبة التطورات التكنولوجية الحديثة ذلك بإرساء إطار قانوني يتلاءم مع خصوصية الجرائم المرتكبة في الفضاء الافتراضي، فتميز بجمعه بين أحكام إجرائية تدعم قواعد قانون الإجراءات الجزائية، وبين تدابير وقائية ترمي إلى التصدي المبكر للاعتداءات المحتمل وقوعها على الأنظمة المعلوماتية[2].

ويتضح من خلال استقراء هذه النصوص أن المشرع الجزائري قد اعتمد أسلوب التجريم غير المباشر للقرصنة الإلكترونية، وذلك من خلال تجريم الأفعال التي تشكلها، مثل الدخول غير المشروع أو غير المسموح له إلى النظام المعلوماتي، أو عرقلة سيره، أو حذف البيانات أو تغييرها، أو إدخال بيانات أو نقلها بطريقة غير مشروعة[3]،

ومنه يستخلص مما سبق أن القرصنة الرقمية في إطار التشريع الجزائري هي كل فعل غير مشروع يستهدف الأنظمة المعلوماتية أو البيانات الرقمية باستخدام الوسائل التقنية، ويؤدي إلى المساس بسرية المعلومات أو سلامتها أو توفرها، وهو ما دفع المشرع الجزائري إلى سن نصوص خاصة لمواجهة هذه الجرائم والحد من مخاطرها، كما يطلق على الشخص الذي يقوم بهذه الأفعال القرصان الإلكتروني، وهو الشخص أو مجموعة الأشخاص الذين يستغلون مهاراتهم التقنية لاختراق الأنظمة المعلوماتية بدون ترخيص صاحبها وبطريقة غير مشروعة.

---

[1] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، **الجريدة الرسمية للجمهورية الجزائرية**، العدد 77، سنة 2004، المعدل والمتمم لقانون العقوبات بالقانون 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156[1].

[2] حسين طايري، **الجرائم الإلكترونية**، مرجع سابق ص 6.

[3] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الالية للمعطيات، دار الخلدونية ،2018 ص32.

كما أن الدعوى الجزائية تناولها الفصل الثاني من الأمر 03_05 المتعلق بحقوق المؤلف والحقوق المجاورة[1] التي تعتبر أن التقليد التدليس والغش جنحة يعاقب عليها القانون، فسعى المشرع من خلال هذا التعديل إلى منع غير مصرح به للأعمال المحمية بحقوق المؤلف، بوصفه كل نسخ أو تقليد غير مرخص له يعتبر خرقا للقانون كما أنه يشكل في نفس الوقت انتهاكا للأعراف التجارية من خلال منافسة غير مشروعة، وتشمل الإجراءات القانونية حجز المواد والأدوات المستعملة في ارتكاب الانتهاكات، مع قيام جهات الضبط القضائي بعد الحصول على إذن من وكيل الجمهورية بتنفيذ إجراءات التحفظ والمعاينة وضعها تحت إشراف الديوان الوطني لحقوق المؤلف والحقوق المجاورة وبإشراف قاضي التحقيق .[2]

وعليه تتجلى أهمية هذه النصوص في أنها وفرت أساسا قانونيا لمتابعة مرتكبي أفعال القرصنة الإلكترونية أمام القضاء الجزائي، أين جاء مفهوما واسعا غير محدد في نوع معين من الأفعال المتعلقة بجرائم الحاسوب وشبكات الانترنيت[3] من أبرزها القرصنة الإلكترونية بحيث شكلت هاته التعديلات خطوة أساسية في تأمين البيئة الرقمية في الجزائر فربطت بين القواعد التقليدية للجرائم الإلكترونية وبين الإجراءات الوقائية الحديثة مما يعزز قدرة الدولة على مواجهة التحديات المتنامية للقرصنة الإلكترونية.

بالتالي فان إدراك ماهية الجريمة الإلكترونية والقرصنة الإلكترونية أمر ضروري لتحديد الطبيعة الموضوعية لهما، من خلال التطرق إلى الفرق بين الجريمتين من خلال استظهار خصائصهما ومخاطرهما حتى يتم التعامل مع كل جريمة على حسب نطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية وتحديد الأبعاد التي تمييزها عن غيرها من الجرائم ذات الصلة التي يكون سببها استعمال شبكات الإنترنيت[4]،

فما يمكن استنتاجه من خلال الطرح السابق فان كل قرصنة إلكترونية هي جريمة إلكترونية ، لكن ليست كل جريمة إلكترونية قرصنة، كون الجرائم الإلكترونية تشمل أفعالا كثيرة مثل الاحتيال الإلكتروني أو الابتزاز عبر الانترنيت ، سرقة البيانات الشخصية، نشر الفيروسات والبرمجيات الخبيثة انتحال الهوية عبر الانترنيت، اختراق الحسابات البنكية فهي بمفهومها الواسع كل جريمة ترتكب بواسطة التكنولوجيا أو ضدها تعد جريمة إلكترونية، على عكس القرصنة الإلكترونية يمكن تصورها في عمليات اختراق موقع إلكتروني،

---

[1] **الديوان الوطني لحقوق المؤلف والحقوق المجاورة**، القانون رقم 03-05 المؤرخ في 16 جويلية 2003، المتعلق بحقوق المؤلف الحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية، العدد40، سنة 2003.

[2] حسين طاهري، القرصنة الإلكترونية، مرجع سابق ص 60.

[3] مناصرة يوسف، **جرائم المساس بأنظمة المعالجة الالية للمعطيات**، مرجع سابق، ص03.

[4] عبد الله عبد الله، **مرجع سابق**، ص37.

الدخول إلى حساب شخصي بدون ترخيص، السيطرة على خوادم أو شبكات، كسر أنظمة الحماية للحصول على بيانات سرية على هذا الأساس فإننا نستنتج جليا الفرق الأساسي بين القرصنة الإلكترونية والجرائم الإلكترونية[1] .

وفي ذات السياق فان التطرق إلى التمييز بين القرصنة الإلكترونية والجريمة الالكترونية يدعو إلى التفرقة بين القرصنة وأنواع أخرى من الجريمة الإلكترونية نذكر من بينها القرصنة الإلكترونية والهجوم السيبيراني، والقرصنة الإلكترونية وسرقة البيانات من خلال الفروع التالية:

ثالثا: التمييز بين القرصنة الإلكترونية والجرائم الإلكترونية الأخرى

لم يجد الفقه والقانون تعريفا موحدا للجريمة الإلكترونية بسبب خشية الفقهاء ورجال القانون من حصرها في مجال ضيق، فتعتبر الجريمة الإلكترونية مجموعة من الأفعال والأنشطة التي تستخدم فيها التقنية الإلكترونية الرقمية بصفة مباشرة أو غير مباشرة لتنفيذ السلوك الإجرامي المقصود، فهي على وجه العموم مجموعة الجرائم المتصلة بعلم المعالجة المعلوماتية،[2]

أما القرصنة الإلكترونية فهي نوع محدد من الجرائم الإلكترونية يركز أساس على الدخول غير المشروع إلى الأنظمة أو الشبكات فيعرفها مختلف الفقهاء على أنها عملية اختراق أو إدخال INTRUSION'l أو دخول غير مصرح به إلى جهاز كمبيوتر أو نظام معلماتي بهدف الحصول على معلومات وسرقتها أو التلاعب بالبيانات أو تعطيل النظام، باعتبارها من الاعتداءات العمدية على المعطيات الموجودة داخل هذا النظام

ويقصد أيضا بفعل الإدخال أو الاختراق في مجال الاعتداء على أنظمة المعالجة الآلية للبيانات قيام الجاني بإضافة معطيات جديدة إلى النظام المعلوماتي أو إلى الدعامة الإلكترونية المخصصة لحفظ البيانات، سواء كانت هذه الدعامة خالية من البيانات أو كانت تحتوي مسبقا على معطيات أخرى، ويعتبر هذا السلوك من صور الاستعمال غير المشروع للأنظمة المعلوماتية المرتبطة غالبا بأفعال القرصنة الإلكترونية[3]، كما

---

[1] عبد الله عبد الكريم عبد الله، **مرجع سابق**، ص 22.

[2] سيد على السيد محمد، **الجرائم الإلكترونية، ماهيتها، صورها، إثباتها، مكافحتها**، دار التعليم العالي، الإسكندرية، 2023، ص 21.

[3] غنية بالطي، **مرجع سابق**، تناولت جريمة الدخول أو البقاء غير المشروع إلى نظام المعالجة الآلية للمعطيات بشيء من التفصيل، باعتبارها الجريمة الأساسية، وقد أولت مختلف التشريعات أهمية كبيرة، حيث تعتبر هي بداية الجرائم الأخرى،

يتحقق أيضا فعل الإدخال عند قيام الجاني بزرع برامج معلوماتية خبيثة داخل النظام المعلوماتي، مثل الفيروسات أو الديدان أو القنابل المنطقية أو غيرها من البرمجيات الضارة، والتي تؤدي إلى إضافة معطيات أو أوامر جديدة داخل النظام بهدف التلاعب بالبيانات أو الإخلال بوظائفه، كما يمكننا إعطاء مثال يتحقق من خلاله الفعل الإجرامي المتمثل في الاختراق غير شرعي لنظام معلوماتي من خلال قيام الحامل الشرعي لبطاقة السحب الممغنطة باستعمال بطاقته في أجهزة السحب الآلي للنقود مع إدخال الرقم السري الخاص به بحيث يكون الهدف وراء ذلك سحب مبالغ مالية تفوق الرصيد المتوفر في حسابه البنكي، ولا يقتصر هذا الفعل على الحامل الشرعي للبطاقة فقط وإنما يمكن أن يتسبب في ذلك الغير في حالة سرقة البطاقة أو ضياعها أو تزويرها فيتم استخدامها بطريقة غير مشروعة للوصول إلى النظام البنكي وإدخال بيانات وأوامر تؤدي إلى الحصول على عائدات مالية دون وجه حق[1].

أ: القرصنة الالكترونية وسرقة البيانات

لم تعد بيانات البرامج المعلوماتية مجرد أفكار ذهنية في عقل صاحبها، بل أضحت في صورة برامج أو بيانات رقمية يتم حفظها ومعالجتها وتداولها واستغلالها، فبمجرد انتقال الفكرة من نطاقها الذهني إلى شكل رقمي منظم داخل نظام معلوماتي، تكتسب صفة المعلومة القابلة للاستخدام الاقتصادي[2]، الأمر الذي منحها قيمة مادية و معنوية في أن احد، لهذا السبب اتجه الفقه القانوني إلى الاعتراف بالبيانات والبرامج المعلوماتية باعتبارها نوعا من الأموال المعنوية التي تستوجب حماية خاصة، ومن هذا المنطلق يتجسد مفهوم سرقة البيانات باعتبارها الاستيلاء غير المشروع على المعلومات أو البيانات المتواجدة في الشبكات الإلكترونية أو نسخها أو نقلها دون إذن صاحبها[3].

ترتبط هذه الجريمة بالقرصنة الإلكترونية، فيعتمد القراصنة على اختراق الأنظمة عبر شبكات الانترنيت للوصول إلى البيانات المستهدفة واستغلالها أو الاستفادة منها بطرق غير شرعية، وهي الأفعال المتعلقة بإدخال المعطيات أو إتلافها بقصد تضييعها ويكون الغرض منها هو إلحاق الأضرار بالآخرين[4]،بذلك يمكن

بمعنى أن الجرائم الأخرى ما هي إلا نتائج عليها، فاعتبرت أن جريمة الدخول والبقاء والتلاعب بالمعطيات أو الاعتداء على النظام أو التعامل غير المشروع في المعطيات كي ترتكب لابد من الدخول إلى النظام أو البقاء فيه.

[1] أمال قارة، **مرجع سابق**، ص 121.

[2] حنان ريحان مبارك المضحكي، مرجع سابق، ص 147

[3] حنان ريحان مبارك المضحكي، **نفس المرجع**، ص 155.

[4] عبد الله عبد الكريم عبد الله، **مرجع سابق**، ص 112.

القول أن سرقة البيانات تمثل أحد أهم صور الاعتداء على المعلومات، كما تمثل في الوقت ذاته نتيجة مباشرة لأفعال القرصنة الإلكترونية التي تستهدف الأنظمة المعلوماتية بقصد الوصول إلى ما تحتويه من بيانات وبرامج ذات قيمة بطريقة غير شرعية .

ب: القرصنة الالكترونية والهجوم السيبيراني

أثار ظهور الفضاء الرقمي مسألة مدى إمكانية إخضاع الأنشطة التي تتم عبره لضوابط قانونية تكفل تنظيمها وحماية المصالح المرتبطة بها، خاصة في ظل تعدد المتدخلين وصعوبة إخضاع هذا المجال لرقابة قانونية تقليدية. وقد ارتبط اتساع استخدام الأنظمة المعلوماتية والشبكات الرقمية بظهور اعتداءات تستهدف هذه الأنظمة وما تحتويه من بيانات، من بينها الهجمات السيبرانية. ويقصد بالهجوم السيبراني كل فعل عدائي يستخدم الوسائل المعلوماتية أو الشبكات الرقمية بهدف الدخول غير المشروع إلى نظام معلوماتي، أو تعطيله، أو السيطرة عليه، أو المساس بالبيانات التي يتضمنها، قصد إحداث أضرار مادية أو معنوية[1].

وقد أصبحت الهجمات السبيرانية في العصر الحديث من الوسائل الجديدة للصراع بين الدول أو الجماعات، إذ يمكن استخدامها لاستهداف مرافق عبر الفضاء الإلكتروني يؤدي إلى تعطيل الخدمات الأساسية وتهديد سلامة السكان[2]

من هذا المنطلق يظهر جليا الارتباط الوثيق بين القرصنة الإلكترونية وما يعرف بالهجمات السيبيرانية، حيث تمثل القرصنة في الغالب من الأحيان المرحلة التقنية التي يتم من خلالها تنفيذ الهجوم السيبيراني، اذ تقوم على أساس الدخول غير المشروع إلى الأنظمة المعلوماتية أو الشبكات الإلكترونية، بينما يتجاوز الهجوم السيبيراني ذلك ليشمل مختلف العمليات التي تقوم بتعطيل وتدمير الأجهزة الإلكترونية المسؤولة عن تنظيم الشبكات لذا تعتبر الهجمات طريقة ووسيلة قتالية في آن واحد، فهي تستخدم في تسهيل تنفيذ هجمات مسلحة تقليدية فيتم استخدامها لتعطيل شبكات الاتصال التابعة لها كما يتم استخدامها لتحديد المواقع الحساسة لدى العدو ليتم قصفها وتدميرها[3].

المطلب الثاني: خصائص جريمة القرصنة الالكترونية وأنواعها ودوافعها

[1] محمد علي محمد التوني، استراتيجية مكافحة الهجمات السيبيرانية، دار الفكر الجامعي، الاسكندرية،2023، ص 262.
[2] إسماعيل محمود الرزاز، **الهجمات والجرائم السيبيرانية**، مركز المحمود لتوزيع الكتب القانونية، 2023، ص 36.
[3] إسماعيل محمود الرزاز، **نفس المرجع**، ص37.

لقد أتاح انتشار الحاسوب والأنظمة المعلوماتية إلى إحداث تحولات عميقة إن لم نقل جذرية في حياة الإنسان، حيث أسهمت وسائل الاتصال في تسهيل وتحسين مستوى الخدمات والتواصل بين الأفراد، لكن هاته التغيرات خلقت أنماطا جديدة من السلوكيات السلبية وغير القانونية من بينها الاستيلاء غير المشروع على البيانات والمعلومات السرية المخزنة داخل قواعد البيانات، مما ولد تقنيات جديدة خلقت جرائم مستحدثة ووفرت وسائل جديدة لارتكاب الجريمة مثل عمليات الغش التلاعب بالمعلومات من خلال تعديل البيانات أو استبدالها داخل الأنظمة المعلوماتية[1]

يستخدم مصطلح القرصنة كثيرا هذه الأيام للتعبير عن العمليات غير المشروعة التي يقوم بها بعض القراصنة كما يشمل أيضا الاختراقات التي يقومون بها على الأنظمة المعلوماتية والهدف منها الاستيلاء على معلومات أو بيانات سرية أو زرع فيروسات في أنظمة الكمبيوتر[2] ، فبصفة عامة تنطبق القرصنة الإلكترونية على الأشخاص من ذوي المهارات المتخصصة في مجال أجهزة الحساب الآلي وعالم المعلوماتية، فيقصد بالهاكر مجموعة من المبرمجين الأذكياء الذين يقومون بتوحيد الأنظمة المختلفة ومحاولة اختراقها، فليس بالضرورة أن يكون ذلك بقصد ارتكاب جريمة ولكن هو نتيجة نجاح قدرات ومهارات المخترقين، إلا أن معظم القوانين اعتبرت أن المتسللين تمكنوا من الدخول إلى مكان خاص بأشخاص آخرين من اجل استغلاله في أعمال التخريب الإجرامية لمسح المعلومات، والبعض الأخر يتم استغلاله تجاريا لأغراض التجسس وسرقة بعض الأموال.[3]

يعتبر هذا النوع إلى حد الساعة هو الشائع من بين الجرائم المعلوماتية، لذلك توجد العديد من المؤشرات التي تبرز الطابع المتميز للقرصنة الإلكترونية وتدعم استقلالها عن غيرها من الجرائم، فتتميز القرصنة الرقمية بعدة مميزات بالنظر إلى الجرائم التقليدية، إذ يصعب غالبا اكتشافها من قبل أجهزة الرقابة والجهات الأمنية، نظرا لطبيعتها التقنية واعتمادها على الوسائل الإلكترونية، لذلك تعد من الجرائم الخفية التي قد تبقى

[1] حنان ريحان مبارك المضحكي، **مرجع سابق**، ص39

[2] فاروق علي الحفناوي، **قانون البرمجيات، دراسة معمقة في الأحكام القانونية لبرمجيات الكمبيوتر**، دار الكتاب الحديث القاهرة، 2001، ص 109

[3]Wiki pedia. Hacker Available ,at: https ://Britannica.com/topic/hacker ,generally a word Describing the S killed team of specialist skill in the file d of computer and information security, accessed: 10/06/2025.

لفترة طويلة دون أن يتم الكشف عنها، كما أن تقدير حجم الأضرار الناتجة عنها يطرح صعوبات كبيرة، خاصة عندما يتعلق الأمر بالبيانات أو المعلومات التي يمكن نسخها أو نقلها دون أن يظهر عليها أي أثر.

الفرع الأول: خصائص القرصنة الإلكترونية

تتميز القرصنة الالكترونية بالعديد من الدلائل التي تميزها عن باقي الجرائم المتعلقة بالأنظمة المعلوماتية، فتمثل جملة من الخصائص ندرجها لبيان أهم ما تتسم به هذه الأخيرة من خصائص باعتبارها أفعال تقنية معقدة يصعب اكتشافها، إلى جانب ذلك يتمتع مرتكبو هذه الجرائم بقدرة كبيرة على إخفاء أثار أفعالهم ومحو الأدلة الرقمية، مما يعرقل عملية الإثبات ويصعب مهمة التحقيق، كما أن هذه الجرائم تتسم بطابعها العابر للحدود، فهي لا ترتبط بمكان جغرافي محدد ولا تخضع لقيود الزمان والمكان،[1]

الأمر الذي يظهر ضرورة تمييزها عن باقي الأنماط الإجرامية، ويعود ذلك بالأساس إلى ما يتمتع به مرتكبها من قدرة فائقة على التخفي وإتلاف الأدلة، إضافة إلى خصوصية وسائل الإثبات المرتبطة بها، واستقلالية الجهات المختصة بالتحقيق فيها، فضلا عن تميز الوسائل المستخدمة في ارتكابها مقارنة بوسائل الجرائم التقليدية[2].

أولا: خصائص الجريمة

يقصد بخصائص القرصنة الإلكترونية مجموعة السمات التقنية والقانونية التي تميز هذه الجريمة عن غيرها من الجرائم التقليدية، سواء من حيث الوسيلة أو الأسلوب أو النطاق، فهي ذات طابع تقني تقوم أساسا على استخدام الحاسوب والشبكات المعلوماتية[3].

أ_ الحاسوب كأداة لارتكاب جريمة القرصنة الالكترونية

تتم عملية القرصنة الالكترونية بالاعتماد على جهاز الحاسب الآلي وهو ما يميز هذه الجريمة عن النوع الآخر من الجرائم التقليدية التي تتطلب استخدام أدوات العنف كما هو الحال في جرائم الإرهاب

[1] حنان ريحان مبارك المضحكي، **مرجع سابق**، ص39.

[2] محمد حماد مرهج الهيتي، **الجريمة المعلوماتية دراسة مقارنة في التشريع الإماراتي السعودي والبحريني والقطري والعماني**، **دار** الكتب القانونية _ دار شتات للنشر والبرمجيات مصر _ الإمارات ،2014، ص03.

[3] حنان ريحان مبارك المضحكي، **مرجع سابق**، ص39

والمخدرات، القتل، الجرح...، فهي جرائم تتصل بجهاز الكومبيوتر من خلال نقل معلومات وبيانات من جهاز لآخر، أو السطو الالكتروني على أرصدة البنك، [1]

يعد النظام الالكتروني محلا للجريمة ووسيلة لارتكابها في أن واحد، فقد ينصب الاعتداء على المكونات المادية للنظام، مثل الأجهزة والمعدات الإلكترونية، كما هو الحال في بعض جرائم السرقة أو التخريب التي تستهدف الحواسيب، وفي مقابل ذلك قد يوجه الاعتداء إلى المكونات غير المادية للنظام ، كالمعطيات أو البرامج من خلال أفعال المحو أو الإتلاف، أو التعديل غير المشروع ، كما قد يكون الحاسوب ذاته هدفا للاعتداء، كحالات الدخول غير المشروع إلى الأنظمة المعلوماتية أو زرع الفيروسات والبرمجيات الخبيثة، بغرض تدمير البيانات والملفات المخزنة أو العبث بها[2]، ولا يقتصر دور الحاسوب فقط على كونه محلا للاعتداء، بل يشكل كذلك وسطا ملائما لارتكاب الجريمة، إذ قد يستغل في تخزين البرامج المقرصنة أو المواد غير المشروعة، كما قد يستخدم كوسيلة لتسهيل بعض الأنشطة الإجرامية مثل ترويج المخدرات أ نشر الأفعال الإباحية وغيرها من الأنشطة غير القانونية ، ومن ثم يعد جهاز الحاسوب أداة أساسية في تنفيذ هذه الجرائم، حيث يستعمل لاختراق الشبكات المعلوماتية أو السيطرة عليها أو التلاعب بالأنظمة والبيانات المخزنة بها، بما يمكن الجاني من إحداث أضرار مختلفة، كالإتلاف التدمير أو غيرها من صور الاعتداء، نظرا لما يتضمنه من كم هائل من المعلومات والبيانات .

فيظهر جليا الدور الثنائي للحاسوب الذي يتمثل في أداة لتخزين المعلومات المقرصنة ولنشرها، ومن جهة أخرى كونه وسيلة يعتمد عليها المحققون في تتبع جرائم القرصنة المعلوماتية، وذلك من خلال تحليل الأنظمة والبيانات الرقمية للكشف عن الأدلة التي تدين الجناة وإحباط محاولات الاختراق أو الاعتداء على المنظومات المعلوماتية، والملاحظ هنا أن اعتماد القراصنة يكون على الحاسب الآلي كأداة للاختراق إلا أنها ليست الوسيلة الوحيدة التي يمكن استخدامها في القرصنة، فأيضا يعتبر الهاتف النقال وسيلة من الوسائل التي يلجأ إليها القراصنة لارتكاب الجريمة.

---

[1] كزيز صباح، سمير قط، **أثر الجرائم الالكترونية على أمن واستقرار الدول: قرصنة الموقع الالكتروني لوكالة الأنباء القطرية نموذجا**، مجلة الناقد للدراسات السياسية، بسكرة، الجزائر، 2018، ص 123.

[2] غانم مرضي الشمري، **الجرائم المعلوماتية (ماهيتها-خصائصها-كيفية التصدي لها قانونيا)**، دار الثقافة، عمان، الأردن، 2016، ص37.

وعلى هذا الأساس نتطرق لرأي الأستاذ عيسى سليم داوود الزيدي، مؤلف قانوني تناول موضوع القرصنة الالكترونية، الذي ذهب إلى القول بأن الجاني يمكنه الاعتماد في ارتكاب جريمته على الهاتف النقال أو الألواح الذكية وغيرها من الأجهزة الالكترونية فلا ينحصر الأمر على الحاسب الآلي لوحده خاصة في ظل التطورات التكنولوجية وتسابق الشركات في مجال صناعة البرمجيات والاهتمام الملحوظ للرقمنة وما يتعلق بها من وسائل وآليات، بحيث بدأ الاهتمام بالحاسوب الشخصي ومن ثم اللوح الرقمي وهذا لسهولة حملها ونقلها من مكان لآخر وأيضا يسهل إخفائها في حال احتوائها لأدلة تدين صاحبه[1].

ب_ القرصنة الالكترونية عملية معقدة وصعبة الاكتشاف

أهم ما يميز هذه الجريمة هو صعوبة اكتشافها، وذلك لعدة أسباب منها أن الضحية لا ينتبه أصلا لوقوع الجريمة عليه، كون الجاني يمتلك مهارات تقنية عالية، فينفذ الجريمة بكل دقة عن طريق إرسال فيروسات و سرقة المال المعلوماتي.[2]، وهو ما يجعل جريمة القرصنة الرقمية صعبة الإثبات بحيث ترجع صعوبتها إلى عدة أسباب منها ما يتعلق بطبيعة الوسائل المستعملة لارتكاب هذا النوع من الجريمة، فالقرصان الرقمي يتصف بالهدوء و اللاعنف، فهو لا يعتمد على استعمال السلاح في تنفيذ جريمته بل يعتمد في ذلك على برامج رقمية وأدوات إلكترونية لهذا سميت بالجريمة الناعمة، على عكس الجريمة التقليدية التي يتسم فيها الجاني بالعنف و استخدام السلاح لتحقيق أهداف إجرامية واختراق أجهزة وبيانات الغير.[3]

وعند تبادل المعلومات والأفكار والخبرات بين المجرمين يمكن لهؤلاء الاستفادة من ذلك وينحصر هذا عموما في المواقع الالكترونية التي تخص القراصنة.[4]

فمن صعوبات اكتشاف هذه الجريمة هي قيام القرصان بإخفاء هويته Encryptions وإخفاء المعلومات Sténographie مما يجعل الأمر صعبا أو مستحيلا، خاصة في وجود بعض البرامج المبرمجة خصيصا لإخفاء هذه المعلومات والبيانات.[5]

---

[1]حسين طاهري، **مرجع سابق**، ص 25-27.

[2]رحموني محمد، **خصائص الجريمة الإلكترونية ومجالات استخدامها**، مجلة الحقيقة، أدرار، الجزائر، المجلد17، العدد41، سنة 2018، ص441.

[3]مزوزي إكرام، الحاج بدر الدين، **مرجع سابق**، ص314.

[4] محمد عبيد الكعبي، **الجرائم الناشئة، عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية القاهرة، 2009، ص32.

[5]أمير فرج يوسف، **العالم ما وراء التقليد: الميتافيرس ومستقبل العالم الافتراضي وتطور الجريمة الرقمية والمعلوماتية الالكترونية**، دار النهضة العربية، القاهرة،2023، ص 202.

ج_ القرصنة الإلكترونية جريمة عابرة للحدود

إن الجريمة عبر الوطنية تعد جريمة منفردة الخصائص، لما يميزها باعتبارها عابرة للحدود فنجد أن الجريمة الإلكترونية لا سيما القرصنة الإلكترونية تتميز بطابعها العابر للحدود الوطنية، الأمر الذي يجعلها ضمن الجرائم ذات البعد الدولي، ذلك أنها ترتبط بإقليم جغرافي محدد، إذ قد يقع السلوك الإجرامي في دولة معينة بينما يوجد الجاني في دولة أخرى، في حين تتحقق النتيجة الإجرامية في دولة ثالثة،

وعليه فان فعل الاختراق أو الاعتداء على أنظمة المعالجة الآلية للمعلومات قد يتم بين أشخاص ليس من بلدان مختلفة و إنما من قارات مختلفة عن طريق الدردشة[1]، فيعود سبب هذا الامتداد الجغرافي إلى الطبيعة اللامادية لشبكات المعلومات، التي تجعل من انتقال البيانات عبر القارات والدول دون عوائق مادية أو حدود مرئية الأمر الذي جعل من العالم فضاءً رقمياً مفتوحاً، كما أطلق عليها البعض جريمة ذات الطبيعة متعدية الحدود.[2]

وأمام هذا الامتداد تبرز ضرورة تعزيز التعاون الدولي لمكافحة هذا النوع من الجرائم والحد من انتشارها، ففي ذات السياق تلعب منظمة الإنتربول دورا مهما من خلال التنسيق بين الدول وتبادل المعلومات، بالاعتماد على شبكات الاتصال وقواعد بيانات مشتركة تساعد في تعقب الجناة والتصدي لهذا النوع من الجرائم.

بالرغم من أن التقنية قد ساعدت المجتمعات على التواصل الحضاري والثقافي بين المجتمعات وتقريب المسافات بينها، إلا انه من ناحية أخرى أدى إلى بروز ظاهرة تسمى بعولمة الجريمة، ذات الطابع الدولي باعتبارها تحديا حقيقيا يهدد الأمن الوطني والدولي ، يعود ذلك إلى ما توفره هذه التقنيات من تسهيلات كبيرة مكنت الأفراد والجماعات الإجرامية المنظمة من توسيع نطاق أنشطتهم غير المشروعة، من خلال إيجاد فضاء ملائم لانتشار السلوك الإجرامي، وهو الأمر الذي يطرح عدة إشكالات قانونية، خاصة فيما يتعلق بتحديد الدولة المختصة قضائيا بنظر الدعوى، مقارنة بتعدد أماكن ارتكاب الفعل وتحقيق نتيجته،

[1] منير محمد الجنيهي، ممدوح محمد الجنيهي، **جرائم الإنترنيت والحاسب الآلي**، دار الفكر الجامعي، مصر، 2005، ص 15.

[2] حسين طاهري، **مرجع سابق**، ص 24.

كما يطرح صعوبات تتعلق بمدى فعالية القوانين الوطنية في مواجهتها، إضافة إلى إشكالية جمع الأدلة الرقمية وقبولها في ظل اختلاف الأنظمة القانونية بين الدول وتباين مواقفها بشأن حجية هذا النوع من الأدلة[1]

ثانيا: مميزات القرصان الإلكتروني

إذا كانت القرصنة الإلكترونية تتميز بمجموعة من الخصائص التقنية والقانونية، فإن مرتكبها بدوره يتسم بصفات خاصة تميزه عن غيره من المجرمين التقليدين.

أ. مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي

المجرم في جريمة القرصنة الإلكترونية له صفة مميزة من حيث الثقافة والعلم التكنولوجي[2]، فقد يكون شخصا عاديا يعمل بمفرده ويهدف إلى تحقيق المصلحة الشخصية له ولكن في الغالب ما يقوم بهذا الفعل لحساب الشخص المعنوي (كشركة عامة أو خاصة) وقد تكون الجهة العاملة في تكنولوجيا المعلومات أو تعتمد عليها لاقتحام نظام معلوماتي أو لإحداث ضرر بالآخرين، ويختلف المجرم في الجريمة الإلكترونية عن المجرم التقليدي بسبب السمات التي تميزه عن غيره وله أشكال وأنماط خاصة به كما أن الدوافع التي تقوده لارتكاب هذه الجريمة تختلف لديه أيضا كما وضحنا سابقا وتظهر الإحصائيات أن مرتكبي هذه الجرائم لا يستهدفون الأفراد عادة بل المؤسسات لأنها تستطيع تحمل الخسائر بفضل رصيدها المالي والاحتياطي، كما أن هذه الجرائم تمس بالأمن العام للبلاد[3].

إذ أن هذه الأضرار لا تقتصر على الأفراد بل تمتد لغيرهم ويرى خبراء الأمن السيبيراني أن المتورطين في هذه الجرائم لديهم قدر كبير من الذكاء والتفوق يجعلهم يباشرون إجرامهم بدقة متناهية خشية افتضاح أمرهم وضبطهم وهم في سن تساعدهم على المخاطرة والمغامرة. ولأن من يقترف هذه الجرائم يكون بين الاثني عشر والسادسة والأربعون وهو مثقفون ومتعلمون وأهل ثقة ممن يعتمدون على حقوقهم في غالب الأحيان[4].

يقال عادة أن الجريمة الإلكترونية هي جريمة يرتكبها متخصصون في مجال الحاسوب والتقنيات المعلوماتية، وغالبا ما يكون مرتكبيها من الأشخاص الذين يشغلون الإدارات أ أصحاب الخبرات التقنية

---

[1] عبد الله عبد الكريم عبد الله، **جرائم المعلوماتية والإنترنيت (الجرائم الإلكترونية)**، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص22.

[2] عبد الله عبد الكريم عبد الله، **نفس المرجع**، ص 23.

[3] طارق إبراهيم الدوسقي عطية، مرجع سابق، ص175

[4] D .B. Parker Combattre la criminalité informatique, édoros 1987, P138

العالية، فيطلق عليهم "المجرمون الأذكياء" بالمقارنة بالمجرم التقليدي الذي يميل إلى العنف المباشر، مع ذلك، يمكن أن تتخذ بعض الهجمات الإلكترونية طابعا عنيفا، إذ تستهدف الأنظمة المعلوماتية بشكل مباشر أو تسبب تلفا في الحاسوب والمعدات الالكترونية المتعلقة به[1].

ب_قدرته على التخفي وإخفاء الهوية

تعتمد معظم هذه الجرائم على أساليب غير مادية، حيث يتم التلاعب بالبيانات والبرمجيات داخل الأنظمة دون الحاجة إلى تدمير الأجهزة نفسها، فتشمل هذه الأساليب استخدام البرمجيات الخبيثة مثل الفيروسات قنوات اتصال غير مشروعة لإحداث أضرار على مستوى البيانات والكيانات المنطقية داخل النظام، بما يمكن أن يؤدي إلى تعجيل عمل النظام أو التلاعب بالمعلمات المخزنة فيه.

يتميز مرتكب الجريمة الإلكترونية بخصائص تختلف في كثير من الأحيان عن المجرم التقليدي، إذ يكون غالبا فردا مندمجا في مجتمعه، يعيش حياة عادية ويتكيف مع بيئته الاجتماعية بشكل طبيعي، إلا انه يتمتع بقدر عال من الذكاء والمعرفة التقنية، ففي هذا السياق لا يقتصر الذكاء على القدرة العقلية فقط وإنما يشمل أيضا القدرة على التكيف مع المحيط التقني، وإخفاء هويته غير أن هذا الأمر لا يقلل من خطورة المجرم الإلكتروني، بل قد يزيدها، لأن قدرته على التكيف الاجتماعي وامتلاكه مهارات تقنية متقدمة وميولا إجراميا، تجعله أكثر قدرة على استغلال الأنظمة المعلوماتية وارتكاب الأفعال غير المشرعة[2]

ج _ تنوع دوافعه

وفي بعض الأحيان قد يقوم بعض الأفراد باختراق الأنظمة المعلوماتية بدافع الفضول أو الرغبة في إثبات المهارة التقنية والتغلب على أنظمة الحماية المعلوماتية، دون أن هدفهم الأساسي إلحاق الضرر بالغير، على الأغلب يكن هؤلاء من فئة المتعلمين يدعون أن غايتهم تكمن في تحسين أمن الأنظمة المعلوماتية،[3]

وفي هذا الإطار، يمكن الإشارة إلى مثال عرض أمام القضاء الجنائي الألماني يتعلق بقاصر يبلغ من العمر 16 سنة[4]، نسب إليه الدخول غير مشروع إلى نظام (فيديوتاكس) التابع لنظام (بي تي اكس)،

---

[1] غنية باطلي، **مرجع سابق**، ص 34، 35

[2] خالد حسن أحمد لطفي، مرجع سابق، ص 80

[3] خالد حسن أحمد لطفي، نفس المرجع 81

[4] حسين طاهري، الجرائم الإلكترونية، دار الخلدونية، الطبعة الأولى، 2022، ص 34

حيث صرح بأنه كان مدفوعا برغبة قوية في اكتشاف عيب النظام إبراز قدرته التقنية، كما أوضح بأنه عثر بالصدفة على بعض الثغرات الأمنية، وقان بإبلاغ الجهة المختصة بها بهدف المساهمة في معالجتها، خاصة وان العديد من هذه الثغرات لم تكن معرفة من قبل ". ومع ذلك فان غياب القصد الإجرامي الصريح لا ينفي وجود خطر اجتماعي للجريمة الإلكترونية وأثارها السلبية، إذ قد يترتب عنها الإضرار بأمن الأنظمة المعلوماتية والمساس بسلامة البيانات المعلومات، الأمر الذي يبرز الطابع الاجتماعي والقانوني المعقد للقرصنة أو الجريمة الالكترونية على حد سواء.

وعليه فان السلوك الغير واعي قد يترتب عنه أضرار بالغة حتى وإن لم يكن موجها بعداء مباشر ضد المجتمع، ومن هذا المنطلق يتميز المجرم الإلكتروني تبعا للفئة أو النمط الذي ينتمي إليه.

ثالثا: أنماط المجرم الإلكتروني

تتعدد أنماط المجرم الإلكتروني تبعا لمعيار التصنيف المعتمد، فيتطلب ارتكابها توافر جملة من الشروط التقنية، على رأسها استخدام الحاسوب والاتصال بشبكة الإنترنت، إلى جانب شروط شخصية تتعلق بمرتكبها، كامتلاك قدرا من الكفاءة التقنية والخبرة العملية، فضلا عن الذكاء والقدرة على التحليل والتخفي، تتعدد أنماط المجرم الإلكتروني تبعا لمعيار التصنيف المعتمد، فقد يصنف وفقا لدوافعه إلى مجرم ذي دافع مادي أو سياسي أو شخصي، كما يمكن تصنيفه حسب مستوى مهارته إلى محترف أو متوسط أو مبتدئ.

أ- **أدوات القرصنة الإلكترونية:** يشترط في مرتكب الجريمة (المجرم الإلكتروني) توافر ثلاثة شروط أساسية على الأقل منها

1-حيازته لجهاز الحاسوب.

2- الاتصال بشبكة الإنترنت (جهاز مودام Modem، أو وسائل الاتصال)

3- قدرا من الكفاءة والحيلة والذكاء[1]

[1] غنية باطلي، **مرجع سابق**، ص36 -37 تطرقت غنية بالطي في كتابها الجريمة الالكترونية إلى المودم(Modem) الذي اعتبرته جهاز صغير يعمل على ترجمة تعليمات مكتبة بالغة الآلة إلى رموز رقمية(الآحاد والاصفار)والعكس، وتحويلها داخل الجهاز إلى ترددات وإشارات صوتية ويسمح للحاسبات الإلكترونية أن تستقبل للحاسبات الإلكترونية أن تستقبل وتنقل المعلومات عن طريق وسيط تلفوني

ب_ فئات المجرم الالكتروني:

حيث صنفهاM Perker عام 1976 بمعهد البحوث Stam ford Research Institute بدراسة تحليل 1000 حالة واستنتج 7 أصناف للمجرم الإلكتروني:

1_ الهواةLes hackers [1]

2_ المحترفون Les crackers[2]

3_ المخادعون Frondeurs

4_ لصوص نظم المعلومات أو قراصنة الهاتف PHreaking

5_ المتطرفون ذو المثل العليا

6 _العاملون في الجريمة المنظمة

7_ مخربي الأنظمة المعلوماتية

الفرع الثاني: أنواع القرصنة الإلكترونية

تتميز القرصنة الالكترونية بتعدد أنواعها فقد تتباين من حيث المدة التي تستغرقها، أو من حيث حجم ونطاق الهجوم، وبحسب الغاية المرجوة منها، ناهيك عن اختلاف درجة خطورتها والآثار المترتبة عنها، فهي لا تمثل سلوكا واحدا بسيطا ، بل هي ظاهرة متعددة الأبعاد يمكن تصنيفها وفق معايير مختلفة، فمن حيث المدة قد تكون وقتية سريعة لا تأخذ وقتا طويلا أو مستمرة فيتم ارتكابها عبر مراحل ، وهذا التنوع يعكس الطبيعة المعقدة لهذه الظاهرة مما يجعل من تناول أنواع القرصنة الإلكترونية وفق هذه المعايير يعد خطوة أساسية لفهم أبعداها المختلفة[3].

وعليه، يمكن تصنيف **أنواع القراصنة** وفقا للعناصر التالية

أولا: أنواع القراصنة من حيث المدة (الزمن)

[1] غنية باطلي، مرجع سابق، 37

[2] خينش دليلة، الجريمة الإلكترونية والأمن الاجتماعي، ص 42

[3] بشرى حسين الحمداني، مرجع سابق، ص 16

تتباين أنشطة القراصنة الإلكترونيين من حيث المدة الزمنية التي تستغرقها عمليات الاختراق، حيث تختلف باختلاف طبيعة الهدف المراد الوصول إليه، ومدى تعقيد الأنظمة المعلوماتية المستهدفة، فضلًا عن درجة احترافية القراصنة والوسائل التقنية المعتمدة. فقد تكون بعض الهجمات سريعة ومؤقتة، في حين تتطلب أخرى وقتًا طويلًا وتخطيطًا دقيقًا للبقاء داخل النظام دون اكتشاف[1].

إلى نوعين رئيسيين:

أ_القراصنة ذو الهجمات قصيرة المدى

وهم القراصنة الذين يعتمدون على عمليات اختراق سريعة ومباشرة، تهدف إلى تحقيق غاية آنية، كالدخول غير المشروع إلى نظام معلوماتي أو تعطيل موقع إلكتروني لفترة محدودة أو سرقة بيانات بشكل فوري. وغالبًا ما تعتمد هذه الفئة على استغلال ثغرات بسيطة أو استخدام أدوات جاهزة، دون الحاجة إلى تخطيط طويل أو بقاء مستمر داخل النظام المستهدف.

ب_ القراصنة ذوو الهجمات طويلة المدى

تتسم هذه الفئة من القراصنة بالاحترافية العالية، حيث تعتمد على التسلل التدريجي إلى الأنظمة المعلوماتية والبقاء فيها لفترات زمنية طويلة دون كشف، بهدف جمع أكبر قدر ممكن من المعلومات أو مراقبة الأنشطة الداخلية للنظام. وغالبًا ما تكون هذه الهجمات موجهة ضد مؤسسات كبرى أو جهات حكومية، وتتطلب تخطيطًا دقيقًا واستعمال تقنيات متطورة لضمان الاستمرارية والتخفي.

ويُبرز هذا التصنيف أهمية البعد الزمني في تقييم خطورة الهجمات الإلكترونية، إذ كلما طالت مدة الاختراق زادت احتمالية إلحاق أضرار جسيمة بالنظام المعلوماتي، سواء من حيث تسريب البيانات أو المساس بأمن المعلومات[2].

ثانيا: الأنواع من حيث الغاية

تختلف أشكال وأنواع القرصنة حسب الهدف والغاية نذكر منها:

[1] محمد صبري السعدي، **الجريمة المعلوماتية في التشريع الجزائري**، دار الهدى، الجزائر، 2019،ص 45.

[2] عبد الفتاح بيومي حجازي، **الجرائم المعلوماتية وحماية المعلومات**، دار الفكر الجامعي، الإسكندرية، 2018، ص 112.

أ-القرصنة الانتقامية: وهي التي تكون غالبا بين الدول على خلاف سياسي أو صراع معين، مثل ما وقع بين إيران وكوريا الشمالية[1]، أو بين بعض القراصنة المؤيدين للقضية الفلسطينية ضد المواقع الإسرائيلية وقد سجلت العديد من الهجومات الإلكترونية على مواقع إسرائيلية[2].

ب- القرصنة السياسية: يعتبر هذا النوع من أكثر أشكال القرصنة انتشارا على شبكة الأنترنت، حيث تشير الإحصائيات إلى أن حوالي 58 بالمئة من البيانات المسروقة يكون وراءها مجموعات تهدف إلى تحقيق أغراض سياسية، ومن أبرز هذه المجموعات(نونيموس) التي تمكنت من تنفيذ عدة هجمات ناجحة وذلك عبر السيطرة على مواقع سياسية مختلفة إضافة إلى سرقة كميات كبيرة من البيانات التابعة لشركات خاصة ومؤسسات حكومية حيث أكد العديد من الخبراء أن هذا النوع من القرصنة أصبح إحدى آليات الاحتجاج السياسي مشرين إلى أنه من الصعب إيجاد نظم دفاعية محددة ضد هذه الهجمات الإلكترونية لأن مجموعات القرصنة السياسية تستعمل وسائل وأساليب خاصة يتم ابتكارها لكل مناسبة بعينها[3].

ج-القرصنة الذاتية: هي نوع من القرصنة تقوم فيه بعض الدول بعمل هجمات على نفسها، ثم تعلن أمام العالم أن دولة أخرى هي التي قامت بهذا الهجوم يعني أن الدولة تقرصن نفسها حتى تتهم غيرها وتظهر في صورة الضحية والهدف من هذا النوع هو من القرصنة وهو تضليل الرأي العام وخلق حالة من الفوضى بين الدول، مثال على ذلك هو ما نشاهده أحيانا من اتهامات إمبريالية او بعض الدول العربية لروسيا بأنها تتدخل في الانتخابات وتأثر على نتائجها.

د-قرصنة الهواة: وتعرف أيضا بقرصنة الفضائح وفيها يقوم بعض القراصنة باختراق المواقع الشخصية أو الحسابات بهدف الحصول على معلومات خاصة أو صور أو محادثات شخصية ثم يقومون بنشرها علنا وفي بعض الأحيان يبتزون أصحابها مطالبين بمبالغ مالية مقابل عدم نشرها[4].

---

[1] حسين طاهري، مرجع سابق، ص 34.

[2] بن شرف أحلام، بن غرارة الصالح: القرصنة الإلكترونية، أنواعها وأشكالها وطرق التصدي لها، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 5، العدد1، جوان 2012، ص 28.

[3] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبن بكر بلقايد، تلمسان، الجزائر،2012، الصفحة70.

[4] بن شريف أحلام، بوغرارة الصالح، **مرجع سابق**، ص 29.

أما في القرصنة المالية فيعتمد قراصنة على استغلال التغيرات الأمنية في أنظمة البنوك والأجهزة الخاصة، أو استعمالها في إجراء عمليات شراء عبر الانترنت دون دفع أي مقابل[1].

ثالثا: انواع القراصنة المعلومات من حيث الخطورة

إلا أنه وعلى الرغم من اختلافهم وتصنيفهم إلا أنهم يشتركون في درجة خطورتهم مما جعل التطرق لهذا التصنيف أمرا ضروريا باعتبار أنهم يشكلون فئات مختلفة وغير متجانسة لا من حيث الدوافع ولا الوسائل المستعملة ولا الأهداف المرجوة.

أ: تصنيف القراصنة من حيث درجة الخطورة

1: الهاكرز " الهواة"

بدأت كلمة hackers في بداية انتشارها بمفهوم يتنافى معناه عما يُشير إليه اليوم، فكانت تسمية تُطلق على مبرمجي الكومبيوتر ذوي المستوى العالي، لعبقريتهم وقدرتهم على ابتكار أنظمة وبرامج الحاسوب أكثر سرعة، ومن أشهر من اكتسب هذه الصفة، (دينيس ريتش) و(كين تومسون) اللذان صمما برامج اليونكس عام 1969، بعد سنة 1981 ومع ظهور أول حاسوب شخصي من تصنيع شركة IBM،ليُصبح بعدها الهاكرز بالمفهوم السيء الذي هو عليه اليوم، [2]وقد تم تعريف الهاكرز بأنهم " الأشخاص الذين لديهم القدرة الفائقة على اختراق الأجهزة والشبكات، على درجة صعوبة إجراءات وبرامج الحماية التي تم اتخاذها، إلا أنهم لا يقومون بإحداث أي ضرر نتيجة اختراق الجهاز أو الشبكة.[3] أيضا يشير المصطلح للمتطفل أو المتسلل ويعني بها كل شخص ذكي يدخل برامج الحساب الآلي باستعمال إحدى طرقه التسلل أو التطفل لكسب المعطيات وكشف الحسابات باستخدام طرق غير مشروعة معظم هؤلاء الهاكرز يكونون شبابا أو مراهقين.[4]

---

[1]بن شريف أحلام، بوغرارة الصالح، **نفس المرجع**، ص 30.

[1]المواد 143 إلى 160 من الأمر 03_05 المؤرخ في 2003/07/19 المتضمن حقوق المؤلف والحقوق المجاورة تضمنت الإجراءات وكذا العقوبات في الشق المدني والجزائي

[2]بشرى حسين الحمداني، **المرجع السابق**، ص .12

[3]خالد حسن أحمد لطفي، **مرجع سابق**، ص .65

[1] الجهني، منصور بن صالح، **الجرائم المعلوماتية، أنواعها وصفات مرتكبيها، المؤتمر الدولي الرابع للعلوم الاجتماعية: حلول عملية قضايا الكويت**2010، ص 14.

ويطلق البعض هذه التسمية على القراصنة الهواة الذين يتخذون من الجرائم الالكترونية والقرصنة هواية أو فضولا، ويكون غرضها تخريبيا ليس هادفا لغايات، وتكون من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الالكترونية والحاسوب، وقد انتشرت في مواقع الإنترنيت في عقد التسعينات العديد من المنظمات التي ترعى ال Hackers، أو القراصنة يهدف بعضها إلى الدفاع عن المفهوم الحقيقي لهذه الجماعات والذي يتمثل في إلغاء الحدود أمام عمليات سبر أغوار الحواسب والشبكات، وابتكار طرق جديدة للتعامل مع أجزائها الدقيقة والتوجه نحو التثقيف المعلوماتي، في حي أنه يوجد منظمات أخرى أهدافها تخريبية كترويج

البرامج الخبيثة ونشر طرق الاعتداء على خصوصيات الآخرين واختراق الشبكات وأطلق عليها بتسمية الطائفة الحاقدة.[1]

2-كراكرز" المحترفون": يعتبر هذا النوع أخطر من النوع الأول ذلك أن هذا النوع يعلمون ماذا يريدون وما الواجب فعله للوصول إلى أهدافهم بتطوير المستوى العلمي في مجال القرصنة باستمرار، إضافة إلى اعتمادهم على البرامج الجاهزة المتطورة، ويعرف بالكراكر والمقتحم وهم القراصنة الذي يعمل على شفرات البرمجيات المحكمة لاستعمالها وينقسمون إلى الكاردر والفريكرد:[2]

3-الكاردر: وهم القراصنة الذين يعتمدون إلى فك شفرات البطاقات بكل أصنافها سواء كانت بنكية أو غير بنكية.

4-الفريكرد: وهم القراصنة الذين يقومون بفك الهاتف السلكي، إلا أنه توجد هنالك عدة أنواع أخرى من الأصناف ثم تحديدها.

إلا أنهم يعتمدون بصفة أكبر على خبرتهم في لغات البرمجة والتشغيل وتصميم وتحليل وتشغيل البرامج بسرعة، كما أن هوايتهم الأساسية معرفة كيفية عمل البرامج لا تشغيلها،[3] ونظرا للخطورة التي يشكلها

---

[2] خنيش دليلة، **مرجع سابق**، ص 42-43.

[2] زايد محمد، **الجريمة والقرصنة، في مجال المعلوماتية والشبكات**، المجلة العربية العلمية للفتيان، الصادرة عن المنظمة العربية للتربية والثقافة والعلوم، تونس، المجلد 10، العدد 19، 2006، ص75.

[3] خالد حسن أحمد لطفي، **مرجع سابق**، ص 66.

الكراكرز فهم أكثر مرتكبي الجرائم الالكترونية خطورة ويكون هذا النوع من القراصنة من الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الالكترونية،[1]

ب_ تصنيف القراصنة حسب الاتجاهات والأهداف

تتنوع ظاهرة القرصنة الإلكترونية بتنوع الدوافع التي تحرك مرتكبيها، إذ لم يعد القراصنة يسعون إلى غاية واحدة، بل تعددت أهدافهم تبعًا لاختلاف مصالحهم وتوجهاتهم. فقد يكون الدافع ماديًا يرمي إلى تحقيق الربح غير المشروع، أو سياسيًا يستهدف التأثير على الأنظمة والقرارات، أو تجسسيًا بغرض الحصول على معلومات سرية، كما قد يتخذ طابعًا تخريبيًا أو شخصيًا.وعليه يكتسي تصنيف القراصنة من حيث الأهداف أهمية بالغة لفهم طبيعة هذه الجرائم وتحديد خطورتها، مما يساعد على وضع آليات قانونية فعالة لمكافحتها.

1_ القراصنة ذوي القبعات البيضاء:

يتميز القرصان ذو القبعة البيضاء بقوة ذكائه وبحنكته وتمكنه من أجهزة الحاسوب وعالم البرمجيات فاستخدامه لهذا الجهاز يقتصر على تشغيل مؤهلاته ولا يمكنه أبدا إيذاء الآخرين، فيطلق عليه بالقرصان الأخلاقي، بحيث يكون هذا القرصان مصرح لاستخدام الطرق الغير شرعية والتقنيات الممنوعة لكن القرض منها ليس الحاث ضرر بالغير إنما لإصلاح الحاسوب أو معالجة أمنه.[2]

2_ القراصنة ذوي القبعات السوداء

وهو الشخص المنحرف والمفسد وسيء النية لديه غرض وحيد هو الاختراق بقصد ارتكاب فعل غير مشروع كالسرقة، أين يقوم القرصان بصنع فيروسات لتخريب جهاز الحاسوب وكسب أرباح مالية جراء فعله.[3]

3_ القراصنة ذوي القبعة الرمادية أو البنية

---

[1] خنيش دليلة، **نفس المرجع**، ص 42.

[2] أشرف السعيد احمد، **القرصنة الالكترونية**، مطابع الشرطة للطباعة والنشر والتوزيع، مصر، 2013، ص 29.

[3] بشرى حسين الحمداني، **مرجع سابق**، ص19.

يتميز هؤلاء القراصنة بحسن النية وليس شريرين إلا أنهم عند قيامهم بأعمالهم القانونية يتعثرون أحيانا فيرتكبون أفعال تتعلق بالاختراق بغرض لإلحاق الأذى فهم يمثلون خليط بين أصحاب القبعة البيضاء والقبة السوداء، كما انه في بعض الأحيان فان هذا النوع من القراصنة لا يقومون بأغراض خبيثة آو لدافع شخصي وإنما لاكتساب مزيد من الخبرة والاكتشافات[1].

4_ لصوص نظم المعلومات أو قراصنة الهاتف(phreaking)

هم في الواقع قراصنة من نوع أخر ومن مجموعات متنوعة منهم الكراشور، الهاكتيفيست، لديه هدف واحد وحيد هو خرق برامج الحساب الآلي بغرض تخريب المنظومات إلحاق الأذى وهذا لأنهم متعلقون جدا بهذه الأفعال الإجرامية [2]

أن مصطلح phreaking يتكون من كلمتين بالإنجليزية PHONE و freak، ومن خلال المصطلحين نفهم أن مهمة لصوص نظم المعلوماتية ترتكز على استعمال كل الطرق من أجل الدخول بطريقة غير مشروعة إلى نظام الهاتف. بحيث يعتبر ثمرة تكنولوجيا الاتصالات ونظم الاتصال الحديثة وتقع عليهم تسمية متعصبي التلفونات. وهم لا ينتمون لفئة الإرهاب الدولي وغايتهم لا يكون الاحتيال بصفة أساسية، ويكونون في أغلبهم طلاب جامعات ومدارس، حيث يقومون بالغش المعلوماتي بواسطة خطوط تلفونية.[3]

إن عملية قرصنة منظومات الحاسوب تكون إما بدوافع شخصية ككسب الأرباح المالية أو التطفل أو التشهير أو دوافع سياسية.

الفرع الثالث: دوافع القرصنة الإلكترونية

تعرف الدوافع بأنها الأسباب والعوامل التي تحرك إرادة القرصان ورغبته في القيام بسلوك إجرامي وبالتالي فان الأسباب والدوافع التي تؤدي إلى ارتكاب القرصنة الالكترونية تتنوع، فقد تكون الدوافع إما سياسية عقائدية، عسكرية، دوافع مادية، دوافع تجارية كما يمكن أن تكون دوافع شخصية تتعلق بالهاكر

[1] فراش جمال شاكر، السيبيرانية وتحولات القوة في النظام الدولي، دار أمجد للنشر والتوزيع، الطبعة الأولى، الأردن، 2023، ص 187.

[2] حسين طاهري، **مرجع سابق**، ص 32-33

[3] Contraction des motanglaise « fishing » :pêcheet « phreaking » ; piratage de ligne ; téléphonique ; voit M .QUEMENER et J .FERRY ; op cit ;83 .

نفسه (دوافع انتقامية–دوافع إجرامية)، وهي كلها محفزات أو الرغبة التي تتكون لدى القرصان حتى يتبين له ارتكاب الجريمة وفيما يلي نُفصل في الأسباب التي تدفع بالهاكر للقرصنة الالكترونية:[1]

أولا: الدوافع الفردية المرتبطة بالفاعل (الهاكر)

تُعد دوافع القراصنة من أهم العناصر التي تساعد على فهم ظاهرة القرصنة المعلوماتية وتحليل سلوك مرتكبيها، إذ تختلف هذه الدوافع باختلاف الأهداف والظروف المحيطة بالفعل الإجرامي، فضلًا عن تطور البيئة الرقمية التي أفرزت أنماطًا جديدة من الجرائم. فيمكن ان تقتصر القرصنة على مجرد الفضول أو التحدي التقني، بل أصبحت ترتبط بمصالح مادية وسياسية وأيديولوجية معقدة.

أ: دوافع الهاكرز المادية

يسعى القرصان من خلال عملية القرصنة الالكترونية إلى الربح المادي السريع، حيث يحيل للقرصان من خلاله أنه بارتكابه لهذا الفعل سوف يحقق أرباحا طائلة ومن أمثلتها قضية الشركة الوهمية للوساطة والاستثمارات المالية بسوريا والتي تم تصميم موقع لها على شبكة الإنترنت، وادعت أنها وكيلة شركة CIPالأمريكية للأوراق المالية وقد استطاعت استثمار أموال طائلة من طرف العديد من الأشخاص بحجة فتح رصيد باسم كل عميل وبرقم خاص به لشراء وبيع الأسهم في البورصة العالمية بحيث يتمكن كل عميل من الدخول إلى موقع الشركة وبيع وشراء الأسهم، إلا أنه وبعد فترة وجيزة فوجئ العملاء بأنهم وقعوا ضحية عملية احتيال بعد أن تبين لهم وهمية مقر الشركة وموقعها الالكتروني وعدم قانونيتها، وبعد التفتيش في حواسيب الشركة تم ضبط العديد من البرامج المخصصة لمتابعة مؤشرات البورصة عبر شبكة الإنترنت إضافة إلى ضبط عدة نسخ من الوثائق الشخصية للعديد من العملاء وضحايا من جنسيات مختلفة، وفي هذا السياق قامت النيابة العامة بتحريك الدعوى العمومية بحق القائمين على هذه الشركة الوهمية بجرم ممارسة الوساطة المالية المرتبطة بالأوراق المالية دون ترخيص[2].

ب: الدوافع الفردية أو الشخصية

[1] العربي بوعمامة، رقاد حليمة، **العنف في الفضاء السيبيراني**، منشورات مخبر الدراسات الإعلامية والاتصالية وتحليل الخطاب جامعة عبد الحميد بن باديس مستغانم الجزائر، ص 104.

[2] بشرى حسين الحمداني، مرجع سابق، ص69.

تبدأ محاولات الاختراق الفردي بين الأفراد بداعي التباهي باختراق أجهزة الغير، أي أنها تدخل في دافع التحدي، [1]و هذه الدوافع ضمن حب الاستكشاف والاستطلاع وغالبا ما تكون هذه الدوافع عند الشباب القراصنة نظرا لتوفر شعور الرغبة في اكتساب عمليات السطو وعمل الأنظمة المعلوماتية، وقد تكون نتيجة الأحقاد المتراكمة والضغينة الدفينة في تدمير ما لدى الغير وإحداث تخريب إما نتيجة لفصل تعسفي عن العمل، فيكون لهم من المعرفة ما يكفي من المعرفة بنظام الشركة أو المصرف الذي فصلوا منه والعمل على تكبيدها خسائر مالية كبيرة وذلك من خلال تدمير النظام المعلوماتي أو إتاحة الفرصة لجهات خارجية عن النظام، ومن القضايا المشابهة في الو.م. أ حكم عن أحد الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات وغرامة مقدارها 1000 دولار لأنه أدخل فيروسات في أجهزة الشركة التي كان يعمل بها مما نتج عنه ضياع 160 تسجيا من سجلات العملاء وذلك انتقاما من الشركة بعد قيامها بفصله من العمل.[2]

ثانيا: الدوافع ذات الطابع غير الفردي (المؤسساتي أو الجماعي)

يقصد بالدوافع ذات الطابع غير الفردي في مجال القرصنة الإلكترونية أو ما يسمى بالدوافع المنظمة المؤسسية، تلك المحفزات التي لا يكون سببها إرادة شخصية بحتة للفاعل، بل ترتبط بجهات أو مصالح جماعية أو مؤسسية، سواء كانت دولا أو منظمات أو شركات، وتتميز هذه الدوافع بكونها منظمة وموجهة نحو تحقيق أهداف استراتيجية أو اقتصادية أو سياسية مما يعكس تحول القرصنة الالكترونية من سلوك فردي إلى أداة تستخدم في مجالات أكثر تعقيدا، كالصراعات السياسية والعسكرية أو المنافسة الإقتصادية بين الشركات ، فتندرج ضمنها عدة عناصر[3].

أ_ الدوافع السياسية والعسكرية

إذ أصبح هذا الاختراق أكثر أهمية، بحيث يتم اللجوء إليه للبحث عن المعلومات عبر خاصية وذلك لتعلقها الشديد بالأمور التي تمس أمن وسلامة الدولة قصد الحصول على معلومات تمس بسياسة الدولة واقتصادها ونظامها العسكري[4]، فتعتمد سياستها على خاصية التجسس وهذا ما ينطبق حاليا على الولايات المتحدة الأمريكية والصين ، وأيضا في عام 2001 شهد العالم هجمات سيبيرانية تمثلت في اختراق مناطق صناعية عسكرية كثيرة في إيران، بحيث تعتبر هذه المناطق الصناعية حساسة منها إطلاق فيروس

[1] بشرى حسين الحمداني، **نفس المرجع**، ص 70

[2] حسين طاهري، **مرجع سابق**، ص 34

[3] سيد على السيد محمد، الجرائم الإلكترونية، دار التعليم الجامعي،2023، ص 59.

[4] فراس جمال شاكر، مرجع سابق، ص 188.

"ستاكسنت" لأجهزة الحاسوب التي تخص معامل ومصانع تخصيب اليورانيوم، إذ أشارت إيران إلى "الو. م. أ"، "إسرائيل" في تلك الوقائع السيبيرانية، والتي أحدثت تغيير في مفهوم الأمن التقليدي المرتبط بالتهديدات التقليدية مثل تهديد حدود دولة.[1]

ب_ الدافع التجاري

تتمثل الدوافع التجارية في المنافسة بين الشركات التجارية الكبرى، تتعرض هاته الشركات إلى عدد كبير من الاختراقات لحواسيبها من قبل شركات منافسة أو من قبل المخترقون الذين يسعون إلى كسب الأموال مقبل بيع المعلومات للشركات المنافسة

وقد ترد أسباب أخري للهاكر تدفعه نحو جريمة القرصنة الإلكترونية منها:[2]

1-التنافس الإيديولوجي بين الدول المتطورة خاصة ومناهضة العولمة

2-غياب الأمانة لدى العاملين في توريد وإنتاج البرامج المقلدة والمغشوشة

3-التحدي لإثبات القدرات الفنية والتفوق على النظام الإلكتروني

4-الانتقام من الفرد أو مؤسسة كجرائم القذف والتشهير

5-صعوبة الإثبات بالنظر إلى العقوبات المقررة لمرتكبي هاته الجرائم[3].

[1] شريفة كلاع، **مرجع سابق**، ص 121.

[2] بشرى حسين حمداني، **مرجع سابق**، ص 70

[3] سيد علي السيد محمد، مرجع سابق، ص 59

المبحث الثاني: طرق وأساليب القرصنة الإلكترونية وانعكاساتها

لقد أدى الانتشار الواسع لشبكات الإنترنيت والتوسع في المعاملات الإلكترونية إلى زيادة انتشار الجرائم وتنوع صورها، فمن بين هذه الجرائم سرقة البيانات المصرفية، والاستيلاء على أرقام بطاقات الائتمان، واختراق الحسابات البنكية، إضافة إلى استغلال الشبكة في نشر المحتويات غير المشروعة، والواقع أن شبكة الإنترنيت تلعب عدة أدوار في مجال الجرائم الإلكترونية بصفة عامة ، فقد تكون هدفا للجريمة، كما قد يحدث عند قيام شخص بالدخول غير المصرح به إلى أنظمة المعلومات أو المواقع الإلكترونية قصد تدمير البيانات أو سرقتها أو التلاعب بها، كما قد يتم بعد ذلك إعادة نشر هذه البيانات عبر نفس الشبكة أو استغلالها لتحقيق مكاسب غير مشروعة[1] .

وفي حالات أخرى قد تكون شبكة الإنترنيت وسيلة لارتكاب الجريمة، حيث يستخدمها المجرمين في تنفيذ عمليات الاحتيال الإلكتروني، مثل تحويل الأموال بطريقة غير مشروعة، أو استخدام التقنيات الحديثة في التزوير والتزييف، كما قد يتم الاستيلاء على أرقام بطاقات الائتمان و استخدامها في عمليات شراء عبر الإنترنيت أو في إجراء عمليات الدفع الالكتروني بهدف الحصول على الأموال بطريقة غير قانونية وإخفاء مصدرها الحقيقي[2]، ولعل أخطر الجرائم التي يمكن أن تتم عن طريق شبكة الانترنيت هي جريمة القرصنة الالكترونية فيشتمل عملية اختراق المواقع الإلكترونية وقواعد البيانات من أجل سرقة البيانات الشخصية، بهدف انتحال هوية الغير بطريقة غير مشروعة، ومنه الحصول على معلومات مهمة وحساسة، كعناوين البريد الإلكتروني، أو كلمات المرور، أو بيانات اعتماد تسجيل الدخول، أو أرقام بطاقات الائتمان، أو أرقام الحسابات المصرفية[3].

على هذا الأساس فان دراسة صور وأساليب القرصنة الإلكترونية تعد أمرا ضروريا لفهم طبيعة هذه الظاهرة وطرق ارتكابها، الأمر الذي يساعد على وضع آليات فعالة لمكافحتها والحد من أثارها السلبية على الأفراد والمؤسسات والمجتمع بصفة عامة

المطلب الأول: طرق القرصنة الإلكترونية

لا تقتصر القرصنة الإلكترونية على هذه الصور فقط، إنما يعتمد القراصنة كذلك على مجموعة من الأساليب والطرق التقنية التي تمكنهم من تنفيذ عمليات الاختراق، كاختراق كلمة المرور باستخدام برامج متخصصة

[1] Gina Angelis, Cyber Crimes, Chelsea House Published ,USA, 2000, p2.

[2] عبد الله عبد الكريم عبد الله، **مرجع سابق**، ص 20.

[3] خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، الاسكندرية، 2009، ص23.

تقوم بتجربة عدد كبير من الاحتمالات حتى يتم العثور على كلمة المرور الصحيحة، ويعتمد كذلك القراصنة على البرمجيات الخبيثة مثل الفيروسات وبرامج التجسس وأحصنة طروادة التي يتم زرعها داخل أجهزة الضحايا بهدف سرقة المعلومات أو التحكم في الأجهزة عن بعد، أو استخدام هجمات حجب الخدمة التي تقوم بإغراق المواقع الإلكترونية بعدد كبير من الطلبات مما يؤدي إلى تعطيلها ومنع المستخدمين من الوصول إليها[1]، كما نجد أن القراصنة يقومون بالبحث عن نقاط الضعف الموجودة في البرامج أو الأنظمة المعلوماتية من أجل الدخول غير المشروع إلى النظام، ويتم أيضا باختراق شبكات الاتصال اللاسلكية غير المحمية، مثل شبكات "الوآي فاي"، مما يسمح للقراصنة بالوصول إلى البيانات المتبادلة عبرها[2]

إن القرصنة الإلكترونية من الجرائم المستحدثة التي هي في تطور سريع نظرا لزيادة الطلب على استخدام شبكة الانترنيت التي أصبحت تعتري كل العالم بأسره، فلا يوجد بيت أو هاتف نقال يخلو من الانترنيت، فأصبحت الحاجة ملحة لاستخدامها إلا أن هذا الاستخدام المفرط أدى إلى ظهور اختراقات جديدة لم تكن في القدم ولا يمكن للعقل تصورها، أين أصبح العنف والاعتداء عبر شبكة الانترنيت في تفاقم ويقابله انعدام أو قصور القوانين والتشريعات لإتباع الطرق السليمة للحماية من هذه الاعتداءات هذا ما حال دون إمكانية حصر هذه الصور[3].

الفرع الأول: الاعتداء على المواقع الإلكترونية والحسابات الشخصية

تظهر القرصنة الالكترونية في شكل اختراق للمواقع والشبكات الإلكترونية من خلال الدخول غير المشروع إلى الأنظمة الرقمية، تغيير محتواها أو تعطيلها، كما قد تتمثل في اختراق الحسابات الشخصية مثل البريد الإلكتروني أو حسابات مواقع التواصل الاجتماعي، مما يسمح للقراصنة بالاطلاع على المعلومات الخاصة بالضحايا أو استغلالها في عمليات الاحتيال، وتأخذ كذلك القرصنة الإلكترونية صورة سرقة البيانات والمعلومات الحساسة مثل بيانات البطاقات البنكية أو المعلمات الشخصية للمستخدمين، كما قد تتمثل في التجسس الإلكتروني من خلال مراقبة أنشطة المستخدمين وجمع معلومات سرية عن الأفراد أو المؤسسات، وتمتد أيضا إلى تخريب الأنظمة المعلوماتية عبر حذف البيانات أو إتلافها أو تعطيل عمل الأجهزة بها [4].

---

[1] علي زياد العلي، الصراع والأمن الجيوسيبيراني في السياسة الدولية، دراسة في استراتيجيات الإشتباك الرقمي، دار أمجد للنشر والتوزيع، الأردن، 2018، ص 85.

[2] أشرف السعيد أحمد، مرجع سابق، ص 35

[3] حسين طاهري، **مرجع سابق**، ص 55.

[4] أمين تجيني، **الجرائم المعلوماتية**، مجلة استشراف للدراسات والأبحاث القانونية، المغرب، العدد 06، 2020، ص 116.

أولا: تقنيات الإعتداء على المواقع الإلكترونية

في عصر المعلومات وبوجود تقنيات عالية التقدم فإن عمليات الاعتداء تتعدد وتختلف باختلاف الدوافع والأهداف المراد تحقيقها والتي ذكرناها سابقا من طرف الهاكر، فنظرا لحداثة عملية القرصنة الالكترونية واستمراريتها وتقدمها مع التطور التكنولوجي فلا يمكن تحديد صورها وأشكالها على سبيل الحصر وفيما يلي نُفصل في بعض الاعتداءات التي تُجسد صور القرصنة باعتبار أن المواقع الالكترونية تتعرض بصفة مستمرة للسلوكيات العدائية وأعمال الاختراق مما يترتب عنه جرائم في حق الغير والدولة.

ومن بين الطرق التي يعتمدها القراصنة في مواجهة المواقع الإلكترونية التالية:

أ: طريقة استغلال الثغرات

إن المواقع الالكترونية اليوم هي أكثر عرضة للهجمات السيبيرانية، حيث يقوم قراصنة الشبكات بتخريب مواقع عالمية واستغلالها، ويكون هذا عن طريق اكتشاف ثغرات باستخدام بعض البرامج التي تسهل عليه تحقيق الاعتداء على الموقع وهذا استنادا على البحث عن ثغرات الموقع، كما قد يكون البحث عن الثغرات بشكل عشوائي[1]

ب: طريقة حجب الخدمة

يمكن أن تكون الطريقة الهجومية تعتمد على المواقع عن طريق إغراقها بالبيانات والرسائل غير المهمة، وهذه الحيلة لتعطيلها عن أداء مهامها واستغلال الهفوات والأخطاء المبرمجة والموجودة في البروتوكولات قصد القيام بأعمال تخريبية[2].

ومن أبرز القضايا في هذا السياق قرصنة شبكة CNN الأمريكية من خلال نشر فيرس يحمل اسم exeantiction، يعتمد على عرض العلم الصيني في إحدى زوايا الموقع وحين يقوم أي مستخدم بالنقر في العلم حيث تظهر نافذة منبثقة على شريط حاملة صورة الزعيم الصيني الراحل " ماوشيشونغ" مؤسس الحركة الشيوعية في الصين وتظهر تحت الصورة عبارة مكتوب عليها "عمل العلم الأحمر قم بعمل معقول للتعبير عن وطنتيك"، حيث يقوم الفيروس بتقديم محاولة لإعادة الاتصال بموقع الشبكة وإنشاء ضغط هائل عليها باستخدام أوامر http و get[3].

---

[1] محمود الرشيدي، **مرجع سابق**، ص 59.

[2] حسين طاهري، مرجع سابق، ص 57.

[3] حسين طاهري، القرصنة **الإلكترونية**، مرجع سابق، ص 57.

ج: طريقة الدخول والبحث الجماعي في موقع معين

وما يميز هذه الطريقة أنها طريقة سهلة لا تحتاج إلى خبرة، بحيث يتفق مجموعة من المهاجمين للدخول إلى موقع معين في وقت واحد وإتلاف الموقع، من أبرز المواقع التي تتعرض للاعتداء نجد موقع الفاسبوك، يعتبر هذا الموقع من أشهر المواقع الاجتماعية على شبة الإنترنت ويشترك فيه الملايين من مستخدمي الشبكة، ومنه يظهر جليا أن الهاكر يتبع عدة طرق تستخدم في تدمير مواقع الأنترنيت نذكر منها الأكثر شيوعا

1-بروتوكول FTPالدخول باستخدام هوية محجوبة [1]من خلال مدخل بروتوكول افتي بي وهذا بعد تحصل القرصان على كلمة السر بعد إجراء اختبارات للرموز والأرقام والحروف.

2-TELENT استخدام الثغرات الأمنية في بروتوكول كذلك في نظام التشغيل:

WINDOW أو UNIX من استخدام تطبيقات تعتمد على بروتوكول TELENTفتنفذ جميع الأوامر المطلوبة[2] تعتمد هذه الخاصية على تمكين أجهزة الحاسوب من الوصول إليها عن بعد وتنفيذ الأوامر عليها

3 Phishing/ هجمات حجب الخدمة أو التصيد

هي خاصية جديدة تعتمد على هجمات تخترق الحاسوب من دون علم أصحابه وذلك بإرسال برنامج خبيث يسمى "حصان طروادة " على حسب المثال ترسل رسالة تتضمن برنامج معين عن طريق البريد الإلكتروني فتدعوهم إلى بث البرامج إلى مزود معين من أجل إيقافه عن العمل ، وهذا ما يصنع الفرق بين عمليات تدمير الموقع وبين هجمات حجب الخدمة فالأولى تعي اختراق مزودات الويب أما الثانية بإرسال مجموعة أشخاص حزم بيانات بصورة مكثفة إلى هذه المزودات من اجل توقفها عن العمل، ومثال ذلك أيضا صور لرسائل بريد إلكتروني مزيفة بها فيروس أو حشرة[3] .

ثانيا: تقنيات الاعتداء على الحسابات الشخصية

في إطار الخصوصية أصبح اليوم لكل فرد حساب شخصي يعبر عن شخصه، تتنوع الحسابات الشخصية ومن أمثلتها البريد الالكتروني، حساب الفيس بوك، الانستغرام، أيضا من الجانب الأكاديمي نجد حسابات تتعلق بالباحث مثل Google scolaire،

---

[1] أشرف السعيد أحمد، **مرجع سابق**، ص51.

[2]Tamrab.orr: Privacy and hacking cyber Citizen stipend Cyber Safety, The Rosen Publishing Group ,Inc., C2008 , P24

[3] أشرف السعيد أحمد، **نفس المرجع**، ص 52.

SNDL وغيرها والتي تخص الباحث أو الفرد بشخصه ولا يمكن مشاركتها مع غيره وسنفصل في بعض منها :

أ-البريد الالكتروني: وهو عبارة عن خط مفتوح على كل أنحاء العالم يعمل على استقبال وإرسال واستقبال كل ما يريده من رسائل **1**.

إن الاعتداء على البريد الالكتروني يتمثل في اختراقه حيث تتم هذه الجريمة باختراق البريد الالكتروني والاستيلاء عليه مع تغيير محتواه أو سرقة ما فيه من الرسائل أو صور ومستندات أو غيرها مع التجسس أو تدمير الأنظمة المعلوماتية، والاختراق هو الدخول الغير مشروع إلى المعلومات والبيانات المرسلة عن طريق البريد الالكتروني تتم العملية من خلال أحصنة طروادة والتي يكون مصدرها البريد الالكتروني والمواقع المشبوهة، وهذه الطريقة ضارة لأنها تقوم بتسهيل التجسس والتعرف على كلمات العبور وتدمير الملفات[2].

يتم الاختراق أيضا عن طريقIPADRESS أو ربط جهازين ببعضهما البعض عن طريق المودم وبذلك يمكن السيطرة عن الجهاز الآخر بطريقة أو أكثر وهذا بالتخفي أو بطرق ظاهرة أو عن طريق تحميل ملفات أو إجراء محادثات أو كتابة أو مسح معلومات.[3]

كما تتم عملية القرصنة عن طريق انتهاك مراسلات البريد الإلكتروني وتعد هذه العملية من أخطر الجرائم وهذا لارتباطها الوثيق بالحريات الشخصية وتنفذ بواسطة الحاسوب أو الهاتف النقال، ويتسم المعتدين بالمهارات العالية ويقع الاعتداء على الصورة الشخصية أو الأسرار المستندات ويتم نسخها والتلاعب بها وقد يصل الأمر في بعض الحالات إلى حذفها وفي حالات أخرى يقوم المخترق بنشر المراسلات والصور إلى عبر مواقع التواصل من واجب المستخدم التأكد بأنه لا يمكن للمخترق ومهما كانت الظروف سرقة كلمة المرور للبريد الالكتروني، أما بالنسبة إلى أساليب اختراق هذا البريد فيمكن ذكرها على النحو التالي:

1_عن طريق التخمين

يتم من خلالها حفظ كلمة المرور في جزئية خاصة مما يشكل ملفا متكونا من قائمة من كلمات السر مخمنة فينطلق البرنامج بتجربة هذه الكلمات حتى يصل إلى المفتاح الصحيح[4]، لكن هذه الطريقة غير

---

[1] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، المحاكمة الإلكترونية، دراسة تحليلية مقارنة مدعمة بالفقه القضاء المقارن، دار العلا، الجزائر، ص 120.

[2] أشرف السعيد أحمد، **مرجع سابق**، ص 53.

[3] علي عوادة، **الحماية الجزائية في جريمة انتهاك مراسلات البريد الالكتروني**، بحث منشور على الموقع الالكتروني 597027 http/ www.doraraliraq.net/the/theeads، تاريخ الزيارة 10/ 05.2025على الساعة 16.00.

[4] أشرف أحمد السعيد، مرجع سابق، ص 53.

مضمونة باعتبار أن معظم مستخدمي البريد الالكتروني يقومون بحضر حساباتهم حفاظا عليها من الاختراق إلا في الحالات التي يعتمد فيها المستخدم على كلمات مرور سهلة مثل أسمائهم وأسماء أبنائهم أو تواريخ ميلادهم ويظهر هذا خاصة [1]في استخدام الهاتف النقال.

2_عن طريق الاحتيال باستخدام الصفحات المزيفة:

يعتبر هذا الأسلوب من الأساليب الأكثر نجاحا، إذ يعتمد فيه الهاكر على استخدام الطرق الاحتيالية إما بالغش أو الخداع للحصول على المعلومات السرية للمستخدم [2]، فيقوم بإرسال صفحات مشابهة لصفحة التسجيل في البريد الإلكتروني فيقوم المستخدم بكتابة اسم البريد أو كلمة المرور في الصفحة الوهمية، وعوض تسجيل الدخول في الخادم تقوم الصفحة بإرسال المعلومات إلى المخترق، أما الطريقة الأخرى هي إرسال الروابط والرسائل المزيفة مثل بطاقات المعايدة فيقوم المستخدم بالضغط عليها فيتم تسجيل الدخول مباشرة من قبله وعند تسجيل دخوله تقوم الصفحة هي الأخرى بإرسال كلمة المرور إلى المخترق.

3_عن طريق البرامج اللاصقة

تعتمد هذه الطريقة على زرع برامج لاصقة في جهاز الضحية، تعمل هذه البرامج على تخزين المعلومات دون أن يشعر المستخدم بها فتسجل ما يكتبه على لوحة المفاتيح مثل عناوين البريد الإلكتروني، اسم المستخدم وكلمة المرور وحتى أرقام البطاقات البنكية لترسل بعدها مباشرة إلى المخترق والتطبيقات المستخدمة في الغالب هي (Kuylogger) وهو تطبيق مهمته التجسس يعمل على رصد كل ما يتم كتابته على لوحة المفاتيح ومن ثم إرساله للمخترق، وهي متعددة تأتي على شكل مستند يرسل للبريد الإلكتروني للضحية وعند التشغيل يتم تثبيت التطبيق، كما نجد نوع أخر يكون على شكل قطعة إلكترونية صغيرة توصل مباشرة بين لوحة المفاتيح واللوحة الأم، فيمكن شراء هذه التطبيقات عن طريق الإنترنيت بأسعار مغرية .[3]

نظرا للأهمية البالغة للبريد الالكتروني فإنه يجب على المستخدم التوجه دائما للمحافظة على حسابه وحمايته من الاختراق أو السرقة، وفيما يلي مجموعة من الإجراءات الاحترازية لذلك:[4]

---

[1]Indira Carr: Computer Crime International Library of Criminology, Criminal Justice and Penology– Second Series, AshgateC2009, P243.

[2]Bunn, Edward Devi, Op. Cit, P126.

[3] أمير فرج يوسف، **مرجع سابق**، ص 79.

[4] أشرف السعيد أحمد، **مرجع سابق**، ص 59.

*اختيار كلمة باس ورد قوية يصعب تخمينها، أي أن تحتوي الكلمة مجموعة رموز، أحرف كبيرة، أحرف صغير...

*تغيير كلمة المرور بين الفترة وأخرى.

*تسجيل الخروج من البريد الالكتروني عند الانتهاء، وبالأخص عندما يكون الجهاز مشترك.

*لحذر عند استلام رسائل مشبوهة مرسلة من طرف أشخاص غير موثوق بهم.

*الأخذ بعين الاعتبار دائما أن مزودو خدمة البريد الالكتروني لن يطلبوا من المستخدمين إرسال كلمة المرور الخاصة بهم.

يراعى استخدام برنامج مكافحة فيروسات جيد ويتم تحديثه بصفة مستمرة عن طريق الانترنت[1].

ب-الاعتداء على منصات التواصل الاجتماعي

تتعرض الحسابات الشخصية بصفة دائمة إلى الاعتداء والاختراق، منها منصة الفيس بوك التي تعد المنصة الأكثر شيوعا حتى أنه أصبح يشكل تهديدا صارخا لرواده، يرى البعض أن دول الخليج أكثر عرضة للاختراق، حيث أصبح من اللازم عليهم اتخاذ الإجراءات الأمنية و الاحترازية لأجل عدم الوقوع في هذا النوع من الجرائم، أين أعلنت وزارة الداخلية القطرية التي أشارت أن معظم الحسابات التي تم اختراقها كانت بسبب الروابط والرسائل ذات المصدر المجهول، والأمر لم يقتصر فقط على المتعاملين من دولة قطر، بل امتد لدول مجاورة منها الكويت، عمَّان، السعودية، التي تعاني هي الأخرى من آثار هذه الجريمة.

1 - قرصنة واختراق الفايس بوك

أما بالنسبة للدول الأجنبية فإنها تشهد جرائم الاختراق بصورة أكثر انتشارا مقارنة بالدول العربية بصفة عامة، حيث تتعرض الصفحات الشخصية التابعة للمؤسسات الحكومية وكذا الأفراد للاختراق.[2]

ومن الملاحظ أن جريمة الاختراق لا تقتصر على فئة معينة ذلك أنه ولكل عملية اختراق دافع كما تطرقنا سابقا.

[1] أشرف السعيد أحمد، نفس المرجع، ص 57

[2] حسين طاهري، **مرجع سابق**، ص 77.

1.1- طرق اختراق الفايسبوك بإرسال الروابط الوهمية

تتمثل هذه العملية في إرسال الروابط الوهمية بحيث تشاركها الصفحات والمجموعات أو بين المستخدمين أنفسهم، وتعد هذه الطريقة من أسهل الطرق لاختراق الحسابات حيث لا يتكبد صاحبها عناء كشف الثغرات والطرق الملتوية، بل يكتفي فقط بإرسال الروابط الوهمية، بل حتى إن المستخدمين يقعون ضحية أنفسهم عند إرسال الروابط ومشاركة الـ«Link» عند الضغط عليه يقوم بتحويل المستخدم إلى صفحة أو موقع وهمي يقوم عند الضغط عليه بتحويل المستخدم لصفحة أو موقع وهمي يعمل أثناء تحميله على تحميل النسخ ونقل المعلومات المستخدم الرئيسية لحساب المستخدم كلمة المرور إلى مرسل أو مصنع الفيروس مباشرة، وما يدفع المستخدم للوقوع في هذه الفجوات هو الطمع، كالرد على رسائل " أحصل على رصيد مجاني"، وبعد وقوع المستخدم في فخ المخترق وضغطه على الرابط، يحصل الهاكر على اسم الحساب وكلمة السر والولوج إلى الفيس بوك واختراقه ومن ثم الحصول على ما يريد من المعلومات والصور والرسائل التي يحتويها حساب الضحية.[1]

2.1-طريقة رقم الهاتف النقال واستغلال شبكات7ssب.

تعتمد هذه الطريقة على ادعاء الهاكر أنه نسي كلمة المرور الخاصة بالحساب، فيرسل الفيس بوك بطريقة آلية رمزا سريا للهاتف كرمز تأكيد بأن الشخص الذي يحاول تسجيل الدخول للحساب هو صاحب الحساب بذاته، وهنا يستغل المخترق شبكة ssd، بغرض تحويل ذلك الرمز من هاتف الضحية إلى جهاز حاسوب الهاكر، وفور إدخال الرمز يكون المخترق قد تَمَكن من حساب المخترق[2].

3.1- طريقة هجمات البرامج النصية

تعتمد طريقة البرامج النصية على إرسال رسالة نصية للضحية تكون على شكل ملف يُرسل عبر البريد الالكتروني أو غيرها من منصات التواصل، وفور أن يقوم الضحية بفتح الملف، تكون المعلومات قد وصلت فورا إلى المرسل (الهاكر)، إلا أنه يشترط لعملية القرصنة بطريقة هجمات البرامج النصية هو أن يتصل صاحي الحساب بالفيس بوك.[3]

---

[1] عيسى داوود الزيدي، مرجع سابق، 98.

[2] حسين طاهري، جرائم القرصنة الإلكترونية، **نفس المرجع**، ص78.

[3] محمد حمادة الهيتي، **البحث عن حماية جنائية للبيانات والمعلومات الشخصية المخزنة في الحاسب الآلي مجلة الشريعة والقانون**، جامعة الامارات العربية، العدد27، يوليو، 2006، ص44-45.

ج: حماية الخصوصية في مواقع التواصل الاجتماعي

نظرا لخصوصية مواقع التواصل الاجتماعي، فإنه يستلزم على المستخدمين إتباع جملة من الاحترازات تتمثل فيما يلي:[1]

1-التدقيق في المعلومات الحساسة، تكتبها والصور والفيديوهات التي يتم تحميلها على حسابه، فيفضل عدم كتابة أي شيء في صفحة الملف الشخصي خاصة المعلومات الشخصية.

2.يجب ضبط إعدادات الخصوصية حسب ما يتناسب مع شخصية المستخدم وطبيعة عمله وبيئته.

3-تقليل دائرة الأصدقاء عن طريق عدم قبول طلبات الصداقة من الأشخاص الغير معروفين.

4-وضع كلمات مرور قوية " تتكون من أرقام وحروف..."

5-أخذ الحيطة والحذر من الحيَّل مثل الرسائل التي تصل، حيث تكون واجهة الموقع المرسل مطابقة لواجهة الموقع المراد سرقة كلمة سره، وعند إدخال البريد الالكتروني وكلمة السر في هذا الموقع المزيف وهذه العملية تسمى بالتصيد«phishing» .

ويستحسن تسجيل الدخول من جهاز واحد، بشبكة انترنيت خاصة بالمستخدم حتى تكون أكثر أمانا.

الفرع الثاني: الاعتداء على البرامج والأنظمة المعلوماتية

مع زيادة الوعي بأهمية المعلومة كوعاء ناقل للمعارف، أصبحت المعلومات ذات قيمة اقتصادية عالية ترتكز عليها الصناعات ذات قدر عال من الأهمية، وذات الأمر بالنسبة للبرامج فالبرامج تعتبر المحرك أساسي للحاسوب وبدونها لا يمكن له آداء وظائفه ومن خلال هذا الفرع سنتطرق لصور الاعتداء على البرامج والنظم المعلوماتية.

إن برامج الحاسب الآلي تعد القلب النابض، وتجسد الكيان المعنوي له وبدونه لا يصبح للمكونات المادية للجهاز أي معنى. فالمقصود هنا بالبرامج جميع المكونات غير المادية لنظام الحاسب الآلي، ويشتمل على برامج النظام والكيانات المنطقية الأساسية المتمثلة في البرامج الأساسية اللازمة لتشغيل الحواسيب

[1] بشرى حسين الحمداني، **مرجع سابق**، ص 166 وما بعدها.

وبرامج التطبيقات أو الكيانات المنطقية التطبيقية وهي البرامج، التي تهدف إلى حل المشاكل المتعلقة باستعمال الحاسب الآلي.[1]

وقد عرفها البعض بأنها " تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد يسمى الحاسب الالكتروني بغرض الوصول إلى نتيجة معينة".[2]

إن الاعتداء على البرامج من خلال طرق النسخ والتزوير للبرنامج الأصلي والذي يتم وضعه على شبكة الإنترنت ومن ثم بيعها والمتاجرة بها حيث يكون هنا القصد من القرصنة ليس فقط التخريب بل جني مكسب مالي طائل من خلال هذه العمليات، كما يعتمد القراصنة على طرق أخرى وهي تقديم البرامج عبر الإنترنت دون مقابل بغرض التباهي بقدراتهم في سرعة كسر نظام حماية النسخ الذي يتم إدراجه بحجة أن البرامج الأصلية مرتفعة الثمن لا يمكن لمستخدمي الكومبيوتر أصحاب الدخل المتوسط تحمل أعباء شرائها، ومن أبرز الفئات فئة الطلبة الذين يشكلون الغالبية العظمى من مستخدمي البرامج المقرصنة في العالم.

أولا: الاعتداء على سير عمل الأنظمة المعلوماتية

تتعدد صور تدمير البرامج ونظم المعلومات وتختلف باختلاف الأهداف وسنفصل فيمايلي آليات التفافها:

أ_عرقلة أو تعطيل نظام المعالجة الالية للمعطيات

تتمثل في عرقلة عمل النظام المعلوماتي عن طريق تباطؤ عمل نظام المعالجة الآلية للبيانات، ما يحدث تغيير في حالة عمل النظام بشكل شلل مؤقت

ب_إعاقة الوصول الى الخدمات والموارد المعلوماتية

فتكون الإعاقة بأساليب مختلقة منها تعديل البرامج بنظام المعالجة أو عمل برنامج احتيالي أو بتحويل المسار على الشبكة ما يدفع به إلى التوقف المؤقت أو الدائم، وهو ما يسمى بالتحويلات الإلكترونية.

ثانيا: الاعتداء على سلامة البرامج والبيانات

يوجد العديد من الوسائل التقنية المستخدمة في عمليات الاعتداء على البيانات داخل النظم المعالجة الآلية للبيانات باستخدام الطرق التقنية ولعل أهمها والأكثر فعالية هي استخدام الفيروسات.

---

[1] خالد حزبي السعدي، **جريمة إتلاف معلومات الحاسب الآلي في التشريعين الكويتي والمقارن**، دار النهضة العربية، الطبعة الأولى، 2012، ص 20.

[2] حسين طاهري، **مرجع سابق**، ص 84.

أ-إدخال الفيروسات

أطلقت تسمية الفيروس المعلوماتي تشبيها بطريقه عمله بالفيروسات التي تصيب الكائنات الحية، إذ يشترك معها في العديد من الخصائص، من أهمها قابلية الانتشار و الانتقال إلى جهاز أخر لإضافة إلى قدرته على إحداث تغييرات في النظام المصاب والتسبب في أضرار متفاوتة الخطورة يرى بعض الباحثين في تاريخ أمن المعلمات أن البدايات الأولى لفكرة الفيروسات تعود لسنة 1981،حيث ظهرت تجربة برمجية ذات طابع علمي هدفت إلى دراسة قدرة البرامج على الانتشار، وقد اعتبرت هذه التجربة النواة الأولى التي مهدت لظهور ما يعرف اليوم بفيروسات الحاسوب أين ينتشر البرنامج فيها من خلال وسائط التخزين مثل الأقراص، لم يكن الهدف منه إحداث أضرار ، إلا أن شهدت سنة 1999 احد أشهر الفيروسات وهو فيرس ميليسا، الذي اعتبر نقطة تحول في تاريخ البرمجيات الخبيثة، فقد جمع هذا الفيروس بين خصائص **فيروسات الماكر** و**ديدان الإنترنيت**، وهو ما أدى إلى تعطل عدد كبير من خوادم الشركات والمؤسسات حول العالم[1].

تجسد الفيروسات برامج غير مرغوب فيها تملك القدرة على الانتشار ويعاد تكوين نفسها والالتصاق ببرامج أخرى، ولها قدرات عالية في تدمير البرامج والمعلومات[2]، كما أنها تصيب الأجهزة بالعطب من خلال مسح أو تغيير بعض ملفات التشغيل، ويبقى خارج الخدمة لفترة محددة، ثم ينشط مجددا في توقيت محدد ليقوم بتدمير البرنامج وإتلاف المعلومات المخزنة عن طريق الخرق أو التعديل، وهذا ما يوضح الارتباط الشديد بين الفيروس والجريمة حيث أن الفيروسات في هذه الحالة تمثل أداة ارتكاب الجريمة[3]. ومن أبرز خصائصه قدرته على النسخ الذاتي التلقائي، فهو عبارة عن برنامج أو مجموعة تعليمات وأوامر للحاسب الآلي هدفها إلحاق الضرر بنظام المعلومات أو البيانات، والمخيف في الفيروسات هو قدرته على التضاعف والانتشار.

تعد الفيروسات المعلوماتية نوعا من البرمجيات الضارة التي يتم تطويرها، بواسطة أشخاص يمتلكون معرفة تقنية متقدمة، حيث تصمم بهدف التأثير على الأداء الطبيعي للأنظمة المعلوماتية، وتعمل هذه البرامج على تعديل وظائف النظام أو تعطيل بعض مكوناته من خلال إدخال أوامر خبيثة تؤدي إلى إتلاف الملفات أو إيقاف تشغيل البرامج أو إضعاف كفاءة النظام الإلكتروني[4].

---

[1] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، **مرجع سابق**، ص 68.

[2] منال البلقاسي، **مرجع سابق**، ص 167.

[3] أشرف السعيد أحمد، **مرجع سابق**، ص 70.

[4] خالد حسن أحمد لطفي، مرجع سابق، 103.

يمكن لهذه البرامج أن تسبب اضطرابات في شبكات المعلوماتية والخدمات الرقمية، وقد تمتد أثارها إلى المساس بوسائل الاتصال وتعطيلها غالبا ما يتم عن طريق استغلال ثغرات أمنية في بروتوكولات البيانات، وهو ما يسمح للمهاجمين من اختراق النظام أثناء تشغيله والتلاعب بوظائفه الأساسية[1]

ولا يقتصر عمل الفيروسات فقط على الغرض التخريبي فقط بل قد يكون الغرض منها حمائي، أو تخريبي

1 _الغرض الحمائي

يقصد به حماية البيانات والبرامج من الأخطار التي ترد على النسخ غير المشروع، ذلك أن الفيروس يعود لحالة النشاط بمجرد نسخه ويدمر نظام الحاسب الذي يعمل عليه[2].

2_ الغرض التخريبي

إن الغرض من الفيروسات يكون في العادة غرض تخريبي قصد تدمير البرامج أو الابتزاز، فالمخترق أثناء تعامله مع الفيروسات تكون غايته تحصيل منافع شخصية[3].

من أبرز الوسائل التي تساعد على انتشار الفيروسات يتم من خلاله إرسال الفيروسات لأكبر عدد من المستخدمين المتصلين بشبكة الإنترنيت حال وصول الرسالة وفتحها يدخل الفيروس في نظام المعالجة الآلية ويبدأ بتدمير البيانات والمعلومات المخزنة فيه.

ب_ نسخ البرامج

تنتقل الفيروسات إلى البرامج أو المعلومات داخل أجهزة الحاسب الآلي بعد عملية التحميل فتنتقل العدوى إلى هذه البرامج آو المعلومات[4].

ج–تحميل البرامج من الشبكات

عند القيام بتحميل البرامج من الشبكات المصابة بالفيروس ينتج عنها إتلاف البرامج والمعلومات المخزنة داخل الحاسب الآلي ومن بينها برامج ضبط البيانات التي يستخدمها صاحب الجهاز في توفير

---

[1] شريفة كلاع، الأمن السيبيراني وأشكال التهديد، **مرجع سابق**، ص 105.

[2] دليلة خنيش ، مرجع سابق، ص 92.

[3] أشرف السعيد أحمد، مرجع سابق، ص 71.

[4] بشرى حسين الحمداني، مرجع سابق، ص 79.

مساحة التخزين، إلا أن هذه البرامج تكون في بعض الأحيان محملة بالفيروس الذي له القدرة على الاختفاء والتمويه على المستخدم[1].

الفرع الثالث: الاعتداء على التجارة الإلكترونية

في مجال التطور الاقتصادي عرفت التجارة قفزة انتقالية من المفاهيم التقليدية للتجارة إلى نوع آخر من أنواع التجارة وهي ما تسمى بالتجارة الالكترونية، فأتاحت بذلك فرصا واسعة أمام المؤسسات الاقتصادية، خاصة الصغيرة المتوسطة، لتوسيع أنشطتها التجارية وتعزيز خضوعها في الأسواق، فقد وفرت شبكة الإنترنيت قنوات جديدة للتسويق والتبادل التجاري، مما مكن هذه المؤسسات من زيادة حجم مع وتوسيع نطاق تداول منتجاتها وخدماتها عبر الفضاء الرقمي[2]، فتشير التجارة الإلكترونية إلى كل عملية تجارية تتم بين طرفين أساسيين هما البائع والمشتري، ويتم ذلك عن طريق عقد الصفقات وتسويق المنتجات وهذا باستخدام الحاسب الالكتروني الموصول بشبكة الانترنت دون حاجة لانتقال الطرفين أو التقائهما حيث يبرم العقد إلكترونيا.[3]

بالرغم من التقدم الملحوظ في قطاع الاقتصاد الرقمي، إلا أن عرف هذا المجال في السنوات الأخيرة، بعض التحديات المتعلقة بتقلبات الأسواق العالمية والانهيارات التي طالت بعض القطاعات الاقتصادية المرتبطة بالإنترنيت، فيؤكد العديد من الخبراء في مجال المال والأعمال إلى ضرورة اتخاذ إجراءات عملية لتعزيز استخدام التقنيات الحديثة في الأنشطة التجارية، بما يحسن كفاءة الأداء الاقتصاد بزيادة فعالية التبادل التجاري.

وفي نفس السياق يرى عدد من الخبراء أن تطوير التجارة الالكترونية يتطلب اعتماد الشركات على التقنيات الحديثة لان ذلك يساعد على توسيع قنوات التسويق، التوزيع وتحسين كفاءة الأداء داخل المؤسسات، ومن جهة أخرى يلاحظ أن غياب الأطر القانونية وضعف الدعم الحكومي للتجارة الالكترونية في بعض الدول يشكل عائقا أمام انتشار هذا النمط من المعاملات الالكترونية، التي تشكل أحد أهم الأسباب التي تدفع العديد من الشركات إلى التردد في الاعتماد على التجارة الالكترونية بشكل كامل[4].

---

[1] بشرى حسين الحمداني، **نفس المرجع**، نفس الصفحة.

[2] هبة مصطفى كافي، **التجارة الإلكترونية**، ألفا للوثائق، قسنطينة، الجزائر ،2017، ص19.

[3] طوني ميشال عيسى، **التنظيم القانوني لشبكة الانترنت، المنشورات الحقوقية**، 2001، ص 253.

[4] دليلة خنيش مرجع سابق، ص 132، نقلا عن عبد الفتاح بيومي حجازي، الذي عرف التجارة الإلكترونية بأنها "النقل الإلكتروني بين جهازين للكمبيوتر للبيانات التجارية باستخدام نظام متفق عليه لإعداد المعلومات"

أولا:الاستيلاء على أرقام البطاقات الائتمانية

تعتبر بطاقة الائتمان وسيلة من الوسائل الحديثة للدفع الالكتروني، تغني صاحبها عن حمل النقود خاصة فيما يتعلق بالمبالغ المالية الكثيرة، وهذه البطاقة تصدر إما عن البنك أو أ مؤسسة لمصلحة العملاء من خلالها يكون له إمكانية التعامل مع المحلات التجارية وشراء حاجاتهم دون دفع اي نقود، وهي أحد أنواع بطاقات الدفع الالكتروني[1]، وتعد بطاقة الائتمان من الوسائل المصرفية الحديثة التي ظهرت في إطار تطور الخدمات البنكية، حيث بدأ استعمالها في الولايات المتحدة الأمريكية في منتصف القرن العشرين، عام 1950[2]، فيقوم هذا النظام على مبدأ منح العميل تسهيلات مالية من طرف المؤسسة البنكية، حتى يتمكن من إجراء عمليات الشراء أو الحصول على خدمات معينة دون دفع قيمتها فورا، بل يتم تسديد المبالغ المستحقة لاحقا خلال مدة محددة وفق الشرط المتفق عليها.[3]

ومع الانتشار الواسع لتكنولوجيا الاتصال والمعلومات، وخاصة انتشار التجارة الإلكترونية واتساع نطاق التعامل عبر شبكة الإنترنيت، ازداد العمل ببطاقات الائتمان بشكل كبير في المعاملات المالية لذلك يمكن تعريفها بأنها "وسيلة دفع إلكترونية تتمثل في بطاقة مصنوعة من البلاستيك، تصدرها مؤسسة مالية لعملائها، وتخول لهم استعمالها في دفع ثمن السلع والخدمات أو في سحب مبالغ مالية، على أن تتم تسوية المبالغ المالية المستعملة لاحقا وفق النظام الائتماني المعتمد من قبل الجهة المصدرة للبطاقة ".[4]

أ -أنواع البطاقات الائتمانية:

يوجد العديد من البطاقات البنكية والتي تمنحها البنوك لعملائها، التي تتيح لهم إجراء مختلف العمليات المالية بطريقة إلكترونية ومن أهم هذه البطاقات ما يلي:

1-بطاقة الائتمان: تسمح هذه البطاقة للعملاء استعمال ائتمان في حدود الاتفاق المبرم بينها وبين المصرف الذي صدرت عنه هذه البطاقة، ويكون التعامل بها بتسديد ثمن المشتريات على دفعات بدلا من تسوية حسابه فورا، ذلك شرط أن يكون في حدود مبلغ معين ومحدد مسبقا[5].

---

[1] خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة عمان – الأردن، الطبعة الأولى، 2011، ص 118-119.

[2] سيد علي السيد محمد، **مرجع سابق**، ص 35.

[3] سيد علي السيد محمد، **نفس المرجع**، نفس الصفحة.

[4] عبد الجبار الحنيص، **الحماية الجزائية لبطاقات الائتمان الممغنطة من التزوير**، مجلة دمشق للعلوم الاقتصادية والقانونية، المجلد 24، العدد الثاني،2008، ص 149.

[5] سيد علي السيد محمد، **نفس المرجع**، ص 38

2-بطاقة السحب: يقوم دورها في سحب المبالغ المالية فحسب إما داخل البلد أو خارجه من أحد الأجهزة التابعة للبنك الذي صدرت عنه البطاقة (سحب مباشر) أو أحد الأجهزة التابعة كمؤسسة أخرى (سحب غير مباشر)، وهذه البطاقة تمنح للعميل لسحب النقود والحصول على السلع والخدمات عبر شبكات الانترنت فيقتصر على العميل الولوج إلى موقع التاجر على الشبكة المعلوماتية وبعدها يختار السلع المراد شرائها ليقوم التاجر بعملية الإرسال لهذه السلع إلى عنوان المشتري[1].

3 _ بطاقة الوفاء أو الدفع: ترتكز مهمة البطاقة في وفاء العميل بثمن السعر الخدمات التي يحصل عليها من بعض التجار المقبولين لدى الجهة مصدرة البطاقة عن طريق خصم مبلغ معين منها، بحيث تمنح الشراء مع التسديد المباشر في المصرف عن طريق ما يعرف بالحسم الفوري أو الدفع الفوري[2].

4-**البطاقة الدائنة أو المسبقة الدفع:** هي نوع آخر من البطاقات يمنح فيها البنك المصدر لحامل البطاقة قرضا في حدود معينة على درجة البطاقة وهذا لمدة زمنية تكون محددة هي الأخرى ويشترط تسديده كاملا من خلال وقت يكون قد اتفق عليه الطرفان من قبل، إلا أنه يجب الإشارة هنا أنه وفي حال تأخر العميل على سداد يترتب عن ذلك زيادة مالية وهي الصورة الأصلية لبطاقة الائتمان[3].

ب_الطبيعة القانونية لبطاقة الائتمان

تعددت الآراء واختلفت بخصوص الطبيعة القانونية لبطاقة الائتمان حيث أن البعض يعتبر أن التعامل مع الغير سواء كانوا تجار أو شركات يكون بمثابة وكالة أي أنه وبمقتضاها يتم توكيل حامل البطاقة البنك الذي أصدر البطاقة في دفع ثمن السلعة أو الخدمة التي حصل عليها وفي المقابل تخصم من الحساب الموجود لديه، في حين كان للبعض الآخر رأي مخالف يقوم على أساس أن السداد بواسطة بطاقة الائتمان يقترب من حوالة الحق باعتبار أن حامل البطاقة هو دائن للبنك المصدر، فيتنازل عن هذا الدين إلى التاجر، إلا أن البطاقة ليست سندا مثبتا لدين حاملها وإنما هو دليل على وجود مبلغ مالي محرر يمكن التعامل في حدوده. [4]

---

[1] حسين طاهري، القرصنة الإلكترونية، مرجع سابق، ص 124.

[2] سيد علي السيد محمد، **مرجع سابق**، ص 36.

[3] أنظر محمد توفيق مسعودي، **بطاقة الائتمان والأسس القانونية للعلاقات الناشئة عن استخدامها**، دار الأمين، القاهرة، 2001، ص 81.

[4] حسين طاهري، **مرجع سابق**، ص 123، 124.

ج-الاحتيال المعلوماتي المرتبط بالبطاقات البنكية

مع انتشار استخدام البطاقات البنكية ظهرت صور متعددة من الجرائم الإلكترونية، من بينها الاحتيال المعلوماتي بواسطة بطاقة الائتمان، والذي يتمثل في استعمال البطاقة أو بياناتها بطريقة غير مشروعة بهدف الحصول على أموال أو خدمات دون وجه حق، مثل سرق بيانات البطاقة أو استعمالها عبر الانترنيت دون إذن صاحبها، ومن هنا يمكن تبيان طرق الاختراق ويكون بثلاث طرق هي:

1_الاختراق غير مشروع لمنظومة خطوط الاتصالات العالمية:

وهي الخطوط التي تشكل همزة وصل بين الحاسب الآلي للتاجر والمشتري وهو أخطر الأساليب التي تهدد عملية التسويق عبر شبكة الانترنت حيث يقوم المخترق بتسخير كل خبراته وبرامجه في إطار محاولة اقتحام وفك رموز الشفرات وكذا تجاوز جدار الحماية للملفات التي تتضمن المعلومات الخاصة بالعملاء والتي تخزن في الكومبيوتر الرئيسي من خلال الشبكة المعلوماتية.[1]

2_الاستراق أو الصيد:

يعد التصيد الاحتيالي من أكثر الأساليب شيوعا التي يستعملها القراصنة للحصول على البيانات الشخصية والمصرفية، فيرتكز هذا الأسلوب على إنشاء موقع إلكتروني مزيف من مصدر موثوق فيه كمصرف مثلا فيقوم المحتالون بإرسال وصلة إلى موقع الكتروني آخر بغرض الخداع بطلب معلومات شخصية مهمة كالاسم واللقب ورقم الحساب المصرفي وكذا الرقم القومي واسم المستخدم وكلمة المرور من المستهلكين ويقوم ضحايا الاختراق بالرد، وتقديم معلوماتهم دون إدراكهم لعملية الاحتيال حتى يتم تقديمها لاستخدامها بعد ذلك من طرف المحتالين على هذه المعطيات، ليتم استغلالها في القيام بعمليات غير مشروعة مثل الدخول إلى الحسابات المصرفية، أو إجراء عمليات شراء عبر الانترنيت، أو تحويل الأموال بطريقة غير قانونية[2].

3_تقنية تفجير الموقع المستهدف

يعتمد هذا النوع من الأساليب على ضخ كم هائل من الرسائل الالكترونية تصل إلى مئات الآلاف والتي تشكل ضغطا، تنطلق الرسائل من حاسوب المجرم لحاسوب الضحية ويهدف للتأثير على ما يسمى السعة التخزينية، وهو ما ينتج عنه تفجير الموقع العامل على الشبكة وتشتت للمعلومات والبيانات المخزنة

[1] محمد عبد الله العواء، جرائم الأموال عبر الأنترنت، دار الفتح، الإسكندرية، الطبعة الأولى، 2013، ص 29.

[3] سيد على السيد محمد، **مرجع سابق، ص** 39.

[4] حسين طاهري، مرجع سابق، ص 126.

فيه[1]، بعدها تنقل من جهاز الضحية إلى الجهاز الخاص بالمجرم فتمكنه من التجول في الموقع المستهدف بسهولة ويسر والاستحواذ على كل ما يحتاجه إما أرقام أو معلومات وحتى بيانات خاصة بالبطاقات الائتمانية، يعمل المجرم لتوجيه هذا الأسلوب إلى الحواسيب المركزية للبنوك والمؤسسات بتحصيل أكبر عدد كبير من البطاقات الائتمان.[2]

ثانيا: التعدي على التوقيع الالكتروني

التوقيع الإلكتروني هو وسيلة حديثة للتعبير عن إرادة الشخص والتصديق على مضمون المحررات الإلكترونية، فيتمثل في مجموعة من البيانات أو الرموز الرقمية التي توضع في وثيقة إلكترونية بهدف إثبات هوية صاحبها، والتأكيد على موافقته على ما ورد فيها، وعلى غرار التوقيع التقليدي الذي يتم بالإمضاء أو البصمة، يهدف التوقيع الإلكتروني إلى تحقيق نفس الوظيفة القانونية والمتمثلة في إثبات الالتزام بمضمون المحرر[3].

ومنه ظهرت فكرة التوقيع الالكتروني في أنظمة الإثبات نتيجة التطور الكبير في تقنيات المعلومات والاتصال، كما عمل المشرع على تحديد الإطار القانوني لهذا النوع من التوقيع من خلال نصوص تنظيمية تبين شروط صحته وحجيته في الإثبات، حيث تم التمييز بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المؤمن، فيقصد بهذا الأخير ذلك التوقيع الذي يرتبط بصاحبه ويكن تحت سيطرته كما يكشف أي تعديل يطرأ على الوثيقة بعد توقيعها.

جل التشريعات المقارنة أخذت بتعريف التوقيع الالكتروني على انه يمثل التوقيع في علامة شخصية خاصة، يضعها الشخص على مستند بقصد الإقرار به والالتزام بمضمونه، كما أن الجزائر حضت حذو التشريعات المقارنة أين نصت من خلال المادة 327 من القانون المدني على التوقيع الذي حصرته في الإمضاء، وبعدها جاء القانون 10/05 الذي أدرج البصمة كشكل من أشكال التوقيع [4]، و عرفه القانون المدني الفرنسي الصادر ب 13-03-2000، بأنه إجراء ضروري لإتمام التصرف القانوني والذي يميز هوية من وقعه ويعبر عن رضاه بالالتزامات الناشئة عن هذا التصرف، غير أن المشرع الفرنسي قد اشترط استعمال وسيلة آمنة لتسجيل التوقيع الالكتروني، مع تحديد هوية الموقع وضمان صلته بالتصرف الذي

---

[1] سيد علي السيد محمد، مرجع سابق، ص 39

[2] حسين طاهري، **مرجع سابق**، 127.

[3] سيد علي السيد محمد، **مرجع سابق**، ص 60.

[4] يوسف مناصرة، **الدليل الإلكتروني في القانون الجزائي، الطريق إلى تحل أدلة بات في المادة الجزائية، دراسة مقارنة، دار** الخلدونية، 2021، ص 249.

وقع عليه[1] وفي ذات السياق قد أقرت محكمة الفرنسية بمنح الأفضلية للتوقيع الالكتروني عن التوقيع بخط اليد ذلك أنه سهل التزوير والتقليد[2].

في حين يأخذ التوقيع الالكتروني العديد من الصور أهمها **التوقيع الرقمي أو الكودي** الذي يعتمد على استخدام منظومة من الأرقام والرموز المشفرة تنشأ وفق آليات تقنية خاصة، فينتج عنها رمز أو شفرة تثبت هوية صاحب التوقيع، كما يمكن أن يتم التوقيع الالكتروني من خلال **القلم الإلكتروني** أين يقوم الشخص بالكتابة على شاشة الحاسوب باستخدام قلم رقمي مخصص، وذلك عبر برامج معلوماتية تمكن من تسجيل التوقيع وحفظه بصيغة إلكترونية داخل النظام المعلوماتي[3]، ونظرا لتزايد الاعتماد على المعاملات الرقمية، الأمر الذي جعل العديد من التشريعات تعترف بالتوقيع الإلكتروني تمنحه قيمة قانونية في مجال الإثبات مثله مثل التوقيع العادي المكتوب بخط اليد [4].

أما الاعتداء على التوقيع الإلكتروني فيقصد به مختلف الأفعال أو السلوكيات غير المشروعة التي يقوم بها الهاكرز وتهدف إلى المساس بسلامة التوقيع الإلكتروني أو استغلاله بطرق غير مشروعة، سواء من خلال تزويره أو تقليده أو استعماله دون إذن صاحبه أو التلاعب بالبيانات المرتبطة به داخل الأنظمة المعلوماتية، فنجد هذه الأفعال ضمن الاعتداءات التي تمس أمن المعاملات الرقمية تؤثر في الثقة التي يقوم عليها التعامل الإلكتروني كونها تؤدي إلى إلحاق أضرارا بصاحب التوقيع.[5]

ومنه نجد أن الاعتداء على التوقيع الإلكتروني يتخذ عدة صور يمكن ذكرها وفقا للاتي:

أ-أساليب التعدي على التوقيع الالكتروني

مما سبق التطرق إليه يتضح أن التوقيع الالكتروني هو وسيلة حديثة لإثبات هوية الشخص في البيئة الرقمية، حيث يتم إنشاؤه باستخدام تقنيات إلكترونية عوضا عن الأساليب التقليدية، فيقوم هذا التوقيع على مجموعة من الإجراءات التقنية التي تسمح بالتحقق من شخصية صاحب التوقيع تأكيد إرادته في الالتزام بمضمون التصرف القانوني المرتبط بالوثيقة أو المعاملة الإلكترونية ومن الناحية التقنية فهو يعتمد على آليات التشفير الرقمي التي تتكون من رموز أو حروف أو أرقام إلكترونية تنشأ وفق أنظمة معلوماتية خاصة،

---

[1] لائحة التوقيع الالكتروني الصادرة في 08 مارس2002.

[2] حسين طاهري، **مرجع سابق**، ص 131.

[3] هبة مصطفى كافي، **مرجع سابق**، ص 222.

[4] نفس المرجع.

[5] حسين طاهري، **نفس المرجع**،147.

غالبا ما تصدر هذه التوقيعات من جهات مختصة أو هيئات موثوقة معترف بها رسميا على المستوى الحكمي أو دولي، من أجل إضفاء طابع الثقة على المستندات المتبادلة عبر شبكة الإنترنيت، من خلال ربط هوية الشخص الموقع بالوثيقة الإلكترونية وربطها حتى لا يتم التلاعب بمحتواها.[1]

بالرغم من التسهيلات التي يقدمها التوقيع الالكتروني بما يقدمه من خدمات عديدة ومتنوعة خاصة في مجال التعاملات التجارية غير أنه يبقى عرضة للخطر بسبب التعدَّي على هذا التوقيع الالكتروني الذي يتمثل أساسا في ذلك السلوك غير المشروع الذي يستهدف تزوير التوقيع أو استعماله دون إذن صاحبه أو اختراق الأنظمة التي تنشئه أو تحفظه.

ب_ تزوير أو تقليد التوقيع الالكتروني

يقصد به استعمال وسائل تقنية متطورة لاختراق أنظمة التوقيع الإلكتروني أو إنشاء توقيع مزيف ينسب إلى شخص أخر دون علمه، فيقع التزوير الالكتروني أو التقليد الالكتروني على وثائق معلوماتية مخزنة في وثيقة قيد المعالجة فهو وسيلة يعبر بها الشخص عن إرادته في الالتزام بتصرف قانوني معين أي ينصرف إلى العلامة والإشارة التي تسمح بتمييز الشخص الموقع عن غيره.[2]

فيرتبط التوقيع الإلكتروني عادة بوثيقة معلوماتية يتم التعامل معها باستخدام الأجهزة الإلكترونية أين تعتمد على المعالجة الآلية للمعطيات، وقد تكون هذه الوثيقة مهيأة أو مبرمجة داخل نظام معلوماتي أو مجرد بيانات رقمية يتم تخزينها أو تبادلها عير الوسائط الإلكترونية، وفي كلتا الحالتين فان الاعتداء عليها من خلال تقييد التوقيع الإلكتروني أو التلاعب به يعد صورة من صور التزوير في المحررات الإلكترونية.

من هذا المنطلق يعتبر تزوير أو تقليد التوقيع الإلكتروني من أهم صور الاعتداء التي يمكن أن تمس المعاملات الرقمية، إذ يقوم هذا الفعل على تحريف الحقيقة أو تغييرها بقصد الغش في محرر أو وثيقة، مما يؤدي إلى إلحاق أضرار بالمصلحة العامة أو الخاصة، فينصب على وثائق وبيانات من طبيعة معلوماتية يتم تداولها عبر الأنظمة المعلوماتية.

---

[1] علي أبو مارية، **التوقيع الإلكتروني مدى قوته في الإثبات**، دراسة مقارنة، مجلة الخليل للبحوث، المجلد 5، العدد 2، 2010، ص110.

[2] نقض مدني،28 يناير 1982، **مجموعة أحكام النقض المصرية** ص33، ق664، ص 10328، نقلا عن عيسى سليم 3 داود الزيدي، مرجع سابق، ص156.

من أبرز الأساليب التي قد تستعمل في هذا المجال استخدام بعض البرامج الحاسوبية أو أدوات الاختراق المصممة للتعامل مع الأنظمة المعلوماتية، بحيث يسعى المخترق إلى الوصول إلى الرموز أو المفاتيح الرقمية المرتبطة بالتوقيع الإلكتروني، ثم نسخها أو إعادة استعمالها بطريقة غير مشروعة بما يوهم بأن التوقيع صادر عن صاحبه الحقيقي[1]

ج-الدخول غير المشروع إلى بيانات تتعلق بالتوقيع الالكتروني

يعتبر الولوج غير المصرح به إلى البيانات المرتبطة بالتوقيع الإلكتروني من أخطر صور الاعتداء الواقعة عليه، فيتمثل أساسا في قيام شخص بالدخول إلى المعلومات أو الأنظمة التي تتضمن معطيات التوقيع الإلكتروني دون امتلاك سند قانوني أو إذن مشروع.[2]

فيعد الدخل غير المشروع سلوكا من سلوكيات الاختراق المعلوماتي، وقد يكون وسيلة للاعتداء على التوقيع الإلكتروني أو البيانات التجارية

ويتمثل في قيام الجاني بالدخول أو محاولة الدخول إلى نظام معلماتي أو قاعدة بيانات تحتوي على معلومات مرتبطة بالتوقيع الإلكتروني دون ترخيص أو إذن من صاحبها الحقيقي[3] فيشمل ذلك الوصول إلى البيانات المخزنة داخل الأنظمة أو الشبكات المعلوماتية، بغض النظر عما إذا كان الهدف مجرد الاطلاع عليها أو نسخها أ تعديلها أو اعتراضها.[4]

في حين ان الركن المعنوي على اعتبار أن هذه الجريمة هي جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي العام بعنصريه (العلم والإرادة)، أي علم الجاني بأنه يدخل إلى نظام معلوماتي لاختراق بياناته، مع اتجاه إرادته إلى القيام بهذا الفعل المجرم قانونا، فيتحقق القصد الجنائي متى كان الجاني مدركا لطبيعة البيانات المرتبطة بالتوقيع الإلكتروني وأهمية حمايتها، ويقوم عمدا بالوصول إليها واستغلالها.[5]

---

[1] سليمان أيمن، عبد الحفيظ عبد الحميد، **استراتيجية مكافحة الجرائم الناشئة عن استخدام الإنترنيت**، رسالة دكتورا، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، (بدون سنة)، ص 287_289.

[2] حسين طاهري، **مرجع سابق**، ص 149.148.

[3] غنية باطلي، مرجع سابق، ص 151.

[4] حسين بن سعيد الغافري، **السياسة الجنائية في مواجهة جرائم الإنترنيت**، دار النهضة العربية، القاهرة،2009، ص 291.

[5] حسين طاهري، **مرجع سابق**، ص 149.

ثالثا: قرصنة العلامة التجارية

تعد العلامة التجارية من أهم وسائل التمييز بين المنتجات والخدمات في النشاط الاقتصادي، إذ تمكن المستهلك من التعرف على مصدر السلعة أو الخدمة وتمييزها عن غيرها من السلع المماثلة في السوق، و تعد العلامة التجارية قيم اقتصاديه معنوية للمؤسسة، نظرا لما تملكه من شهرة لدى الجمهور، وفي هذا الجانب أشار المؤلف شريف محمد غانم في كتابه حماية العلامات التجارية عبر شبكة الإنترنت من الاعتداء عليها من العنوان الإلكتروني إلى أن العلامة التجارية تمثل وسيلة أساسية لتمييز المنتجات والخدمات، كما تؤدي دورا مهما في حماية المستهلك من الخلط بين المنتجات المتشابهة[1].

ويقصد بها قيام بعض القراصنة باستغلال العلامة التجارية المملوكة للغير في الفضاء الإلكتروني دون إذن صاحبها، خاصة من خلال تسجيل العناوين الإلكترونية للمواقع المرتبطة بالعلامات التجارية من أجل الاستفادة من شهرتها أو تحقيق مكاسب مالية غير مشروعة، وقد أشار المؤلف إلى هذه الممارسات مبينا" **تسجيل اسم نطاق يتطابق مع علامة تجارية مملوكة للغير قد يؤدي إلى خلق لبس لدى المستخدمين حول هوية صاحب الموقع الإلكتروني** ".

وعليه فان قرصنة العلامة التجارية عبر شبكة الإنترنت لا تمثل مجرد وسيلة استعمال غير مشروع لعلامة مملوكة للغير، بل قد تشكل أيضا اعتداءات على الوظيفة الأساسية للعلامة التجارية المتمثلة في تمييز المنتجات الخدمات، ناهيك عن إمكانية تضليل المستهلكين وإلحاق الضرر بالمصالح الاقتصادية لأصحاب العلامة[2].

أ: مفهوم العلامة التجارية

المقصود بقرصنة العلامة التجارية: بأنه تسجيل اسم موقع الكتروني بشكل قانوني لدى الجهات المختصة، من طرف بعض الأشخاص أو الشركات بحيث يتضمن اسم الموقع الالكتروني اعتداء على علامة تجارية قائمة مسجلة باسم شخص أو شركة أخرى وذلك بقصد الإضرار بمالك العلامة أو بقصد إعادة بيع اسم الموقع الإلكتروني إلى المالك الأصلي للعلامة بسعر مبالغ فيه، فتظهر هنا سوء نية مسجل

[1] شريف محمد غانم، **حماية العلامة التجارية عبر شبكة الإنترنت من الاعتداء عليها من العنوان الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، مصر ،2016، ص 109.

[2] شريف محمد غانم، نفس المرجع، ص 107

اسم الموقع الإلكتروني الذي يسعى إلى تحقيق الربح المادي جراء منع مالك العلامة التجارية من تسجيل هذا العنوان، ومن ثمة إعادة بيعه إليه أو بيعه لأحد منافسيه[1].

ومن هذا المنطلق تظهر القرصنة الإلكترونية كأحد أخطر التهديدات التي تواجه التجارة الالكترونية، حيث يقوم بعض القراصنة باستغلال الثغرات الأمنية في الأنظمة المعلوماتية أو في مواقع التجارة الإلكترونية بهدف الاستيلاء على البيانات المالية أو معلومات بطاقات الدفع الالكتروني الخاصة بالمستخدمين، قد يتم عن طريق استخدام عدة وسائل تقنية، مثل إنشاء مواقع وهمية تحاكي المواقع التجارية الأصلية، أو إرسال رسائل احتيالية تهدف إلى الحصول على المعلومات السرية للعملاء، أو اختراق قواعد البيانات الخاصة بالمؤسسات التجارية[2]، أيضا ورد عن منظمة التجارة العالمية، تعريف لها بأنها: "مجموعة متكاملة من عمليات عقد الصفقات وتأسيس الروابط التجارية وتوزيع وتسويق وبيع المنتجات عبر وسائل الكترونية"[3].

بعد التدقيق في تعريفات التجارة الالكترونية نرى بأنها ترتبط بالاتصال المباشر بشبكة الانترنت الأمر الذي يتركها عُرضة للجرائم المعلوماتية على رأسها القرصنة الالكترونية،

التسجيل وحرمانهم ميزات الاستفادة من عالمته التجارية عبر شبكة الإنترنت.[4]

ب: أسلوب الاعتداء على العلامة التجارية

نتيجة توسع النشاط التجاري عبر شبكة الإنترنيت، انتشرت ظاهرة الاعتداء على العلامات التجارية في الفضاء الرقمي ومن أبرز العوامل التي ساعدت على انتشار هذه الاعتداءات التي ترتب عليها منذ البداية قيام أصحاب العلامات التجارية بدفع مبالغ مالية لمسجلي العناوين وذلك بقصد الحصول على أسماء المواقع الإلكترونية التي تخصهم، فتظهر جليا صور الاعتداء على العلامة التجارية من خلال:

1-تسجيل مواقع إلكترونية تحمل نفس العلامة التجارية

أي قيام شخص بتسجيل موقع الكتروني باسم علامة تجارية معروفة قبل صاحبها الحقيقي مما يؤدي ذلك إلى حرمانه من استعمالها في الإنترنت.

---

[1] هبة مصطفى كافي، مرجع سابق، ص 205

[2] حسين طاهري، القرصنة الإلكترونية، مرجع سابق، ص 119.

[3] نفس المرجع.

[4] شريف محمد غنام، **مرجع سابق**، ص115.

2-إحداث اللبس أو التظليل لدى المستهلكين:

حيث يؤدي استعمال العلامة في البيئة الرقمية بطريقة غير مشروعة إلى الاعتقاد بوجود علاقة بين الموقع وصاحب العلامة الأصلي[1].

3-استغلال شهرة العلامة التجارية في المواقع الإلكترونية:

وذلك باستعمال العلامة أو ما يشابهها في موقع إلكتروني لجذب المستخدمين أو الترويج لمنتجات لا علاقة لها بصاحب العلامة.

4-الاستفادة المادية غير المشروعة من العلامة التجارية:

كطلب مبالغ مالية مقابل التنازل عن الموقع المسجل باسم العلامة أو استغلاله في نشاط تجاري غير مشروع.[2]

ولقد كان المشرع الأمريكي السباق في مواجهة ظاهرة القرصنة الإلكترونية لما تسببه من خسائر للمستهلكين والمشروعات وذلك من خلال إصداره لقانون جديد يسمى قانون حماية المستهلك من القرصنة الإلكترونية صدر في الولايات المتحدة الأمريكية في 29 نوفمبر 1999، كما كان للقضاء دور كبير في إدانة القرصنة الإلكترونية وذلك من خلال حكمه على مرتكبي هذه الممارسات غير المشروعة بتحويل أسماء المواقع الإلكترونية لأصحابها الشرعيين والتعويض لهم عند الاقتضاء لما لها من انتهاك لحقوق الآخرين في علاماتهم التجارية، وكذا التضليل الذي يقع فيه مستخدمي شبكة الإنترنت[3]،

كون معظم الاعتداءات هنا تتم عبر استخدام غير مشروع للعلامة التجارية في المجال الرقمي وليس عبر الدخول غير المشروع إلى أنظمة المعلومات.

المطلب الثاني: انعكاسات القرصنة الالكترونية

تعتبر القرصنة الإلكترونية أحد التحديات المعاصرة التي تواجه الاقتصاديات الحديثة، إذ لم يعد تأثيرها مقتصرا على الجانب التقني فقط، وإنما امتد ليشمل الأبعاد الاقتصادية و المالية للدول، فالهجمات المعلوماتية التي تستهدف الأنظمة الرقمية للمؤسسات والشركات قد تؤدي إلى تعطيل الخدمات الإلكترونية أو الاستيلاء

---

[1] لواعر فاطمة، بوهنتالة إبراهيم، **الاعتداء على العلامة التجارية في المجال الإلكتروني**، المجلة العربية للعلوم القانونية، العدد 12، 2019 ص 87-101

[2] لواعر فاطمة، بوهنتالة إبراهيم، **نفس المرجع**، ص101.

[3] Anti-Cyber squatting Consumer Protection Act (ACPA) , 1999

على البيانات والموارد المعلوماتية، وهو ما يخلف أثارا تتمثل في خسائر مالية مباشرة نتيجة توقف النشاط أو تكاليف إصلاح الأنظمة المتضررة،[1] كما يمكن لهذه الاعتداءات التأثير بصورة مباشرة على تكاليف إصلاح هاته الأنظمة الفاسدة، ولا يتوقف الأمر عند هذا القدر من الخسائر وإنما يمكن لهذه الاعتداءات التأثير بصورة غير مباشرة على مناخ الاستثمار، بحيث يؤدي ذلك إلى فقدان الثقة في أمن المعاملات الرقمية ومنه تردد المستثمرين في توسيع أنشطتهم في القطاعات المرتبطة بالاقتصاد الرقمي، وبالتالي فان انتشار ظاهرة القرصنة الإلكترونية يشكل عامل ضغط على الاقتصاد الوطني، لما تسببه من إضعاف البنية المعلوماتية وتعطيل لمظاهر التطور الاقتصادي المرتبطة بالتكنولوجيا الحديثة[2].

تخلف القرصنة الإلكترونية آثاراً متعددة وخطيرة، لا تقتصر على الجانب التقني فقط، بل تمتد لتشمل الجانب الاقتصادي إذ تسبب خسائر مالية فادحة للأفراد والمؤسسات، وتعطيل الأنظمة المعلوماتية وكذا المساس بالخصوصية من خلال سرقة البيانات الشخصية والحساسة، كما تؤدي إلى الإضرار بالسمعة. وتمتد آثارها لتشمل تعطيل الأنشطة الحيوية للشركات والبنية التحتية، ونشر البرامج الضارة وعمليات الاحتيال الإلكتروني، وقد تتطور هذه النتائج في بعض الحالات إلى حد تهديد الاستقرارين الاقتصادي والسياسي للدول.

تمثل القرصنة الإلكترونية تهديدا حقيقيا ومستمرا للأمن المعلوماتي في الأنظمة الرقمية، حيث يؤثر ذلك سلبا على قدرة المؤسسات والأفراد على حماية البيانات الحساسة والتحكم فيها، فتشير الدراسات الحديثة إلى أن مثل هذه الاعتداءات قد تؤدي إلى فقدان الخصوصية، وإتلاف أو تعديل المعلومات المخزنة، كما تؤدي كذلك إلى تعطيل الخدمات الإلكترونية، وهو ما يسبب الكثير من المخاطر و الضغوطات على إدارة الأمن المعلوماتي، من هذا المنطلق، يشدد الباحثون على ضرورة اعتماد استراتيجيات فعالة لتعزيز الأمن الرقمي ومواجهة أساليب القرصنة الحديثة، بما يضمن الحد من أثارها الضارة على الأنظمة المعلوماتية وحماية البيانات من الاختراق أو التلاعب.[3]

من حيث التطرق إلى القوانين الإلكترونية، يظهر الفرق بين النتائج المباشرة للتشريع وهو ما تم التطرق إليه من خلال التعريج على أثار القرصنة والأثر الذي يحدثه على سلوك المجتمع والمؤسسات، وهنا يختلف

---

[1] عبد الرحمن خليفي، **الحماية الجنائية لحقوق الملكية الفكرية**، دار هومة، 2018، ص 112.

[2] ينظر: أشرف السعيد أحمد، **مرجع سابق**، ص26.

[3] بالطة مريم اسيا برغيث،" **الأمن المعلوماتي في مواجهة القرصنة الإلكترونية** "، مجلة دراسات في الحقوق الإنسان، المجلد 6، العدد 1، 2022، ص 11-24.

رأي الفقهاء، نجد أن بعضهم ركزوا على الجوانب القانونية والتنظيمية للتشريعات، مؤكدين أهمية وضوح النصوص وتحديد العقوبات والإجراءات، بينما ركز آخرون على البعد العملي، من خلال الإشارة إلى أن قوة ونجاعة القانون تعتمد على تأثيره في حماية البيانات من خلال الالتزام بالإجراءات الصحيحة. وبجمع هذين الرأيين يتضح أن دراسة أثار القرصنة الإلكترونية يجب أن يشمل كلا من النتائج القانونية المباشرة والتأثير الفعلي على الأفراد والمؤسسات، مما يعكس صورة متكاملة لقدرة التشريع على مكافحة جريمة القرصنة الإلكترونية وتعزيز الأمن المعلوماتي.[1]

الفرع الأول: الانعكاسات الاقتصادية للقرصنة الالكترونية

نظرا لما للقرصنة الالكترونية من تأثيرات كثيرة على الدول وأمنها واقتصادها وسيادتها، فان ارتكابها يؤدي إلى تهديد الأمن المعلوماتي للدول والمؤسسات، بسبب قيام القراصنة باختراق الأنظمة المعلوماتية الحساسة للوصول إلى البيانات السرية من اجل التلاعب بها أو تعطيلها، فتنتج أثارا مباشرة تتمثل في خسائر مالية، تسريب بيانات وتعطيل الأنظمة.

لا يقتصر خطر القرصنة الإلكترونية على ما تحدثه من أثار مباشرة، كخسارة البيانات أو الأموال، بل يتجاوز ذلك إلى إحداث تأثيرات استراتيجية عميقة تمس كيان الدولة واستقرارها.[2]

وهو ما سنتطرق من خلال هذه العناصر للتفصيل فيها:

أولا: آثار القرصنة الالكترونية على الاقتصاد الوطني

تنتج القرصنة الالكترونية على الاقتصاد الوطني والذي ينجم عنه ارتكاب جرائم القرصنة إذ تعيش الشركات التجارية الكبرى حربا الكترونية فيما بينها وعددا من الشركات، تتعرض للعديد من محاولات الاختراق لمواقعها كل يوم بغرض الحصول على معلومات وبيعها للشركات المنافسة.[3]

بمرور السنوات ازداد حجم الخسائر الناتجة عن القرصنة الالكترونية وخاصة في الدول التي تعتمد على نظم المعلوماتية وهذه الوقائع تقتضي ضرورة مواجهة جادة لهذه الجرائم ومكافحتها، إلا أن الصعوبة

---

[1] مريم بالطا،أسيا برغيت، **مرجع سابق**.

[2] محمد علي محمد التوني، استراتيجية مكافحة الهجمات السيبيرانية، دار الفكر الجامعي، الإسكندرية، 2023، ص 246.

[3] أشرف السعيد أحمد، **مرجع سابق**.

تكمن في وضع رقم محدد وواضح المعالم لحجم الخسائر في مجال الجرائم المتعلقة بالقرصنة وهو ما يعبر عنه بالرقم الأسود[1].

ثانيا: زيادة الاعباء المالية على الدولة

وذلك بتخصيص أعباء إضافية لمكافحة الجرائم الالكترونية وتموين أجهزة التحري والتحقيق والتكوين المتخصص وكذا تطوير البنى التحتية الرقمية، يؤكد الخبراء الاقتصاديون أن المنطقة العربية ستتعرض إلى أزمة خطيرة في السنوات القادمة القليلة بسبب الإحجام عن استخدام الشيكات لتفعيل التجارة الالكترونية بين الدول العربية والدول المتقدمة وهو ما لم يكن وليد الصدفة فقد ساهمت جرائم القرصنة الالكترونية وانتشار أشكالها خاصة مع تكرار سرقة بطاقات الائتمان في إضفاء حالة من الرعب على المؤسسات العربية الضخمة بدلا من معالجة الأخطاء وتفعيل القوانين ووسائل الحماية القانونية والوقاية[2].

الفرع الثاني: الانعكاسات السياسية والقانونية للقرصنة الالكترونية

لم تعد الحروب تدار فقط بالأسلحة، بل بالمعلومات، فأصبحت القرصنة الإلكترونية الوسيلة الأساسية في الحروب السيبيرانية، التي تحولت إلى إحدى أدوات التأثير في المعلومات المستخدمة في مستويات ومراحل القتال الإلكتروني والصراع المختلفة، سواء على الصعيد الاستراتيجي أو التكتيكي المعلوماتي بهدف التأثير بشكل سلبي على هذه المعلومات ونظم عملها[3].

أولا: تأثير القرصنة الالكترونية على سيادة الدول وعلى الامن القومي

مما يميز الجريمة الالكترونية أنها جريمة من الجرائم العابرة للحدود الجغرافية، وقد سعت الدول في الطريق لسيادتها واستقلالها لسن القوانين والتشريعات التي تعمل للحد من القرصنة الالكترونية، فقد أظهرت التشريعات الراهنة عجزا وقصورا في مواجهة هذه الجرائم، ومثال ذلك جريمة سرقة الأموال وتحويلها عبر الإنترنت وسرقة البنوك وبطاقات الائتمان من دون الحاجة للسطو الفعلي على البنك. وتجدر الإشارة هنا أنه يمكن ارتكاب جريمة القرصنة من خلال حاسب آلي متصل بشبكة الإنترنت في دولة ما وتتحقق نتيجة هذا الفعل الإجرامي في دولة أخرى[4]

---

[1] يُقصد **بالرقم الأسود** أنه يشير إلى عدم التبليغ عن جرائم القرصنة الالكترونية مما يخفي الرقم الحقيقي لها ويقلل الشعور بخطورتها مما يرفع من نسبتها.

[2] حسين طاهري، **مرجع سابق**، ص .39

[2] المقدم كحل محند أكلي، **الأمن السيبيراني في الفضاء العسكري**، مجلة الميزان ، مجلة دورية صادرة عن مديرية القضاء العسكري بوزارة الدفاع الوطني الجزائرية، العدد الثالث، جويلية 2023، ص 40.

[4] مصطفى عثمان إسماعيل، **الأمن القومي العربي**، دار مدبولي للنشر، القاهرة، 2009، ص20.

أ_ تأثير القرصنة الالكترونية على سيادة الدول

شهدت الدول تراجعا لسيادتها وتناقصت استقلالية قراراتها فأصبحت تصدر بالمشاركة بين السلطات الوطنية وغيرها من السلطات الخارجية مثل المنظمات الدولية.[1]

ففي عالم مترابط رقميا، لم تعد الهجمات الإلكترونية تقتصر على سرقة المعلمات أو تعطيل الخدمات البسيطة، بل تجاوزت ذلك إلى نشاطات متطورة تستهدف القدرات التكنولوجية للدول ذاتها، بما في ذلك الشبكات الحيوية، قواعد البيانات الحكومية، والمنظومات الأمنية الوطنية، هذا التطور يعكس تطور القراصنة من فاعليين فرديين إلى جهات ذات قدرات تقنية مقعدة، بعضها يتصف بارتباطه بالاستخبارات أو بالدول، مما يجعل أفعالهم مؤثرة على الأمن سيادة الدولة بشكل مباشر.

بحيث تكون جريمة القرصنة الالكترونية ماسة لسيادة الدولة تؤدي الى تعطيل الأعمال الحكومية وتنفيذ القوانين والإخفاق في الإبلاغ عن الجرائم المعلوماتية والحصول على معلومات سرية والإرهاب الإلكتروني، ومع انتهاء عصر العزلة وانتشار فكرة العولمة، من أخطر الصور والأشد تأثيرا على أمن الدولة هو الإعتداء على الأنظمة المعلوماتية عن طريق تدمير البيانات والمعلومات الخاصة بها.

ب: تأثير جريمة القرصنة الالكترونية على الأمن القومي

كما يعرف الأمن القومي على أنه "حماية الأمة من خطر القهر على يد قوة أجنبية، وقد صرح وزير الدفّاع الأمريكي السابق بأن الأمن الحقيقي للدولة ينبع من معرفتها العميقة للمصادر التي تهدد مختلف قُدراتها ومواجهتها بهدف إعطاء الفرصة لتنمية تلك القدرات تنمية حقيقية في كل المجالات سواء الحاضر أو المستقبل. حيث أن الأمن القومي هو الركيزة الأساسية في استقرار المجتمع،[2]

ثانيا: انعكاسات القرصنة الالكترونية على الملكية الفكرية

ولد تأخر استخدام تقنيات الكمبيوتر وبصفة خاصة في دول العالم العربي مقارنة بباقي دول العالم الأثر الكبير لتأخر إصدار تشريع يخص توفير حماية قانونية لبرامج الحاسوب من السرقة والاختراق، غير

[1] حسين طاهري، **مرجع سابق**، ص 46.

[2] محمود مدين عبد الرحمان، **مرج سابق**، ص92.

أن أغلب الدول العربية اهتمت اهتماما كبيرا بقوانين الحماية الفكرية حتى أن بعضها قد ساهم وبشكل كبير في الجهد الدولي بهدف حماية الملكية الفكرية.[1]

فالقرصنة الإلكترونية التي تستهدف البرمجيات، قواعد البيانات، المصنفات الأدبية والفنية، والابتكارات التقنية، وقد أدرك المجتمع الدولي منذ عقود الحاجة إلى وضع معايير واتفاقيات دولية تحمي الحقوق الفكرية عبر الفضاء السيبيراني، بما يضمن مكافحة الاستخدام غير المشروع للمعلومات والمواد المحمية.

في ظل اهتمام المجتمع الدولي بمكافحة الجريمة الالكترونية صدرت العديد من الاتفاقيات نذكر منها:

أ-اتفاقية بودابست لمكافحة الإجرام المعلوماتي:

من أهم هذه الاتفاقيات الرائدة، اتفاقية بودابست لمكافحة الجريمة السيبرانية(2001) جاءت في الباب الرابع من القسم الأول من الفصل الثاني المتعلق بالقرصنة الالكترونية من خلال الجرائم المتعلقة بانتهاكات حق المؤلف والنشر والحقوق المجاورة، حيث قامت بوضع جملة من الإجراءات والتدابير الوقائية التي تؤكد على حق المؤلف من كل شكل من أشكال الانتهاكات بما فيها الإجراءات التي نصت عليها الاتفاقيات السابقة،2 كما تعتبر الإطار الأول الذي ضع حدودا قانونية للأفعال المستهدفة لأنظمة المعلومات، بما في ذلك الاعتداء على حقوق الملكية الفكرية الرقمية، فتنص الاتفاقية على ضرورة تجريم أي استخدام غير قانوني للحواسيب أو الشبكات الرقمية بهدف نسخ أو تعديل وتوزيع المواد المحمية دون إذن أصحابها، كما تشجع على التعاون الدولي في التحقيق وتبادل الأدلة الرقمية.[3]

تكونت اتفاقية بودابست من 48 مادة تلح على واجب اتخاذ كامل الإجراءات وإنشاء القوانين لمحاربة الجريمة الإلكترونية مما اعتبرت هذه المعاهدة مرجعا هاما، لتأكيده على عناصر أساسية تمثلت في تعزيز

---

[1] **المنظمة العالمية للمكية الفكرية للويبو**، التقرير العالمي للملكية الفكرية، تلعب المنظمة دورا محوريا في تنظيم وحماية حقوق الملكية الفكرية على المستوى الدولي، من خلال وضع المعايير القانونية، وتقديم الخدمات المتعلقة بتسجيل الحقوق، وإصدار تقارير عالمية تعكس واقع الابتكار والتنمية، كما تؤكد تقاريرها أن الملكية الفكرية تمثل أداة أساسية لدعم الاقتصاد الرقمي وتعزيز الإبداع.

https://www.wipo.int/ar/web/world-ip-report، 2024، بتاريخ 2025/10/17، 12.00س.

[2] تم توقيع الاتفاقية في عاصمة المجر بودابست عام 2001 بحضور 26 دولة إضافة إلى كندا واليابان وجنوب إفريقيا وتم إقرارها بعد 4 سنوات من المفاوضات.

[3] طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي، النظام القانوني لحماية المعلوماتي**، دار الجامعة الجديدة للنشر، 2009، ص 232.

أهمية القوانين المقننة في تحديد الجريمة المعلوماتية، بالإضافة إلى التدابير الإجرائية وكذا تدابير التعاون الدولي في نفس المجال.[1]

ب-اتفاقيات الويبو للإنترنت بشأن حق المؤلف:

معاهدة الويبو بشأن حقوق المؤلف هي اتفاق خاص في إطار اتفاقية برن وتتناول حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية.

جاء في فحوى الاتفاقية أن الأطراف المتعاقدة حتى وإن لم يكن ملزم باتفاق برن ملزم بأن يمتثل للأحكام الموضوعية الواردة في وثيقة 1971 (باريس) لاتفاقية برن.

بشأن حماية المصنفات الأدبية والفنية لسنة 1886، وللإشارة فان الاتفاقية تم صياغة نصوصها لتستوعب كل الصور المستحدثة للاعتداء على المصنفات الرقمية المنشورة عبر الانترنت مثل القرصنة الالكترونية والنشر الالكتروني الغير مرخص به.

وقد اقترحت الاتفاقية كحل للحد من القرصنة الالكترونية ضرورة تبني نظام التسيير الالكتروني لحقوق المؤلف الذي يمكن المؤلف من التحكم في جميع نسخ المصنف عند نشرها على منصة الانترنت بحيث يمنع الغير من استخدامها إلا بترخيص منه.[2]

ج_ قانون SOPA

يعرف قانون Stop Online Piracy Act بأنه مشروع قانون طرح داخل الكونغرس الأمريكي بهدف الحد من القرصنة عبر الإنترنت، يقوم هذا المشروع على منح السلطات صلاحيات واسعة للتعامل مع المواقع التي يُشتبه في انتهاكها لحقوق المؤلف أو تسهيلها لعمليات القرصنة، حيث يمكن حجب هذه المواقع أو تقييد الوصول إليها، كما قد يتعرض القائمون عليها لإجراءات قانونية قد تصل إلى الغرامة أو العقوبة السالبة للحرية.

غير أن هذا التوجه لم يحظَ بإجماع، إذ واجه معارضة قوية من عدد كبير من شركات التكنولوجيا العالمية مثل **Google** و **Facebook**و **Twitter** و **Mozilla**و **Wikipedia.** وقد عبّرت هذه الجهات عن

---

[1] بدري فيصل، **مرجع سابق**، ص 29.

[2] معاهدة الويبو المتعلقة بحقوق المؤلف، بشأن حق المؤلف، هي اتفاق خاص في إطار بورن وتتناول حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، وفضلا عن الحقوق المنصوص عليها في اتفاقية برن، تمنح هذه المعاهدة بعض الحقوق الاقتصادية للمؤلفين، وتتناول المعاهدة أيضا موضوعين يتعين حمايتهما بموجب حق المؤلف وهما:"1" برامج الحاسوب، أيا كانت طريقة التعبير عنها أو شكلها، "2" ومجموعات البيانات أو المواد الأخرى "قواعد البيانات".

تخوفها من أن يؤدي تطبيق مثل هذا القانون إلى فرض نوع من الرقابة على الإنترنت، بما قد ينعكس سلبًا على حرية التعبير وتداول المعلومات.

ويستند هذا الرفض إلى فكرة أن مكافحة القرصنة، رغم أهميتها، لا ينبغي أن تكون على حساب المبادئ الأساسية التي يقوم عليها الفضاء الرقمي، خاصة ما يتعلق بحرية الوصول إلى المحتوى وتداوله. لذلك، يرى بعض المنتقدين أن هذا القانون لا يقتصر فقط على حماية الحقوق الفكرية، بل قد يمتد أثره إلى توسيع نفوذ الرقابة على الشبكة العالمية [1].

ثالثا: الاستراتيجية الجزائرية في مواجهة القرصنة الالكترونية في مجال الفكرية الوطنية

مع تفشي ظاهرة القرصنة الالكترونية بادرت الجزائر بسن مجموعة من القوانين كان على رأسها القانون 09-04، والذي وضعت قواعده للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وطرق مكافحتها، كما أعطى تعريفا للمصطلحات التي تصب في خانة الجرائم المتعلقة بأمن المعلومات، ومن أبرز المجالات التي مستها القرصنة الالكترونية في الجزائر الملكية الفكرية التي تعتبر حقا ماليا قائما بذاته، يرد على نتاج الفكر الإنساني بمختلف أشكاله، مثل برامج الحاسوب، ومحركات البحث، إضافة إلى المصنفات الأدبية والعلمية التي تشمل الكتب، والمقالات، والوثائق، والصور، والخرائط. كما تمتد لتشمل المصنفات السمعية والبصرية، كالأفلام والموسيقى والمحتويات الرقمية المتاحة عبر الوسائط الحديثة[2].

وتتميز هذه الحقوق بكونها أموالًا غير مادية، إلا أنها تتمتع بقيمة اقتصادية كبيرة، بالنظر إلى ما تؤديه من دور في دعم الابتكار والإبداع وتداول المعرفة. ومن ثم، لم تعد الحماية القانونية المقررة لها تقتصر على صون الجانب المعنوي للمصنف، وإنما امتدت كذلك إلى حماية المصالح المالية المرتبطة باستغلاله، ولا سيما مع اتساع استخدام الوسائل الرقمية في إنتاج المصنفات وتداولها,

وفي هذا الإطار، أولى المشرع الجزائري أهمية خاصة لحقوق المؤلف والحقوق المجاورة، من خلال الأمر رقم 03-05 المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، حيث أقر حماية للمصنفات الفكرية بمختلف أنواعها، متى توافرت فيها الشروط القانونية للحماية، بصرف النظر عن شكلها أو الوسيلة التي تم من خلالها تثبيتها أو إتاحتها للجمهور. كما أكدت المادة 12 من الأمر ذاته

[1] بشرى حسين الحمداني، **مرجع سابق**، 245

[2] حسين طاهري، الجرائم الإلكترونية، **مرجع سابق**، 54.

تمتع المؤلف بحقوق معنوية على مصنفه، بما يضمن له حق نسبة المصنف إليه وحمايته من كل اعتداء يمس سلامته أو شخصيته الفكرية.

وتكتسي هذه الحماية أهمية خاصة بالنسبة للبرامج المعلوماتية، التي أصبحت من أكثر المصنفات عرضة للاعتداء في البيئة الرقمية، لسهولة نسخها وإعادة إنتاجها وتداولها دون إذن صاحب الحق. ومن أبرز صور هذا الاعتداء استعمال البرامج بصورة غير مشروعة أو تداول نسخ غير مرخصة منها، وهو ما يجعل القرصنة البرمجية صورة من صور المساس بالمصالح التي أحاطها المشرع بالحماية القانونية

ولا تقتصر آثار استعمال البرامج المقرصنة على الإضرار بالحقوق المالية لأصحابها، بل قد تمتد إلى المساس بأمن الأنظمة المعلوماتية ذاتها، خاصة عندما تكون تلك البرامج معدلة أو مجهولة المصدر أو غير قابلة للتحديث بصورة سليمة. وفي هذا السياق، أشار مركز البحث في الإعلام العلمي والتقني (CERIST) إلى انتشار استعمال البرامج المقرصنة في الجزائر، بما في ذلك أنظمة التشغيل وبعض البرمجيات المستخدمة على نطاق واسع، وربط ذلك، من بين عوامل أخرى، بضعف الوعي بأهمية الأمن المعلوماتي وبالمخاطر التي قد تنشأ عن استخدام برمجيات غير موثوقة[1]

ويُستفاد من ذلك أن مواجهة القرصنة البرمجية لا ينبغي أن تنحصر في حماية حقوق المؤلف والحقوق المالية المرتبطة بالمصنف، وإنما تقتضي كذلك مراعاة ما قد يترتب عن استعمال البرمجيات غير الموثوقة من مخاطر تقنية وأمنية؛ الأمر الذي يبرز الطابع المتعدد الأبعاد للاعتداءات المرتبطة بالبرمجيات في البيئة الرقمية[2].

1 المادة 12 من الأمر رقم 03-05 المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

[2] بشرى حسين الحمداني، مرجع سابق، ص 200_201.

خاتمة الفصل الأول:

في ختام هذا الفصل، يتضح أن جريمة القرصنة الإلكترونية تمثل إحدى أخطر صور الإجرام المستحدثة التي برزت مع التطور السريع لتقنيات الاتصال ونظم المعلومات، حيث استدعت هذه الجريمة تأطيرا مفاهيميا دقيقا يبرز أهميتها وخصوصيتها مقارنة بالجرائم التقليدية، فقد تم الوقوف على مفهوم القرصنة الالكترونية وبيان خصائصها، التي تتسم بالطابع التقني، واللامادية، وسهولة ارتكابها وصعوبة اكتشافها والتي أصبحت تستهدف المعطيات والأنظمة المعلوماتية بطرق غير مشروعة، سواء عبر الولوج غير المصرح به أو نسخ أو تعديل أو إتلاف البيانات الرقمية.

فمن حيث **التعريف**، يمكن اعتبار القرصنة الإلكترونية هي كل فعل غير مشروع يهدف إلى اختراق الأنظمة المعلوماتية أو الاستيلاء على محتوياتها أو تعطيلها، بما يحقق مصلحة شخصية أو إضرارًا بالغير، دون إذن من صاحب النظام أو البيانات

أما خصائصها، فهي تتميز بعدة سمات أهمها

*أنها جريمة غير مادية تعتمد على الوسائل التقنية الحديثة.

*أنها جريمة ذات طابع عابر للحدود، مما يصعب تتبع الجناة.

*أنها جريمة تقوم على عنصر السرية صعبة الكشف

*أنها جريمة تتسم بالسرعة في التنفيذ وسهولة الإخفاء

* أنها جريمة تستهدف معطيات رقمية غير ملموسة لكنها ذات قيمة قانونية واقتصادية كبيرة.

كما تم التطرق إلى الطرق والاساليب التي يتم من خلالها ارتكاب هذه الأفعال المجرمة،

وخلاصة القول، فإن الإحاطة بهذه الجوانب مجتمعة تشكل أساسا ضروريا لفهم الإطار القانوني لجريمة القرصنة الإلكترونية.

الفصل الثاني

الإطار القانوني لجريمة القرصنة الإلكترونية

لم ينتج عن التطور السريع للتكنولوجيا وسائل حديثة للتعامل الرقمي فقط، بل أدى ذلك الى ظهور أنماطا إجرامية حديثة تتطلب تكييفا قانونيا خاصا، حتى يتحقق التوازن بين حرية استخدام هذه التكنولوجيا وحماية الأنظمة المعلوماتية، فلو نظرنا من زاوية أن هذه الوسائل قد تُستعمل في تحسين الخدمات الإلكترونية أو تسهيل عملية التصفح، إلا انه من زاوية أخرى فان إساءة استعمالها قد يؤدي إلى المساس بحقوق الأفراد، وعلى رأسها الحق في حماية الخصوصية المعلوماتية.[1] ويتحقق الاعتداء على الخصوصية في البيئة الرقمية عندما يتم جمع البيانات الشخصية أو تخزينها أو تحليلها دون علم صاحبها أو موافقته، أو عندما تُستغل هذه المعلومات لأغراض غير مشروعة، كاستعمالها في الإعلانات التجارية الموجهة أو تمريرها إلى جهات أخرى تقوم بتحليلها واستغلالها لتحقيق منافع مختلفة. وقد يتخذ هذا الاعتداء أشكالاً أكثر خطورة عندما يتمكن الفاعل من الوصول إلى نظم المعالجة الآلية للمعطيات أو اختراقها بهدف الحصول على بيانات سرية أو معلومات شخصية تخص المستخدمين، الأمر الذي يندرج ضمن صور القرصنة الإلكترونية التي تمثل تهديداً حقيقياً لأمن المعلومات وللحقوق الأساسية للأفراد في المجتمع الرقمي[2].

وأمام تزايد هذه الممارسات غير المشروعة، تدخلت التشريعات الوطنية لوضع إطار قانوني يهدف إلى تجريم الأفعال التي تستهدف الأنظمة المعلوماتية أو المعطيات الرقمية المخزنة فيها، فحرص المشرع الجزائري على مواجهة جرائم القرصنة الإلكترونية من خلال إدراج نصوص خاصة ضمن قانون العقوبات، لا سيما المواد 394 مكرر إلى 394 مكرر 7، التي تناولت مختلف الأفعال التي تشكل اعتداءً على نظم المعالجة الآلية للمعطيات فيقوم التكييف القانوني لهذه الأفعال على اعتبارها جرائم ماسة بأمن الأنظمة المعلوماتية وسلامة البيانات الرقمية، حيث يندرج ضمنها الدخول غير المشروع إلى نظام معلوماتي أو البقاء فيه دون ترخيص، أو اعتراض المعطيات أو نسخها أو تحويلها بطرق غير قانونية[3].

وفي ذات السياق تدخل المشرع الجزائري من خلال القانون 09_04 ليضع منظومة قانونية خاصة تجرم مختلف صور الاعتداء على الأنظمة المعلوماتية، سواء تعلق الأمر بالدخول غير المشروع، أو اعتراض البيانات، أو إتلافها أو تعديلها أو التلاعب بالأنظمة المعلوماتية، مع إقرار جزاءات تتفاوت في شدتها

---

[1] عبد الفتاح بيومي الحجازي، **مرجع سابق**، ص 110

[2] محمد أمين الشوابكة، **جرائم الحاسوب والانترنت**، درا الثقافة للنشر والتوزيع، عمان، 2011، ص 65-70.

[3] "تنص المادة 394 مكرر 7 من قانون العقوبات الجزائري ,

بحسب جسامة الفعل المرتكب والنتائج المترتبة عنه، ويعكس هذا التوجه تبني السياسة الجنائية الجزائرية لفكرة الحماية الجزائية المتخصصة في مواجهة الجرائم المعلوماتية.[1]

ومن خلال هذه النصوص يتضح أن المشرع الجزائري تبنى سياسة جنائية ترمي إلى توفير حماية فعالة للبيئة الرقمية، وذلك عبر تجريم مختلف الأفعال التي تنطوي على اختراق الأنظمة المعلوماتية أو الاستيلاء على البيانات الرقمية أو استغلالها دون وجه حق، كما تعكس هذه السياسة حرص المشرع على تحقيق التوازن بين الاستفادة من التطور التكنولوجي وضمان احترام الحقوق الأساسية للأفراد، وفي مقدمتها الحق في الخصوصية وحماية المعطيات الشخصية. وبالتالي فإن تجريم أفعال القرصنة الإلكترونية وفرض العقوبات المناسبة على مرتكبيها يشكلان أحد أهم الآليات القانونية التي يعتمد عليها المشرع الجزائري لمواجهة التهديدات المتزايدة التي تفرضها الجريمة المعلوماتية في العصر الرقمي[2].

المبحث الأول: الطبيعة والتكييف القانوني لجريمة القرصنة الإلكترونية

يعد الدخول غير المصرح به إلى المواقع الإلكترونية أو نظم المعلومات من أكثر الأفعال التي تندرج ضمن صور الاعتداء على أمن المعلومات، ويتحقق هذا السلوك عندما يقوم شخص بالولوج إلى موقع إلكتروني أو نظام لمعالجة البيانات دون الحصول على إذن من الجهة المالكة أو المسؤولة عن ذلك النظام، وقد يتم هذا الدخول بصورة مباشرة باستخدام الحاسوب المتصل بالنظام، أو بصورة غير مباشرة عبر الشبكات المعلوماتية ووسائل الاتصال عن بعد التي تسمح بالاطلاع على البيانات المخزنة أو المتبادلة داخل النظام[3].

كما قد يلجأ الفاعل إلى استخدام وسائل تقنية مختلفة تمكنه من تجاوز التدابير الأمنية المفروضة على النظام المعلوماتي، مثل برامج كشف كلمة المرور أو أدوات فك الشفرات، أين عالجت بعض التطبيقات القضائية هذه المسألة، حيث اعتبرت أن استخدام وسائل تقنية لكسر كلمات السر أو تجاوز أنظمة الحماية بهدف الاطلاع على البيانات المخزنة في الأنظمة المعلوماتية يشكل اعتداءات على النظام وخرقا للقواعد المنظمة لاستخدامه، ومن ثم فان الولوج إلى المواقع أو قواعد البيانات يجب أن يتم في إطار إحترام القوانين واللوائح التي تنظم استخدام الأنظمة المعلوماتية وتحمي البيانات وحقوق الملكية الفكرية المرتبطة بالمحتوى الرقمي.[4]

---

[1] القانون 04/09 **الجريدة الرسمية للجمهورية الجزائرية**،2009.

[2] بشرى حسين الحمداني، **مرجع سابق**، ص 85-86.

[3] خالد حسن أحمد لطفي، **مرجع سابق**، ص 62

[4] حنان ريحان مبارك المضحكي، **مرجع سابق**، ص 101-102.

وفي ضوء ذلك، لم يعد من الكافي تناول القرصنة الإلكترونية باعتبارها مجرد مفهوم تقني أو ظاهرة معلوماتية، بل أصبح من الضروري دراستها في إطارها القانوني الجنائي بوصفها سلوكا يستوجب التجريم والعقاب بسبب أنها تمس بأمن وسلامة المعالجة الآلية للبيانات، وتستدعي تدخل المشرع لضبطها من خلال قواعد قانونية تحدد أركانها، وتقرر لها الجزاءات المناسبة[1]، ومنه فإن الربط بين هذه النظم والجريمة يقتضي الوقوف على الطبيعة القانونية لهذه الأفعال، ومدى انطباق النصوص الجزائية التقليدية عليها أو الحاجة إلى نصوص خاصة تستجيب لخصوصيتها.

وعليه فان تناول القرصنة الإلكترونية من الزاوية القانونية يهدف إلى تبيانها كجريمة قائمة الأركان من خلال تحليل أركانها المادية والمعنوية، وبيان محل الحماية الجنائية فيها، فضلا عن تحديد نطاق التجريم والعقاب في التشريع الجزائري.

المطلب الأول: الطبيعة القانونية لجريمة القرصنة الالكترونية

دفع التطور التكنولوجي التشريعات الجنائية لسن عقوبات على هذا النوع من الجرائم، بهدف توفير الحماية الجزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، والمشرع الجزائري هو الآخر قام بتعديل القانون العقوبات بموجب القانون **04-15** المعدل والمتمم، كما نجد أن المشرع الجزائري قد أقر بأن جوهر المعلوماتية هي المعطيات التي تدخل إلى الحاسوب فيقوم بتحويلها إلى معلومات بعد معالجتها والقيام بتخزينها.[2]

ومن حيث الطبيعة القانونية فتتخذ الجرائم طبيعة خاصة في حال لم تكن القواعد التقليدية قد تم تشريعها خصيصا لهذه الظواهر الإجرامية المستحدثة، ذلك يرجع في أن تطبيق النصوص التقليدية على هذا النوع من الجرائم يلقى العديد من الصعوبات أبرزها صعوبة إيجاد الدليل المادي أو ما يسمى بصعوبة الإثبات في الجرائم الالكترونية.

كذلك الأمر بالنسبة لمحل جريمة القرصنة الالكترونية فهو يتميز عن محل الجرائم التقليدية، حيث أن المحل في النوع الأول من الجرائم هو المال المعلوماتي الذي يتميز عن المال التقليدي في الجريمة الثانية

---

[1] محمد حسين منصور، **المسؤولية الجنائية عن جرائم الحاسب الآلي الانترنت**، دار الجامعة الجديدة، الإسكندرية، 2003، ص 45.

[2] **القانون 04-15** المؤرخ في 2004/11/10، والمعدل والمتمم بالقانون رقم 24-06 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 30، المؤرخ في 30 أبريل سنة 2024.

بكل عناصره، بمعنى أن الجرائم المعلوماتية بما فيها جرائم القرصنة الالكترونية تشمل كل أفعال السرقة أو التغيير أو حذف المعلومات مثل النشاط الإجرامي الذي يكون الهدف منه اختراق أنظمة وبيانات الغير والعبث بمحتوياته، ويحمل في طياته انتهاكات للخصوصية وحقوق الملكية الفكرية وأنماطا إجرامية أخرى.[1]

إذن حسب ما تناولناه أعلاه فإنه عند الحديث عن الطبيعة القانونية لجريمة القرصنة الالكترونية فالأمر يتعلق بالوضع القانوني للبرامج والمعلومات من ناحية القيمة المادية لها أي أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء ويمكن الاعتداء عليها بأي طريقة كانت، لذلك فقد انقسم الفقه لاتجاهين:

الاتجاه الأول: يرى أصحاب الرأي الأول بأن الأشياء المادية هي وحدها من تقبل الحيازة والاستحواذ، بحيث أن ما يقع عليه فعل السطو يجب أن يكون ماديا بحيث يمكن نقله وحيازته واختلاسه، وعلى اعتبار أن المعلومة لها طبيعة معنوية فلا يمكن اعتبارها من قبل القيم القابلة للحيازة والاستحواذ، غير أنه وفي ضوء حقوق الملكية الفكرية، فهي بذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة، ما لم تكن مسجلة على شريط أو أسطوانة، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية، فلا تثور مشكلة قانونية في تكييف الواقعة على أساس أنها سرقة للمال العام معلوماتي لها طبيعة مادية، والمشكلة تثور عندما نقف أمام سرقة مال معلوماتي غير مادي[2].

الاتجاه الثاني: يرى أصحاب هذا الاتجاه أن القرصنة الإلكترونية لا تعد جريمة واحدة ذات طابع محدد إنما تتخذ صورا وأشكالا متعددة وهناك الكثير من التشريعات اعتبرت جريمة تحول هي الحد الفاصل بين الجاني وبين ارتكابه لمختلف الجرائم الأخرى.

الفرع الأول: نظام المعالجة الالية للمعطيات محلا لجريمة الدخول أو البقاء غير المشروع

تفترض جريمة الدخول غير المشروع أو الجرائم المترتبة عنها وجود نظام للمعالجة الآلية للمعطيات **Le système de traitement automatisé des données** وهذا النظام يعتبر العنصر الجوهري

[1] حمزة خضري–عشاش حمزة، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، المجلد 06 العدد 02 جوان 2020، ص 173

[2] جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة دار الثقافة للنشر والتوزيع، عمان الأردن، 2010، ص 124.

المشترك بين مختلف هذه الجرائم في غيابه لا يمكن الحديث عن باقي الأركان القانونية للجريمة، فالنصوص العقابية لا تطبق إلا عند تحقق هذا الركن الأساسي ونفس الأمر بالنسبة للركن الشرعي[1]

يتضح موقف المشرّع الجزائري، بعد صدور القانون رقم 04-15، أنه لم يتبن وصفا موحدا لجريمة القرصنة الإلكترونية، وإنما أقر مجموعة من الأفعال المجرّمة التي تستهدف نظام المعالجة الآلية للمعطيات، فنص على صور متعددة للاعتداء، لكل منها أركانها وعقوبتها الخاصة، ومع ذلك، فإن هذه الجرائم تشترك جميعها في عنصر جوهري يتمثل في النظام المعلوماتي، باعتباره محل الحماية الجنائية، الأمر الذي يجعله نقطة الانطلاق الأساسية في تحديد قيام الجريمة.

ومن هذا المنطلق، تم تخصيص دراسة مستقلة لمفهوم نظام المعالجة الآلية للمعطيات، باعتباره الركيزة الأساسية التي تقوم عليها مختلف صور الاعتداء المعلوماتي، وتمهيدًا لتحليل باقي الأركان القانونية لهذه الجرائم بصورة أكثر دقة ووضوحًا[2]

اولا: مفهوم نظام المعالجة الالية للمعطيات

[3]لقد اختلفت التشريعات في تحديد مفهوم نظام المعالجة الآلية للمعطيات، تبعًا لاختلاف طريقة تناولها لهذا النظام والعناصر التي يتكون منها. وفي هذا الإطار، تم تعريف النظام المعلوماتي في القانون الجنائي اللبناني في المادة الأولى من الكتاب الثاني، تحت عنوان «الاعتداءات الواقعة على النظام المعلوماتي»، وهو تعريف مستمد من المفهوم الوارد في المادة الأولى من اتفاقية بودابست الخاصة بالجريمة الإلكترونية، باعتباره كل جهاز يتيح المعالجة الإلكترونية للمعطيات، سواء عمل بصورة مستقلة أو كان مرتبطًا بأجهزة أخرى

ويُفهم من هذا التعريف أن النظام المعلوماتي لا يقتصر بالضرورة على جهاز منفرد، وإنما يمكن أن يتكون من عدة أجهزة مترابطة، متى كانت مهيأة للقيام بعملية معالجة إلكترونية للمعطيات. ومن هذا المنطلق، اهتم التشريع الفرنسي بدوره بتحديد مفهوم نظام المعالجة الآلية للمعطيات، وذلك بمناسبة تجريم الأفعال الماسة بالأنظمة المعلوماتية.

---

[1] Nicolas Arpagian, La cyber sécurité, éditions L'héritier,2014 ,P07.

[2]بن شريف أحلام، بوغرارة الصالح، المرجع السابق، ص31.

[3] غنية باطلي، مرجع سابق، ص 136.

فقد اقترح مجلس الشيوخ الفرنسي، خلال الأعمال التحضيرية للقانون رقم 88-19 المعروف بقانون «Godfrain» ، الصادر في 5 يناير 1988 والمتعلق بمكافحة الغش المعلوماتي، تعريفًا لنظام المعالجة الآلية للمعطيات، باعتباره كل منظومة مكوّنة من وحدة أو عدة وحدات للمعالجة، تضم الذاكرة والبرامج والمعطيات، إضافة إلى أجهزة الإدخال والإخراج وأجهزة الربط، التي تتكامل فيما بينها من خلال علاقات معينة تسمح بإنتاج نتائج محددة، أي معالجة المعطيات، وبناءً على ذلك تكون هذه المنظومة محلًا للحماية الجزائية[1].

وتكتسي الأعمال التحضيرية لمشاريع القوانين أهمية في تفسير بعض النصوص، لما يمكن أن تكشف عنه من تصور للمشرع عند إعداد النص القانوني. غير أن التعريف المقترح خلال هذه المرحلة لا يُعدّ هو النص التشريعي النهائي، ولذلك ينبغي الرجوع إلى الصياغة التي استقر عليها النص عند اعتماده

وفي هذا السياق، لم يعتمد التعريف الوارد في الأعمال التحضيرية بصيغته ذاتها في النص النهائي للمادة 462-2 من القانون رقم 88-19، التي نصت على أن نظام المعالجة الآلية للمعطيات يشمل كل جهاز منفرد أو مجموعة من الأجهزة المترابطة التي تقوم، من خلال تنفيذ برنامج معين، بإجراء معالجة آلية[2].

ومن المقرر أن الأعمال التحضيرية لمشاريع القوانين تعد أداة مهمة في تفسير بعض النصوص، ورغم أن التعريف الوارد لم يعتمد بصيغته في النص النهائي للمادة 2/462 من القانون 88/19 التي تنص على أنه يشمل كل جهاز منفرد أو مجموعة من الأجهزة المترابطة التي تقوم عبر تنفيذ برنامج معين، بإجراء معالجة آلية للبيانات.

أ-المكونات المادية والمعنوية لنظام المعالجة الالية للمعطيات

يمكن القول أن نظام المعالجة الآلية للمعطيات يتمثل في كل بنية تقنية، بسيطة أو معقدة، تمكن من إدخال البيانات ومعالجتها وتخزينها واسترجاعها بشكل ألي، وهو ما يجعله الإطار الأساسي الذي تقع عليه أفعال الاعتداء في جرائم القرصنة الإلكترونية[3].

---

[1] خليفة محمد، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن**، دار الجامعة الجديدة، الاسكندرية، دون سنة نشر، ص 27-28.

[2] غنية باطلي، **مرجع سابق**، ص135-140.

[3] Convention sur la cybercriminalité, Adoptée à Budapest le 23 novembre 2001, Conseil de l'Europe , article 01 « Le système informatique désigne tout dispositif isolé ou ensemble de dispositif sinter

ويتألف نظام المعالجة الالية من مكونات مادية وأخرى غير مادية

1: مجموعة من المكونات المادية والمعنوية المرتبطة ببعضها البعض بعلاقات أو روابط تؤدي إلى تحقيق هدف أو نتيجة معينة

2: وجوب أو ضرورة خضوع النظام للحماية الفنية[1].

ثانيا: عناصر نظام المعالجة الآلية للمعطيات:

يتألف نظام المعالجة الآلية من مكونات مادية وأخرى غير مادية.

أ-**المكونات المادية:** تتمثل في الحاسوب، والدعامات التي تخزن البرامج والمعطيات، ووحدات الإدخال والإخراج إضافة إلى أسلاك الاتصال.

ب-**المكونات غير المادية:** فتستعمل الخوارزميات التي تشكل البرامج والمعطيات المخزنة في صورة معلومات مشفرة.

ج-**تكامل مكونات النظام:**

ويتطلب النظام توافر الأجهزة والبرامج والمعلومات بشكل متكامل ومتزامن، غير أن هذه العناصر لا ترد على سبيل الحصر، وإنما على سبيل المثال، الأمر الذي يترك المجال مفتوحا لإضافة مكونات جديدة أو الاستغناء عن بعضها وفقا لما تفرضه مستجدات وتطورات تقنية في هذا المجال[2].

ومفاد ذلك أن الاعتداء على أي عنصر منفرد، إذا لم يكن مدمجا ضمن مكونات النظام المعلوماتي، لا ينهض سببا لقيام الجريمة، وعلى سبيل المثال، فإن الاعتداء على البرامج المعروضة للبيع أو على الحواسيب التي لم تدخل بعد حيز الاستعمال الفعلي أو على المكونات المخزنة التي صار التخفي طور التجربة، أو التي أخرجت من الخدمة أو كانت في طريقها إلى التلف، لا يشكل في حد ذاته اعتداءً على النظام المعلوماتي[3].

---

connectés ou apparentés, qui as sureau dont un ou plusieurs éléments assurent, inexécution d'un programme, un traitement automatise de données ».

[1] أمال قارة، **مرجع سابق**، ص 102.

[2] أشرف السعيد أحمد، **مرجع** سابق، ص 43.

[3] غنية باطلي، **مرجع سابق**، ص 141.

وعلى العكس من ذلك، فإن الجريمة تقوم متى كان الاعتداء موجه على النظام المعلوماتي، حتى وإن وقع خارج أوقات العمل أو أثناء توقفه عن التشغيل العادي أو إذا كان أحد عناصره في حالة العطل، بل وحتى في حال تعطل النظام كليا مادام قابل للإصلاح، كما تعد الجريمة قائمة إذا استهدف الاعتداء عنصرا يدخل ضمن مكونات أنظمة متعددة مترابطة فيما بينها بواسطة أجهزة الاتصال، كالحاسب الآلي، باعتباره جزءا من أحد تلك الأنظمة.

وحتى إذا كان الدخول إلى الجهاز مشروعا فإن الجريمة تقوم متى ثبتت علاقة سببية بين هذا الدخول المشروع به وبين الاعتداء الذي لحق بالأنظمة ككل، ثم يبحث بعد ذلك في توفر حسن النية أو سوئها لدى المتدخل، كما يعتبر الاعتداء على شبكة الاتصال اعتداء على الأنظمة المرتبطة بها، لكونها تعد عنصر مكونا لكل نظام من تلك الأنظمة[1].

الفرع الثاني: الحماية الفنية لنظام المعالجة الالية للمعطيات

تنقسم الأنظمة إلى ثلاثة أقسام تتمثل في أنظمة مفتوحة للجمهور وأنظمة قاصرة على أصحاب الحق ولكن غير محمية فنيا، وأنظمة قاصرة على أصحاب الحق لكن محمية فنيا[2].

ويثار التساؤل حول ما إذا كان وجود الحماية الفنية يعد شرطا أساسيا للاستفادة من الحماية الجنائية أم لا؟

وقبل الإجابة عن هذا التساؤل، يجدر بنا أولا توضيح معنى الحماية الفنية[3].

أولا: مفهوم الحماية الفنية ووسائلها

تقتضي دراسة الحماية الفنية لنظام المعالجة الآلية للمعطيات الوقوف على مضمونها التقني، باعتبارها من التدابير الأساسية الرامية إلى تأمين الأنظمة المعلوماتية وحمايتها من مختلف صور الاعتداء. ولا يقتصر دور هذه الحماية على منع الولوج غير المشروع، بل يمتد إلى ضمان سلامة البيانات وسريتها واستمرارية عمل الأنظمة. ومن ثم، يقتضي تحديد نطاقها التطرق إلى مفهوم الحماية الفنية، ثم بيان أهم الوسائل المادية وغير المادية المعتمدة لتحقيقها.

---

1 **نفس المرجع**، ص 142-143.

[2] نشناش مينة، الركن المفترض في الجريمة المعلوماتية، **مداخلة ألقيت بمناسبة انعقاد الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة**، كلية الحقوق والعلوم السياسية، بسكرة، 16-17 نوفمبر 2015، ص 8

[3] علي عبد القادر القهوجي، **مرجع سابق**، ص 121

أ- **مفهوم الحماية الفنية**

الحماية الفنية هي مجموعة الوسائل والتدابير التقنية التي تعتمد لتأمين نظام المعالجة الآلية للمعطيات، بهدف منع الولوج غير المشروع، أو تقييده، أو كشفه، وضمان سرية البيانات وسلامتها وتوافرها، بمعنى ليس الحماية القانونية، بل الحماية التقنية التي يضعها صاحب النظام، مثل كلمة المرور، أنظمة التشفير، الجدران النارية، أنظمة التحقيق من الهوية.

ب-وسائل الحماية الفنية

توجد عدة وسائل مادية وغير مادية لحماية المعلومات والأنظمة وطرق معالجتها فمنها ما يعرف بقواعد الأمن المادي ومنها ما يتمثل في وسائل غير مادية مخصصة لتحقيق هذه الحماية[1].

1-وسائل الأمن المادي

المقصود بذلك هو المحافظة على أجهزة الحاسوب وملحقاته، وضمان الحماية اللازمة للأسطوانات والشرائط والطابعات وأماكن التخزين والاتصالات وتتمثل إجراءات الأمن المادي في مجموعة من التحصينات والإجراءات العملية التي تهدف إلى حماية المنشآت من الكوارث الطبيعية، والحوادث المختلفة، والظروف البيئية وكذلك كم أعمال الإتلاف المعتمد[2].

2-وسائل الأمن غير المادي

توجد أنظمة اتصال مفتوحة يمكن لأي شخص الوصول إليها وهو ما يجعل امن الاتصالات مرتبطا بشكل وثيق بأمن الشبكات وتنقسم هذه الشبكات إلى ثلاث أنواع رئيسية:

الشبكات المحلية، الشبكات الواسعة النطاق داخل الإقليم الواحد إضافة إلى شبكة المعلومات الدولية (Internet[3]).

توجد عدة وسائل لضمان حماية شبكات الاتصال ويعد الجدار الناري من أهمها، إذ يعمل على منع الوصول عند المصرح به لحماية وحدات التحكم في الإرسال عبر الشبكات ويهدف هذا الإجراء إلى إنشاء

---

[1] أمال قارة، **مرجع سابق**، ص 103

[2] أيمن عبد الحفيظ، **المخاطر التي تتعرض لها شبكة الانترنت وسبل حمايتها**، مجلة البحوث الشرطة، العدد 20، القاهرة، 2001، ص 452.

[3] حزام فتيحة، **حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية**، قراءة في أحكام المرسوم الرئاسي05-20، مجلة الحقوق والعلوم الإنسانية، جامعة بومرداس، الجزائر، العدد الثالث، 2020، ص 182.

بيئة اتصالات مؤمنة ومحصنة ضد محاولات الاختراق الغير مشروع، وهو ما يعرف بالتصدي الفني أو التقني، ويعد من أنجح الوسائل في الحفاظ على سلامة وأمن المعلومات.

ويقصد بالجدار الناري مجموعة من الأنظمة التقنية التي تضع سياسات أمنية، بين شبكة المؤسسة وشبكة الانترنت بحيث تلزم جميع عمليات الدخول والخروج بالمرور عبره حصرا ويقوم هذا الجدار بصد محاولات وصول غير مشروعة أو من قبل مستعملين غير مصرح لهم، مما يجعله بمثابة حاجز قانوني وتقني يحمي الشبكة الداخلية للمؤسسة.

كما يوفر آليات لتنظيم الاستخدام وفق سياسات المؤسسة، تشمل ضبط صلاحيات الدخول إلى الشبكة والخدمات، التحقق من هوية المستعملين المحليين والخارجيين، ومراقبة عمليات الدخول والخروج، اعتماد تقنيات التشفير، فضلا عن الإجراءات الوقائية للحماية من الفيروسات والبرمجيات الضارة.

ومن أبرز تطبيقات برامج الجدار الناري Zone alarm، الذي يتميز بفعاليته العالية في مراقبة وضبط مختلف محاولات اختلاف للأجهزة، مع تنبيه المستخدم فور وقوع أي اعتداء[1]، كما يتعامل البرنامج مع مرفقات البريد الإلكتروني التي تعد من أهم مصادر انتشار الفيروسات حيث يقوم باحتجازها أو حذفها أو منعها من الوصول إلى النظام حفاظا على أمنه وسلامته[2].

توجد وسائل أخرى للحماية الفنية تعتمد على الخصائص البيولوجية للإنسان مثل بصمة الإبهام، حدقة العين أو نبرة الصوت، بالإضافة إلى استخدام التوقيع الالكتروني، كما يستعمل التشفير كوسيلة أساسية حيث، يتم من خلاله تحويل النص الأصلي للرسالة إلى نص مشفر بواسطة المرسل.

وتعتمد غالبية تقنيات التشفير على نظام المفاتيح العامة ومن أشهرها نظام RSA.

ثانيا: الجدل الفقهي حول إشتراط الحماية الفنية

يتضح أن الحماية الفنية رغم أهميتها الكبيرة في الحد من الجرائم المعلوماتية لا تكفي وحدها لتحقيق الأمن الكامل، فقد أثبتت التجربة والتطور التكنولوجي أن مرتكبي الجرائم الإلكترونية يمتلكون قدرات متجددة على ابتكار وسائل وبرامج جديدة للاعتداء، وهو ما يجعل وسائل الحماية الفنية عاجزة عن مواكبتها بشكل كامل ومستمر.

[1] أيمن عبد الحفيظ، **مرجع سابق**، ص 466.

[2] غنية باطلي، **مرجع سابق**، ص 150.

وأدى تطور وسائل الاختراق إلى صراع دائم بين شركات الأمن الإلكتروني والمجرمين المعلوماتيين، مما يجعل الحماية الفنية وحدها غير كافية رغم أهميتها، وهو ما يفترض تدعيمها بحماية جنائية تحقق الردع. وهنا يثار التساؤل: هل تعتبر الحماية الفنية شرطا أساسيا للخضوع للحماية الجنائية؟[1]

لم يشترط الشروع في نصوص جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات وجود حماية فنية، غير أن الأصل في تفسير النص هو عدم تقييد أو تخصيص القاعدة العامة إلا إذا ورد نص صريح يجيز ذلك، وهو ما لم يحدث وبناء عليه اختلف الفقه بين اتجاه مقيد يقصر الحماية على الأنظمة المحمية فقط، واتجاه موسع يمد الحماية لتشمل الأنظمة المحمية والغير المحمية.

والسؤال الذي يمكننا طرحه هنا هو: هل تحقق الحماية الفنية الغاية المرجوة منها، أم أنها تبقى قاصرة وتحتاج إلى وسائل مكملة؟ بحيث هل تضمن جدران الحماية وحدها التصدي الكامل لمخاطر الفيروسات والاعتداءات الإلكترونية؟ أم أن الأمر يقتضي تطوير تلك الجدران بصفة مستمرة؟

أ-الاتجاه المقيد للحماية

تظهر الأعمال التحضيرية لقانون الغش المعلوماتي الفرنسي في عدة مواضع[2]، أن المشرعين قد ربطوا هذه الجرائم بضرورة وجود أنظمة محمية[3].

إن وجود مثل هذه الأنظمة يساهم في تسهيل عملية الكشف عن الجريمة عند اختراقها، إذ يترك المجني عادة آثار تدل عليه، مما يساعد على إثبات القصد الجنائي لديه وبناءً على ذلك، فإن التفسير الصحيح لنص التجريم الدخول الغير مصرح به يقتضي الحصر في حالات اختراق الأنظمة المحمية دون غيره[4].

ب-الاتجاه الموسع للحماية الجنائية:

على عكس ما جاء به الاتجاه الضيق فان أصحاب هذا الاتجاه يرون أن خضوع المال المسروق لحماية صاحبه أو عدمه لا يغير من قيام جريمة السرقة، هذا الشرط يغفل العديد من حالات الدخول عن

---

[1] غنية باطلي، **مرجع سابق**، ص 151.

[2] أيمن عبد الله فكري، **مرجع سابق**، ص 234.

[3] نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة،2003، ص 367.

[4] محمد خليفة، مرجع سابق، ص 134.135.

طريق الخطأ مما يؤدي إلى تضييق نطاق تطبيق النص، وهناك من يرى وجوب امتداد الحماية الجنائية لتشمل جميع الأنظمة المعلوماتية.

ثالثا: مبررات الحماية الجنائية

فيتضح أن للحماية الجنائية العديد من الفوائد يمكن توضيحها على النحو التالي.

أ_ المبررات الواقعية: نظرا للتطور المتسارع في المجال التكنولوجي وما يترتب عليه من خسائر ناتجة عن جرائم إلكترونية وخاصة تفاقم مخاطر على المجتمع الدولي المعاصر أصبح من الضروري أن تتدخل الدولة بنصوص قانونية مناسبة لبسط حمايتها الجنائية على مشروعاتها الوطنية في مواجهة هذا النوع من الجرائم[1].

ب_ المبررات الاقتصادية: إن العقوبة تهدف إلى ردع مرتكبي الأفعال الإجرامية وقد أوضحت النظرية الاقتصادية للجريمة الطبيعية العلاقة بين الإجرام والظاهرة الاقتصادية من خلال ما يقوم به الفرد، من تقييمه للفعل قبل الأقدام عليه وموازنته بين الفائدة الناتجة عن الفعل والثمن الذي سيدفعه وهو العقوبة فإذا طغى جانب العقوبة على جانب الفائدة المثنى الفرد عن ارتكاب ذلك الفعل[2].

ج_ المبررات الجنائية: يلعب قانون العقوبات دورا بارزا من الناحية القانونية إذ تتميز إجراءات البحث عن الجرائم بقدر من السهولة النسبية يتيح إمكانية تطبيقه، الأمر الذي يجعل من الحماية الجنائية وسيلة ردع لا يوفرها القانون المدني[3].

المطلب الثاني: التكييف القانوني لجريمة القرصنة الإلكترونية

يُعدّ التكييف القانوني لجريمة القرصنة الإلكترونية من المسائل التي تكتسي أهمية خاصة، بالنظر إلى تعدد صور الاعتداء التي يمكن أن تستهدف الأنظمة المعلوماتية والمعطيات التي تتضمنها. ويقصد بالتكييف القانوني تحديد الوصف الذي يضفيه القانون على الفعل المرتكب، من خلال إخضاعه للنص الجزائي الذي تتوافر شروط تطبيقه، بما يسمح بتحديد طبيعته القانونية والآثار المترتبة عنه[4].

وقد تدخل المشرع الجزائري لتنظيم الأفعال التي تستهدف أنظمة المعالجة الآلية للمعطيات، دون أن يضع تعريفًا تشريعيًا مستقلًا لمصطلح القرصنة الإلكترونية، وإنما اعتمد أسلوب تحديد الأفعال المجرّمة

---

[1] R. Gassin. op.cit, p15.

[2] محمد خليفة، مرجع سابق، ص 30-31.

[3] خالد حسن أحمد لطفي، مرجع سابق، ص 85.

[4] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، ص 87.

وصورها، لاسيما الدخول أو البقاء غير المشروعين في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، وإدخال أو إزالة أو تعديل المعطيات بطريق الغش، فضلًا عن الأفعال التي من شأنها المساس بسير النظام أو سلامة المعطيات[1].

وعليه، فإن تحديد التكييف القانوني لجريمة القرصنة الإلكترونية في التشريع الجزائري يقتضي الرجوع أساسًا إلى الأحكام التي أدرجها المشرع ضمن قانون العقوبات تحت عنوان «المساس بأنظمة المعالجة الآلية للمعطيات»، مع الاستعانة بالقوانين الخاصة والمكملة كلما كان الفعل المرتكب يمس بمصالح أو معطيات تحظى بحماية قانونية خاصة. ومن ثم، نتناول ذلك من خلال الفرعين الآتيين:

الفرع الأول: أساس التكييف القانوني لجريمة القرصنة الإلكترونية في التشريع الجزائري

الفرع الثاني: نطاق التكييف القانوني لجريمة القرصنة الإلكترونية في التشريع الجزائري

الفرع الأول: أساس التكييف القانوني لجريمة القرصنة الإلكترونية في التشريع الجزائري

لم يعتمد المشرع الجزائري مصطلح «القرصنة الإلكترونية» كتسمية قانونية لجريمة مستقلة، كما لم يضع لها تعريفًا تشريعيًا جامعًا، وإنما اختار تحديد الأفعال التي تشكل اعتداءً على أنظمة المعالجة الآلية للمعطيات، وهو ما يسمح بتحديد التكييف القانوني للفعل بحسب طبيعته ومحل الاعتداء والنتيجة المترتبة عنه.

ويستند هذا التوجه أساسًا إلى القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، والذي استحدث القسم السابع مكرر تحت عنوان «المساس بأنظمة المعالجة الآلية للمعطيات»، متضمنًا الأحكام الجزائية الخاصة بهذا النوع من الاعتداءات، وقد شكل هذا التنظيم الأساس الموضوعي للتجريم والعقاب في مجال الاعتداء على الأنظمة المعلوماتية في التشريع الجزائري.

أولًا: التكييف القانوني للقرصنة الإلكترونية باعتبارها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات

يتضح من استقراء أحكام قانون العقوبات الجزائري أن المشرع لم ينظر إلى القرصنة الإلكترونية بوصفها جريمة مستقلة تحت هذه التسمية، وإنما أدرج الأفعال التي تدخل في مدلولها ضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات. ويظهر ذلك بصفة خاصة من خلال المادة 394 مكرر من قانون العقوبات، التي تجرّم فعل الدخول والبقاء في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، أو محاولة ذلك.

[1] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الالية للمعطيات، دار الخلدونية، 2018، ص 320_325

ويستفاد من هذا النص أن الدخول غير المشروع إلى النظام المعلوماتي والبقاء فيه دون حق يمثلان صورتين أساسيتين للاعتداء على النظام، بحيث يتحقق التجريم متى اتجه سلوك الجاني إلى الولوج إلى النظام أو الاستمرار فيه، دون أن يكون مخولًا بذلك قانونًا. كما أن المشرع لم يحصر الحماية في مجرد الدخول والبقاء، وإنما رتب آثارًا أشد عندما يترتب عن ذلك حذف أو تغيير للمعطيات أو تخريب لنظام اشتغال المنظومة.

ولا يقتصر نطاق التجريم على الاعتداء على النظام ذاته، إذ امتدت الحماية إلى المعطيات التي يحتويها، حيث جرّم المشرع، بموجب المادة 394 مكرر 1، إدخال المعطيات في نظام المعالجة الآلية أو إزالة أو تعديل المعطيات التي يتضمنها من دون وجه حق[1].

وبذلك يظهر أن التكييف القانوني لأفعال القرصنة لا يتوقف عند مرحلة الولوج إلى النظام، وإنما يتحدد كذلك بحسب السلوك اللاحق الذي يستهدف المعطيات أو وظائف النظام.

ومن ثم، فإن القرصنة الإلكترونية، من منظور التشريع الجزائري، لا تشكل وصفًا جزائيًا واحدًا ثابتًا، وإنما تمثل مفهومًا يستوعب مجموعة من الأفعال غير المشروعة التي يمكن أن تتخذ صورًا متعددة، يكون أساس تكييفها القانوني هو النص الجزائي الذي ينطبق على الفعل المرتكب بحسب عناصره ومحل الاعتداء والنتيجة التي ترتبت عنه.

كما عزز المشرع هذه الحماية بإقرار أحكام خاصة تتعلق بالشروع، والمسؤولية الجزائية للشخص المعنوي، والمصادرة، فضلًا عن تجريم المشاركة في مجموعة أو اتفاق بغرض الإعداد لارتكاب الجرائم المنصوص عليها ضمن هذا القسم.[5] ويؤكد ذلك أن السياسة التشريعية الجزائرية اتجهت إلى بناء حماية جزائية خاصة للأنظمة المعلوماتية، بدل الاكتفاء بالقواعد العامة المقررة للجرائم التقليدية[2].

ثانيًا: التكييف القانوني لأفعال القرصنة بحسب محل الاعتداء

لا يقتصر التكييف القانوني للقرصنة الإلكترونية على فعل الدخول أو البقاء غير المشروعين، وإنما يتحدد أيضًا بالنظر إلى محل الاعتداء الذي قد يكون النظام المعلوماتي في حد ذاته، أو المعطيات المخزنة داخله، أو الوظائف التي يؤديها النظام.

فإذا انصب السلوك الإجرامي على الولوج إلى النظام أو الاستمرار فيه دون حق، فإن التكييف يكون في إطار أحكام الدخول أو البقاء غير المشروعين المنصوص عليهما في المادة 394 مكرر من قانون

[1] حسين طاهري، الجرائم الالكترونية، مرجع سابق، ص 46.
[2] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الالية للمعطيات، دار الخلدونية، 2018، ص 320_325.

العقوبات. أما إذا تجاوز السلوك مرحلة الولوج واتجه إلى إدخال المعطيات أو حذفها أو تعديلها بطريق الغش، فإن الفعل يأخذ وصفًا قانونيًا آخر وفقًا للمادة 394 مكرر 1.[1]

أما إذا أدى الاعتداء إلى تخريب نظام اشتغال المنظومة، فإن المشرع رتب عليه وصفًا وعقوبة أشد، بالنظر إلى ما يمثله هذا الفعل من مساس بوظائف النظام وقدرته على أداء المهام المخصصة له. وبذلك يربط المشرع بين طبيعة السلوك المرتكب والنتيجة المترتبة عنه عند تحديد الوصف القانوني للفعل والعقوبة المقررة له.

وعليه، فإن التكييف القانوني للقرصنة الإلكترونية في التشريع الجزائري يقوم على أساس طبيعة السلوك الإجرامي ومحل الاعتداء والنتيجة المترتبة عنه، وليس على مجرد استعمال الوسائل الإلكترونية في ارتكاب الفعل. فالوسيلة التقنية لا تكفي وحدها لإضفاء وصف القرصنة على السلوك، وإنما العبرة بالفعل الذي ارتكبه الجاني ومدى انطباق النص الجزائي عليه

الفرع الثاني: نطاق التكييف القانوني لجريمة القرصنة الإلكترونية في التشريع الجزائري

إذا كان قانون العقوبات يمثل الأساس المباشر لتجريم الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات، فإن الحماية القانونية للبيئة الرقمية في التشريع الجزائري لا تقتصر عليه، وإنما تتكامل مع مجموعة من القوانين الخاصة التي تحمي بعض المصالح المرتبطة بالأنظمة والمعطيات الرقمية[2]. ولذلك، فإن تحديد التكييف القانوني للفعل يقتضي التمييز بين الجريمة التي يكون محلها النظام المعلوماتي ذاته، وبين الحالات التي تستعمل فيها القرصنة وسيلة للاعتداء على مصالح أخرى يحميها القانون

أولًا: القرصنة الإلكترونية باعتبارها اعتداءً على النظام المعلوماتي

تظهر الصورة الأساسية للقرصنة الإلكترونية في الاعتداء المباشر على نظام المعالجة الآلية للمعطيات، سواء عن طريق الدخول أو البقاء غير المشروعين، أو عن طريق المساس بالمعطيات أو وظائف النظام.

[1] محمد حزيط، جرائم الإعلام الالي في القانون الجزائري، دار هومة، الجزائر، ص 45.

1 الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم، لا سيما القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات؛ والقانون رقم 09-04 المؤرخ في 5 أغسطس سنة 2009، المحدد للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر في 16 أغسطس سنة 2009

وقد أقر المشرع الجزائري هذه الحماية صراحة من خلال القسم السابع مكرر من قانون العقوبات، المستحدث بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، والذي تضمن المواد من 394 مكرر إلى 394 مكرر 7، تحت عنوان «المساس بأنظمة المعالجة الآلية للمعطيات».[1]

ويستفاد من هذا التنظيم أن المشرع اعتمد أسلوبًا يقوم على تعداد الأفعال المجرّمة بدل وضع تعريف عام للقرصنة الإلكترونية. ويُعد هذا الأسلوب أكثر ملاءمة للطبيعة المتغيرة للاعتداءات المعلوماتية، إذ يسمح بإخضاع كل سلوك تتوافر فيه عناصر الجريمة للنص القانوني المناسب دون ربط الحماية بتعريف تقني جامد.

كما يتكامل هذا التنظيم مع القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي وضع إطارًا خاصًا للوقاية والتحري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ونظم عددًا من الإجراءات المرتبطة بجمع الأدلة الإلكترونية وحفظها والتفتيش والحجز والمراقبة الإلكترونية والتعاون القضائي الدولي.

وقد عرّف هذا القانون الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وكذا كل جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.[9] وبذلك يتضح أن القانون 09-04 لا يشكل المصدر الأساسي لتجريم الدخول غير المشروع أو الاعتداء على المعطيات، وإنما يمثل إطارًا خاصًا للوقاية والتحري ومكافحة الجرائم المرتبطة بالبيئة الرقمية، إلى جانب الأحكام الموضوعية الواردة في قانون العقوبات.

كما ينبغي الإشارة إلى القانون رقم 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والذي أدخل تعديلات على عدد من أحكام قانون العقوبات، دون أن يؤدي ذلك إلى إلغاء الأساس الموضوعي المتمثل في الأحكام الخاصة بالمساس بأنظمة المعالجة الآلية للمعطيات.[10] ومن ثم، فإن التكييف القانوني الأساسي للقرصنة الإلكترونية يظل مرتبطًا بالأحكام الخاصة الواردة في قانون العقوبات، مع مراعاة التعديلات التشريعية اللاحقة كلما كانت ذات صلة بالفعل المرتكب.

---

2 القانون رقم 04-15 المؤرخ في 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، الصادر في 10 نوفمبر سنة 2004، ص 8، القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

ثانيًا: القرصنة الإلكترونية باعتبارها وسيلة للاعتداء على مصالح أخرى

يرى البعض بأن جريمة القرصنة الالكترونية هي عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الالكترونية، أي أنها تقوم بتوجيه هجمات إلى معلومات الكمبيوتر أو خدماته بنية المساس بالسرية أو المساس بسلامة المحتوى والتكاملية وأيضا تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، فهذا النمط الإجرامي يعتمد في أساسه على أجهزة الكومبيوتر، وبشكل خاص فهو يهدف إلى الوصول إلى المعلومات المخزنة داخله، فالقرصنة الالكترونية إذن تعني الوصول بطرق غير مشروعة لمعلومات الغير من خلال ثغرات في أنظمة الحماية الخاصة بالهدف.[1]

وقد أثار تحديد مفهوم جريمة القرصنة الإلكترونية جدلا فقهيا واسعا، نظرا لحداثة هذا النوع من الجرائم وتطوره المستمر ، فضلا عن تعدد التسميات التي أطلقت عليه، كالجريمة المعلوماتية أو القرصنة المعلوماتية، بل وذهب بعض الفقه إلى تسميتها في بعض التشريعات المقارنة بجريمة البلطجة الإلكترونية كما هو الحال بالنسبة إلى التشريع المصري[2].

وعلى الرغم من هذا الاختلاف، حاول الفقه تقديم تعريفات متعددة، يمكن ردها إلى اتجاهين رئيسيين:[3]

حيث ذهب **الاتجاه الأول** إلى تعريف القرصنة الالكترونية بأنها عملية اختراق لأنظمة الحاسوب عبر شبكة الإنترنت بوسائل تقنية متقدمة، في حين يرى **الاتجاه الثاني** أنها تتمثل في مجرد الدخول غير المشروع إلى أنظمة المعلومات أو البقاء فيها دون ترخيص، بغض النظر عن الوسيلة المستعملة[4].

ويعكس هذا التباين صعوبة وضع تعريف جامع مانع لهذه الجريمة، الأمر الذي يفسر توجه المشرعين، ومنهم المشرع الجزائري، إلى تجريم الأفعال المكونة لها دون وضع تعريف دقيق لها، وهو الأمر الذي دفعنا إلى البحث في موقف المشرع الجزائري من تجريم هذه الأفعال بدلا من تعريفها.

---

[1] جميل زكريا محمود، الجريمة المعلوماتية وأساليب التأمين، **المؤتمر الدولي لأمن المعلومات الالكترونية** " معا نحو تعامل رقمي آمن"، سلطنة عمان 2005، ص 147.

[2] محمد حزيط، **جرائم الإعلام الآلي في القانون الجزائري**، دار هومة، الجزائر، ص 45

[3] مزوزي إكرام، الحاج علي بدر الدين، **القرصنة الرقمية كعائق تقني لنظام التقاضي الالكتروني**، مجلة البصائر للدراسات القانونية والاقتصادية، الجزائر العدد: الخاص (ديسمبر 2021)، ص312.

[4] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 23

ثالثا: التنظيم القانوني لجريمة القرصنة الإلكترونية

إن جريمة القرصنة الالكترونية هي صورة من صور الجرائم الالكترونية التي ظهرت حديثا في ظل التطور التكنولوجي وتسارع الدول نحو الرقمنة بعد ظهور وسائل اتصال لم تكن موجودة في وقت سابق، وقد كرست الدول جهودها من أجل الحد من المشاكل الناجمة عن هذه الأفعال التي تعتبر أفعالا غير مشروعة، تعتمد في أساسها على استخدام أجهزة الكومبيوتر أو أية وسائل تقنية للمعلومات. [1]

وفي هذا الإطار، تم سن مجموعة من الأحكام التي تجرم الأفعال الماسة بأنظمة المعالجة الآلية للبيانات، سواء تعلق الأمر بالولوج غير المشروع إلى هذه الأنظمة، أو الاستمرار فيها دون ترخيص، أو التلاعب بالمعلومات المخزنة داخلها. كما شمل التجريم مختلف صور الاعتداء التي قد تمس بسلامة البيانات أو تؤثر على سير النظام، بما في ذلك إدخال معطيات مغلوطة أو حذفها أو تعديلها بطرق غير مشروعة.

وامتد نطاق الحماية القانونية ليشمل أيضًا الأفعال المرتبطة باستغلال المعطيات، كحيازتها أو نشرها أو تداولها متى كانت ناتجة عن سلوك غير قانوني، وهو ما يعكس توجّهًا تشريعيًا نحو إحاطة شاملة بمختلف مظاهر الاعتداء المعلوماتي، ويبرز هذا التوسع في إدراك المشرّع لخطورة هذه الجرائم، باعتبارها تمس بمصالح متعددة قد تكون اقتصادية أو أمنية أو حتى سيادية[2].

ومن جهة أخرى، يلاحظ أن تخصيص قسم مستقل لهذه الجرائم ضمن قانون العقوبات يعكس الاعتراف بخصوصيتها، سواء من حيث طبيعتها التقنية أو من حيث أساليب ارتكابها، مما يجعلها متميزة عن الجرائم التقليدية ويصعب إدراجها ضمن التصنيفات الكلاسيكية كما لم يقتصر تدخل المشرّع على النصوص الحديثة، بل سبقه تنظيم جزئي لبعض الجوانب المرتبطة بحماية البرامج والمنتجات الرقمية في إطار قوانين الملكية الفكرية، حيث تم إدماجها ضمن المصنفات التي تحظى بالحماية القانونية، مع إقرار جزاءات على الاعتداء عليها، وهو ما يعكس تطورًا تدريجيًا في السياسة التشريعية لمواكبة التحولات الرقمية[3] .

---

[1] لورنس سعيد الحوامدة، **الجريمة المعلوماتية أركانها وآلية مكافحتها**، الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، السعودية، 2016-2017، ص08.

[2] العربي بوعمامة، **خطاب الكراهية داخل منصات التواصل الاجتماعي**، الفا للوثائق، قسنطينة، الجزائر، 2023، ص 51-52.

[3] سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة ماجستير في العلوم الجنائية، جامعة الحاج لخضر باتنة، 2012-2013، ص 41.

من خلال استقراء نصوص المواد في قانون العقوبات الجزائري نجد أن المشرع لم يتناول جريمة القرصنة الالكترونية بل لم يستعمل مصطلح الجريمة المعلوماتية واكتفى فقط بالاعتماد على تسمية جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وهذا من خلال استحداثه للفصل السابع مكرر بموجب تعديله لقانون العقوبات بالقانون 04-15 المؤرخ في 10 نوفمبر 2004، أين أدخل المشرع جرائم الإعلام الآلي، وخصص لها قسما خاصا بعنوان" المساس بأنظمة المعالجة الآلية للمعطيات "، وذلك من المادة 394 مكرر إلى غاية 394 مكرر 07، و يعتبر هذا القسم الأساس الموضوعي (التجريم والعقاب) تضمنت كل من جرائم الدخول والبقاء (الاختراق)، تخريب الأنظمة، التلاعب بالمعطيات[1].

أ_ تجريم القرصنة الإلكترونية في قانون العقوبات الجزائري

بموجب الأحكام المنصوص عليها في الأمر رقم 66-156 المتضمن قانون العقوبات، المعدل والمتمم بالقانون 04-15 لم يكتفي المشرع الجزائري بالقواعد العامة للتجريم فقط، بل تم إدراج نصوص خاصة ضمن قانون العقوبات تقوم بحماية أنظمة المعالجة الآلية للبيانات، حيث تم تجريم الأفعال التي تمسّ بسرية وسلامة وتوافر هذه الأنظمة، مثل الدخول أو البقاء غير المشروع، أو عرقلة سير النظام، أو إدخال وتعديل المعطيات بطريقة غير مشروعة. ويُلاحظ أن هذه النصوص تتسم بطابع وقائي وزجري في آن واحد، إذ لا تقتصر على الأضرار المحققة، بل تمتد لتشمل الأفعال التي من شأنها تعريض النظام للخطر.

فيتبيّن أن التشريع الجزائري، رغم حداثة تدخله، قد اعتمد إلى حدّ بعيد النهج الفرنسي، سواء من حيث بنية النصوص أو طبيعة الأفعال المجرّمة، مع محاولة تكييفها مع البيئة القانونية الوطنية. كما أن الاتجاه الفقهي الغالب يسير نحو تبني مفهوم مركّب للجريمة المعلوماتية يجمع بين وسيلة ارتكابها ومحلها، بما يسمح باستيعاب مختلف صور الاعتداءات الرقمية، وهو ما يُمهّد لتكييف أدقّ لجريمة القرصنة الإلكترونية باعتبارها إحدى أبرز تطبيقاتها، فيعتمد كلا النظامين الفرنسي والجزائري على تعداد الأفعال المجرمة، وهو ما يمنح مرونة في التطبيق[2]

ومنه يمكن القول أن جريمة القرصنة الإلكترونية في التشريع الجزائري تقوم على حماية الأنظمة المعلوماتية والمعطيات الرقمية من أي اعتداء غير مشروع، من خلال تجريم الأفعال المرتبطة بالاختراق

[1] مزوزي إكرام، الحاج علي بدر الدين، **مرجع سابق**، ص 313.

[2] مناصرة يوسف، **الدليل الإلكتروني في القانون الجزائي، الطريق نحو أدلة الإثبات في المادة الجزائية، دراسة مقارنة**، دار الخلدونية، 2021، ص 12

والتلاعب، مع اعتماد مقاربة عملية تركز على السلوك الإجرامي بدل التعريف النظري، وهو ما يجعلها من الجرائم ذات الطبيعة التقنية المتجددة التي تتطلب تأطيرا قانونيا مستمرا[1].

ب_ القانون رقم 24-06 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، يعدل ويتمم الأمر رقم 66-156.

مس القانون رقم 24-06 [2]المؤرخ في 28 أبريل المنظومة الجزائية الجزائرية أي وسع الحماية الجزائية في بعض الجوانب ذات الصلة بالبيئة الرقمية لكنه لم يتضمن نصوصًا مستقلة تتعلق بجريمة القرصنة الإلكترونية، ولم يمس المواد 394 مكرر وما بعدها من قانون العقوبات، وإنما اقتصر دوره على تعديل بعض أحكام السياسة الجزائية وتعزيز الحماية الجنائية للمعطيات والخصوصية الرقمية، مما يجعل الإطار القانوني للقرصنة الإلكترونية لا يزال خاضعًا أساسًا لتعديل 2004 (القانون 04-15)[3].

ج_ التجريم في القوانين المكملة

فإلى جانب الأحكام المنصوص عليها في الأمر 66-156 المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 04-15، والتي كرست التجريم الصريح لأفعال المساس بأنظمة المعالجة الآلية للمعطيات، عمل المشرع على تدعيم هذا الإطار بجملة من القوانين الخاصة التي توسع نطاق الحماية الجنائية، ويبرز في هذا السياق القانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي، القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين المعدل والمتمم بموجب القانون 26-02 ، وكذا القانون 18-05 المتعلق بالت

1_ التجريم في القانون 03-05 بتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 73-14.

ادخل المشرع الجزائري تعديلا بموجب الأمر 03-05 المؤرخ في 2003/07/19 على الأحكام القانونية لحماية البرامج التي أنشأها الأمر 97-10 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة، بالإضافة إلى التعديل الخاص بقانون العقوبات 04-15المؤرخ في 2004/11/10 المعدل والمتمم

[1]عبد الفتاح بيومي حجازي، مرجع سابق، ص 83.

[2] قانون رقم 24-06 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 30، المؤرخ في 30 أبريل سنة 2024.

[3] القانون رقم **24-06** المؤرخ **في 28 أفريل 2024**، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 31، الصادر بتاريخ 30أفريل 2024.

للأمر 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات، الذي عالج المساس بأنظمة المعالجة الآلية للبيانات[1].

كما عرفت المادة 2 من الآمر 03-07 أن الاختراع هو " فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية[2] "

يُقصد بالاختراع في الإطار القانوني أنه ثمرة جهد ذهني وتقني يؤدي إلى إيجاد حل عملي لمشكلة معينة في مجال التكنولوجيا، سواء تعلق الأمر بابتكار شيء غير مسبوق أو الكشف عن عنصر قائم لم يكن معروفًا من قبل وإبرازه للاستغلال الصناعي. وقد اختلف الفقه في تحديد معيار أهميته، فذهب اتجاه إلى أن قيمة الاختراع لا تتوقف على مدى مردوده الصناعي، بينما يرى اتجاه آخر أن استحقاق الحماية القانونية يظل مرتبطًا بمدى إسهامه في تحقيق تقدم تقني يتجاوز القدرات العادية للخبير المهني. أما نظام براءة الاختراع، فيُفهم في مدلوله القانوني كمنظومة من القواعد التي تنظم شروط منح البراءة وإجراءاتها وآثارها، في حين تعد البراءة في حد ذاتها سندا رسميا تمنحه السلطة المختصة للمخترع، تخوله بموجبه حق الاستغلال الحصري لاختراعه لمدة محددة وفي إطار شروط قانونية معينة. وللاستفادة من هذه الحماية، يتعين أن يتوافر في الاختراع عدد من الشروط الجوهرية، تتمثل أساسًا في الجدة، وقيام نشاط ابتكاري وقابليته للتطبيق الصناعي[3].

ولا تقتصر هذه الأفعال على النقل المادي للبرامج (كالأقراص)، بل تشمل أيضا النشر عبر الوسائط الرقمية، خاصة من خلال شبكة الإنترنت، مما يضفي عليها طابعًا عابرًا للحدود ويزيد من خطورتها[4]. أما من حيث أركان الجريمة، فيتمثل الركن المادي في كل سلوك يؤدي إلى الاعتداء على أحد حقوق المؤلف دون ترخيص، ويكون محل هذا الاعتداء هو المصنف المحمي، بما في ذلك برامج الحاسوب التي اعترف بها القانون كمصنفات أدبية. ومع ذلك، فإن حق المؤلف في منع النسخ ليس مطلقًا، إذ يرد عليه

---

[1] فيصل بدري، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، مرجع سابق، ص 125.

[2] المادة 3 من الأمر 03-07 تنص على "**أن الاختراع يكون قابلا للحماية إذا توافرت فيه الشروط التالية: الخبرة النشاط الابتكاري_ القابلية للتطبيق الصناعي و4 من لأمر 03-07 المتعلق ببراءة الاختراع تنص على أنه "يعتبر الاختراع جديدا إذا لم يكن داخلا ضمن حالة التقنية السابق أي لم يتم الكشف عنه للجمهور من قبل، سواء بالوصف، أو الاستعمال، أو أية وسيلة أخرى.**

[3] فيصل بدري، نفس المرجع، ص 128.

[4] بدري فيصل، **نفس المرجع**، ص 143.

بعض الاستثناءات التي يسمح فيها القانون بالنسخ في حدود ضيقة، كالاستخدام الشخصي أو لأغراض تعليمية، وفق الشروط المحددة قانونا[1].

وبهذا يتضح أن حماية برامج الحاسوب في إطار حق المؤلف تُشكل آلية أساسية لمكافحة القرصنة الإلكترونية، خاصة مع تطور وسائل النسخ والنشر الرقمي التي سهلت من انتشار هذه الاعتداءات .

2_ تجريم القرصنة الإلكترونية في القانون 09-04 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصالات إلى جانب قانون العقوبات

جاء القانون المؤرخ في 05 أوت لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصالات إلى جانب قانون العقوبات، فنجد القانون 09-04 السابق الذكر الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وطرق مكافحتها كجانب وقائي للحد من الجرائم المعلوماتية، وهو أهم قانون إجرائي خاص، ينظم التحري الإلكتروني، جمع الأدلة، التعاون الدولي، مراقبة الاتصالات، وهذا عن طريق ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتسجيل وتجميع محتواها في حينها مع القيام بإجراءات التفتيش داخل المنظومة المعلوماتية.

وقد عبر هذا القانون عن الجريمة المعلوماتية باختياره لمصطلح " المساس بأنظمة المعالجة الآلية للمعطيات"، وقد اعتبر المشرع النظام المعلوماتي في حد ذاته بكل ما يشتمله من مكونات غير مادية محلا للجريمة، فقد نصت المادة 02 من القانون المذكور أعلاه في الفقرة "أ" على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو تسهل ارتكابها عن طريق منظومة معلوماتية أو أنظمة الاتصالات الالكترونية، وعرفت الفقرة "ب" من نفس المادة المنظومة المعلوماتية بأنها " مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".[2]

3_التجريم في القانون 18-05 المؤرخ في 10 ماي 2018 والمتعلق بالتجارة الإلكترونية

ان القانون 18-05 جاء لتنظيم المعاملات التجارية عبر الإنترنت، وضبط العلاقة بين المورد الإلكتروني، المستهلك، مزودي خدمات التطبيقات، المنصات الرقمية، وتعتبر التجارة الإلكترونية كل نشاط يتم عبر شبكة الإنترنت لبيع أو شراء السلع أو الخدمات تشمل المواقع التجارية، التطبيقات،

[1] قارة أمال، **مرجع سابق**، ص 85.

[2] المادة **02 من الأمر 09-04** المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، سنة 2009.

المنصات الرقمية، فيهدف القانون إلى تنظيم المعاملات الالكترونية، حماية المستهلك الإلكتروني، ضمان الشفافية، مكافحة الغش والاحتيال الإلكتروني.[1]

القانون 18-05 يكمل قوانين الجرائم الإلكترونية من خلال حماية المستهلك من الاحتيال الرقمي، تنظيم المعاملات التي قد تكون محل اختراق[2]

4_ تجريم القرصنة الإلكترونية في قانون التوقيع والتصديق الإلكتروني 15-04

المؤرخ في 1 فيفري 2015 المعدل والمتمم بموجب القانون رقم 26-02 المؤرخ في 17 فبراير 2026 يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية.

يهدف هذا القانون إلى إعطاء الحجية القانونية للوثائق الإلكترونية وكذا تأمين المعاملات عبر الإنترنت ، ومكافحة التزوير الإلكتروني، فيتمثل التوقيع أساسا في بيانات إلكترونية تستخدم لتحديد هوية صاحب التوقيع والمصادقة على الوثيقة مثل التوقيع عبر شهادة رقمية، الرموز المشفرة، أما التصديق الإلكتروني فهو عملية التحقق من صحة التوقيع بواسطة جهة معتمدة مثل هيئات التصديق الإلكتروني، كما أن له نفس الحجية القانونية للتوقيع العادي و يعتمد كدليل أمام القضاء، أين يعاقب القانون على تزوير التوقيع الإلكتروني، واستعمال التوقيع المزور، اختراق وسائل التصديق، إنتهال الهوية الرقمية [3]

حيث أن المادة 113 من القانون الجديد تنص على انه تواصل السلطة الوطنية للتصديق الإلكتروني والسلطة الحكومية ممارسة مهامها بموجب القانون رقم 15-04 المذكور أعلاه إلى غاية التنصيب الفعلي للسلطة[4].

ج_ تجريم القرصنة الإلكترونية في القانون 18-07 المؤرخ في 10 جوان سنة 2018 المتعلق بحماية الأشخاص الطبيعيين المعدل بموجب القانون رقم 25-11 المؤرخ في 24 جويلية 2025

---

[1] القانون رقم 18-05، مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 28، المؤرخ في 16 مايو 2018، ص. 4 وما بعدها.

[2] القانون رقم **18-05 المؤرخ في 10 ماي 2018، المتعلق** بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، الصادر بتاريخ 16 ماي 2018.

[3] القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 6.

المعدل والمتمم بموجب القانون رقم 26-02 المؤرخ في 17 فبراير 2026 يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية العدد14.

القانون 18-07 المؤرخ في 10 جويلية سنة 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي يهدف إلى تكريس حماية قانونية فعالة للأشخاص الطبيعيين عند معالجة معطياتهم ذات الطابع الشخصي، ويقصد بهذا الشخص كل فرد طبيعي ترتبط به بيانات شخصية، ساء بشكل مباشر أو غير مباشر، وهو ما أكدته المادة الثالثة من القانون التي عرفت الشخص المعني بأنه كل شخص طبيعي تكون معطياته محل المعالجة.

وفي هذا الإطار، وضعت المادة الثانية مجموعة من المبادئ الأساسية التي يجب احترامها عند معالجة البيانات، من بينها ضرورة احترام الكرامة الإنسانية، والحياة الخاصة، والحريات العامة، مع عدم المساس بحقوق الأشخاص أو شرفهم أو سمعتهم، وتعكس هذه المبادئ توجه المشرع نحو تأطير استعمال المعطيات الشخصية ضمن ضوابط قانونية وأخلاقية، خاصة في ظل توسع خدمات الاتصال الرقمي وتزايد الجهات التي تقوم بجمع معالجة البيانات.

يعتبر هذا القانون مكملا وأساسياً لأنه يضمن حماية البيانات والتي تعتبر محل للجريمة والتي تكون مستهدفة من طرف القراصنة الذين يقومون باختراق قواعدها وسرقة المعلومات الشخصية وتسريب بيانات حساسة، فيظهر جليا دور القانون18-07 كونه يحدد ماهي البيانات الشخصية ويقرر أنها محل حماية قانونية (مثل سرية البيانات و عدم معالجتها دون إذن)

وفي إطار تحيين هذا الاطار التشريعي، صدر القانون رقم 25-11 المؤرخ في 24 يوليو سنة2025، المعدل و المتمم للقانون رقم 18-07، والذي جاء بمجموعة من المستجدات الرامية إلي تعزيز الحماية القانونية للمعطيات ذات الطابع الشخصي ومواكبة التطورات التي فرضتها البيئة الرقمية، فشملت إعادة تنظيم بعض الأحكام المتعلقة بمعالجة المعطيات، وادراج أحكام جديدة ذات صلة بمعالجة المعطيات لأغراض الشرطة والعدالة، فضلا عن استحداث وتعزيز بعض المفاهيم المرتبطة بحماية المعطيات الشخصية[1].

المبحث الثاني: صور جريمة القرصنة الإلكترونية وأحكامها القانونية

تعتبر القرصنة الإلكترونية من أبرز صور الإجرام الذي ارتبط بالانتشار الواسع لتكنولوجيات الإعلام والاتصال، حيث خلق بيئة رقمية معقدة أتاحت إمكانيات غير مسبوقة للتدخل غير المشروع في الأنظمة المعلوماتية والمعطيات الرقمية، وقد أدى هذا التحول إلى ظهور أنماط جديدة من الاعتداءات التي لم تعد

القانون رقم 25-11 المؤرخ في 24 يوليو سنة 2025، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع [1]الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، 2025

تقتصر على الوسائل التقليدية، بل أصبحت تعتمد على تقنيات متطورة تستهدف سلامة نظم المعالجة الآلية للمعطيات وسريتها[1].

وفي ظل هذه الخصوصية، لم يعد من الممكن إخضاع جريمة القرصنة الإلكترونية للقواعد العامة، بل استلزم الأمر تحديد أركانها على نحو دقيق يراعي طبيعتها التقنية، باعتبارها الإطار الذي يحدد متى يقوم الفعل المجرم وتتحقق به المسؤولية الجزائية، إذ لا يكفي مجرد وقوع سلوك مادي في البيئة الرقمية، بل يتعين توافر مجموعة من العناصر القانونية التي تبرر إسناد الفعل إلى مرتكبه.

وتتمثل هذه الأركان، على غرار سائر الجرائم، في الركن المادي الذي يعكس النشاط الإجرامي، والركن المعنوي الذي يتصل بالإرادة الإجرامية والقصد الجنائي، فضلًا عن الركن الشرعي الذي يقتضي وجود نص قانوني يجرّم الفعل ويقرر له جزاءً،

وتكمن أهمية تناول أركان جريمة القرصنة الإلكترونية في إبراز الخصوصيات التي تميزها عن باقي الجرائم الإلكترونية سواء من حيث طبيعة محل الاعتداء الذي يتمثل في المعطيات والأنظمة المعلوماتية، أو من حيث الوسائل المستعملة في ارتكابها، كما يتيح هذا التحليل الوقوف على مدى كفاية النصوص القانونية في استيعاب مختلف صور السلوك الإجرامي المعلوماتي، ومدى قدرتها على تحقيق الحماية الجنائية المطلوبة.

وعليه، فإن دراسة جريمة القرصنة الإلكترونية تقتضي تحليل كل سلوك إجرامي على حدي، مع بيان خصائصه وتطبيقاته في المجال الرقمي، بما يسمح بتحديد الإطار القانوني الذي تقوم في ظله هذه الجريمة وتترتب عنه المسؤولية الجزائرية، وهو ما سنعرضه من خلال هذا المطلب.

المطلب الأول: صورة الدخول والبقاء غير المشروعين

يري بعض الاتجاه ضرورة إضافة قسم مستقل للجرائم الإلكترونية، منفصلا عن الأجزاء التقليدية لكونها تمثل قيمة اقتصادية جديدة ذات طبيعة خاصة، ويرى البعض الآخر أنه من الأفضل إلحاق كل جريمة إلكترونية بما يقابلها في قانون العقوبات التقليدي، كإدراج التزوير المعلوماتي ضمن جرائم تزوير المحررات والاعتداء على المعطيات ضمن جريمة الإتلاف[2].

[1] حسين طاهري، **جرائم القرصنة الالكترونية**، مرجع سابق، ص 93.

[2] غنية باطلي، **مرجع سابق**، ص 148.

كما أن إشكالية المصطلح القانوني (القرصنة/ الدخول غير المشروع) تعد الطريقة أو المصطلحات التقنية من المسائل المعقدة المرتبطة بمكافحة الجريمة الإلكترونية ذات الطابع التقني، حيث تعتمد غالبًا على منطق قانوني يهدف إلى ضبط المفاهيم التقنية في إطار تشريعي واضح.

وفي هذا السياق، يبرز اختلاف بين النظم القانونية الأنجلوسكسونية التي تميل إلى تحديد دقيق ومسبق لمفاهيم الصلاحية التقنية المرتبطة بالبيانات والبرامج وأنظمة المعالجة، وبين النظم اللاتينية، وخاصة التشريع الفرنسي التقليدي، الذي يعتمد أكثر على المرونة في تحديد المصطلحات ويترك مجالًا أوسع لتفسير القاضي في إطار القواعد العامة للتفسير الجنائي

أما في التشريع الجزائري، فقد تم اعتماد مقاربة مزدوجة تجمع بين الاتجاهين، نظرا للتطور السريع لتكنولوجيا الإعلام والاتصال وعدم قدرة القواعد التقليدية للقانون الجنائي على مواكبة هذا التطور بشكل كامل، لذلك تم إدماج صور من هذه الجرائم ضمن قانون العقوبات، إلى جانب استحداث نصوص خاصة تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، [1]وذلك استجابة لمتطلبات التجريم الحديثة[2]. وقد جاء هذا التوجه أيضًا متأثرًا بالاتفاقيات الدولية والشراكات القانونية، بما في ذلك التعاون بين الجزائر والاتحاد الأوروبي في مجال مكافحة الجريمة المنظمة والجرائم المعلوماتية، وما تضمنته من آليات للتنسيق وتبادل المساعدة القضائية [3].

تنص المادة 394 مكرر من قانون العقوبات الجزائري على " يعاقب بالحبس من ثلاثة أشهر ستة أشهر إلى سنتين وبغرامة من60000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك

إن فعل الدخول يتحقق في حالات متعددة على سبيل المثال، كأن يتضمن الصفحة في جرائم الدخول إلى حسابات الغير مثلاً، غير أن القانون لم يعرف جرائم الدخول على نحو دقيق، مما دفع بعض الفقه الجنائي لزعم أنه على وشك الافتراق التي يمكن فيها الدليل على أن يكون الدخول إلى النظام كله أو حتى الانفصال عنه.

---

[1]R. Gassin, **ibid**, p9.

[2]عبد القادر القهوجي، **مرجع سابق**، ص 129.

[3] غنية بالطي، **نفس المرجع**، ص 148

إن الإشكال المطروح هنا: من يملك الحق بإعطاء الترخيص بالدخول؟ وما هي الحالات التي يكون فيها الدخول غير مصرح به؟ وهو ما سنتطرق إليه لاحق في فعل الدخول غير المشروع كركن مادي من أركان الجريمة

الفرع الأول: جريمة الدخول غير المشروع

تتجلى جريمة الدخول غير المشروع إلى منظومة المعالجة في سلوك غير مشروع يمس أمن الأنظمة المعلوماتية وسلامتها، وقد عالجها كل من التشريع الجزائري والتشريع الفرنسي من خلال تحديد صورها البسيطة والمشددة[1].

ففي التشريع الجزائري، يجرم القانون فعل الدخول والبقاء غير المشروع داخل نظام معلوماتي عن طريق الغش، سواء تم ذلك كليا أو جزئيا، حتى ولو كان في مرحلة الشروع، وتقوم هذه الجريمة في صورتها البسيطة بمجرد تحقق فعل الدخول أو البقاء غير المشروع دون أن يترتب عنها أي أثر ضار على النظام، وتعاقب بعقوبات أصلية تتمثل في الحبس والغرامة

أما في صورتها المشددة، فإن الجريمة تأخذ طابع أكثر خطورة تنتج عن الفعل إحداث خلل أو تعطيل في النظام أو إتلاف أو تغيير في المعطيات، وهو ما يبرر تشديد العقوبة بالنظر إلى حجم الضرر المترتب عن المساس بوظائف النظام المعلوماتي.

وبالمقارنة، اعتمد المشرع الفرنسي نفس التدرج التقريبي في التجريم، حيث فرّق بين الدخول و البقاء غير المشروعين داخل النظام في صورته البسيطة، وبين الحالة التي يترتب عنها تعطيل أو تغيير في البيانات أو الإضرار بوظائف النظام[2].

وعليه، يمكن استخلاص أن هذه الجريمة تتخذ صورتين أساسيتين: صورة بسيطة تتحقق بمجرد الدخول أو البقاء غير المشروع دون أثر مادي على النظام، وصورة مشددة تقوم عند ترتب نتيجة ضارة تمس سلامة المعطيات أو كفاءة تشغيل المنظومة، وهو ما يعكس منطق التدرج في الحماية الجنائية للأنظمة المعلوماتية[3].

أولا: الركن الشرعي لجريمة الدخول غير المشروع

يتمثل الركن الشرعي لجريمة الدخول غير المشروع في وجود نص قانوني يجرّم هذا السلوك ويحدد العقوبة المقررة له، تطبيقًا لمبدأ شرعية الجرائم والعقوبات. وقد كرّس المشرّع الجزائري هذا المبدأ في المادة الأولى من قانون العقوبات، التي تقضي بأنه لا جريمة ولا عقوبة أو تدبير أمن بغير قانون

[1] غنية باطلي، **مرجع سابق**، 150.

[2] Code pénal français, article 323-1, relatif à l'accès ou au maintien frauduleux dans un système de traitement automatisé de données, Version en vigueur.

[3] عبد القادر القهوجي، مرجع سابق، ص 129

وفي مجال الجرائم المعلوماتية، خصّ المشرّع الجزائري الدخول غير المشروع بنص جزائي صريح، يتمثل في المادة 394 مكرر من قانون العقوبات، المعدّلة بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024. وتعاقب هذه المادة كل من يدخل أو يبقى، عن طريق الغش، في كل أو جزء من منظومة المعالجة الآلية للمعطيات، أو يحاول ذلك

وتكمن أهمية هذا النص في أنه يجرّم الدخول غير المشروع في حد ذاته، دون اشتراط أن يترتب عليه بالضرورة حذف المعطيات أو تغييرها أو تخريب نظام اشتغال المنظومة؛ فهذه النتائج تخضع للأحكام التي خصّصها المشرّع لها ضمن المادة نفسها.

ويُفهم من ذلك أن الحماية الجزائية لا تقتصر على سلامة المعطيات أو منع إتلافها، وإنما تمتد إلى حماية النظام المعلوماتي من الولوج غير المشروع ذاته

وتكون العقوبة وفق الصيغة المعدلة للمادة 394 مكرر بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024، كما يأتي:

الدخول و البقاء عن طريق الغش أو محاولة ذلك الحبس من 6 أشهر إلى سنتين، وغرامة من 60.000 إلى 200.000 دج

إذا ترتب على الفعل حذف أو تغيير معطيات المنظومة تضاعف العقوبة

إذا ترتب على الفعل تخريب نظام اشتغال المنظومة الحبس من سنة إلى 3 سنوات، وغرامة من 100.000 إلى 300.000 دج

يتضح من صياغة المادة 394 مكرر أن المشرّع الجزائري حدد ثلاث صور أساسية للسلوك المجرّم

الدخول غير المشروع: يتحقق عندما يلج الفاعل إلى كل النظام المعلوماتي أو جزء منه عن طريق الغش، دون أن يكون له حق في ذلك.

البقاء غير المشروع: يتحقق عندما يستمر الفاعل في الوجود داخل النظام المعلوماتي بعد زوال حقه في الدخول و الاستمرار فيه، متى توافرت شروط التجريم.

محاولة الدخول و البقاء: أدرجها المشرّع صراحة ضمن نطاق التجريم، فلا يتوقف تطبيق النص بالضرورة على نجاح محاولة الدخول.

ثانيا: الركن المادي لجريمة الدخول غير المشروع

تعتبر هذه الجريمة من أخطر الجرائم المعلوماتية وأكثرها انتشارا، إذ قد تسبب في الكثير من الأحيان في حدوث جرائم أخرى حيث أن الدخول إلى الأنظمة المعلوماتية يعد شرطا لارتكاب أفعال إجرامية لاحقة ولذلك فإن المشرع الجزائري أعطاها أهمية خاصة حيث أنه نص على أركانها وعقوبتها[1].

[1] معاشي سميرة، **آليات مكافحة الجريمة المعلوماتية-دراسة مقارنة**-أطروحة دكتورا علوم في الحقوق تخصص قانون الأعمال جامعة محمد خيضر بسكرة،2019-2020، ص 83.

حرص المشرع الجزائري على تجريم كل سلوك يشكل دخولا غير مصرح به إلى أنظمة المعالجة الآلية للمعطيات سواء نتج عنه ضرر مادي أو لم يؤدى إلى نتيجة تذكر باعتبار أن مجرد الدخول يشكل في حد ذاته جريمة[1]، وقد نصت المادة 394 مكرر على تعريف الدخول و البقاء غير المشروع وهناك من عرف الدخول غير المصرح به بأنه الوصول إلى المعطيات والمعلومات داخل النظام المعلوماتي دون موافقة أو ترخيص من المسؤول على هذا النظام[2].

كما يمكن تعريفه أيضا بأنه سوء استعمال الحاسوب ونظامه من طرف شخص غير مخول له يقوم بالدخول إليه بغرض الوصول إلى البيانات والمعلومات المخزنة، سواء كان ذلك للاطلاع عليها أو بدافع التسلية، أو لمجرد إشباع رغبة في إثبات قدرته على اختراق النظام.

ومن صوره أيضا أنه يجد الجاني نفسه داخل نظام المعالجة الآلية للمعطيات مصادفة ودون قصد منه، إلا أنه بعد أن يدرك وجوده في النظام يستمر داخله ولا ينسحب في الوقت الذي كان يجب عليه مغادرته[3].

ولا يشترط القانون توفر صفة محددة في الشخص الذي يقوم بالدخول و البقاء غير المشروع حيث نصت المادة 394 مكرر بعبارة كل من يدخل أو يبقى كما لم تحدد طريقة معينة لارتكاب الفعل فجاء النص عاما وشاملا[4].

ومنه يستوجب التطرق إلى كل من فعل الدخول وفعل البقاء وفق الاتي:

أ-فعل الدخول غير المشروع

يقصد بفعل الدخول غير المصرح بجريمة الولوج غير المشروع إلى نظام المعالجة الآلية للمعطيات، أي تمكن شخص من النفاذ إلى نظام معلوماتي أو إلى جزء منه دون إذن صاحب الصلاحية، سواء تم ذلك باستعمال طرق احتيالية أو تقنيات أو حتى نتيجة استغلال ثغرات في النظام، ولا يشترط أن يترتب عن هذا الدخول إحداث ضرر فعلي، إذ يكفي تحقق فعل النفاذ في حد ذاته لقيام الجريمة.

---

[1] قارة أمال، **مرجع سابق**، ص 32.

[2] معاشي سميرة، **مرجع سابق**، ص 84.

[3] خالد حسن أحمد لطفي، **مرجع سابق**، ص .61

3 غنية باطلي، **مرجع سابق**، ص 152.

ويفهم "الدخول" هنا بمعناه غير المادي، أي الولوج إلى وظائف المنظومة الفكرية التي يقوم عليها النظام المعلوماتي، وليس مجرد الدخول الفيزيائي إلى مكان تواجد الأجهزة[1]، لذلك فهو أقرب إلى اختراق البنية المنطقية للنظام أو التفاعل مع معطياته وبرامجه، وليس إلى اقتحام مادي لموقع معين كما أن التمييز بين "الدخول إلى النظام" و"الدخول فيه" لا يترتب عليه أثر قانوني مهم، لأن المشرع يعاقب على مجرد النفاذ، سواء كان كليا أو جزئيا. وبالتالي يصل شخص إلى عنصر من عناصر النظام حتى تتحقق الجريمة، كما أنه لا يعتد أيضا بالوسيلة المستعملة، إذ يمكن أن يتم الدخول بشكل مباشر، مثل استخدام كلمة مرور صحيحة دون ترخيص، أو إدخال برنامج داخل نظام أثناء تشغيله، أو بشكل غير مباشر، كالوصول عن بعد عبر الشبكات، خاصة الإنترنت[2].

وفي جميع الحالات العبرة ليست بطريقة الدخول بل بغياب الترخيص ومخالفة إرادة المسؤول عن النظر، فيعد الدخول غير مشروع حتى في حالات التي يبدأ فيها بشكل عرضي أو عن طريق الخطأ، إذا استمر الشخص في التصفح أو الاستغلال بعد علمه بعدم أحقيته في ذلك، فالقانون يرتب المسؤولية على الاستمرار في الولوج غير المصرح به[3].

كما أن هذه الجريمة من الجرائم التي يصعب إثباتها عمليا، نظرا لطابعها غير المادي، وإمكانية محو أثارها أو الادعاء بعدم القصد، وهو ما يجعل الإثبات يعتمد غالبا على القرائن التقنية، ولا تؤثر صفة الفاعل في قيام الجريمة، إذ يكفي أن يكون غير مخول بالدخول، حتى ولو لم يحقق فائدة أو لم يلحق ضررا بالنظام، فالحماية القانونية لا تنصرف إلى صون سرية وسلامة الأنظمة المعلوماتية، سواء تعلقت بمصالح خاصة أو ببيانات ذات طابع حساس كأسرار الدولة أو المؤسسات.

1: صور الدخول غير المشروع

يُعدّ الدخول غير المشروع إلى نظام المعالجة الآلية للبيانات من أبرز صور الاعتداء على سلامة الأنظمة المعلوماتية، وقد أولاه المشرع الجزائري عناية خاصة من خلال تجريم فعل الدخول و البقاء غير المشروعين في النظام، متى توافرت الشروط التي يتطلبها النص الجزائي

[1] غنية بالطي، مرجع سابق، ص 151.

[2] سميرة معاشي، مرجع سابق، ص 89-90

[3] عمر محمد أبو بكر يونس، **الجرائم الناشئة عن استخدام الانترنت**، أطروحة دكتوراه، جامعة عين شمس، القاهرة، 2004، ص 320

وبالرجوع إلى التشريع الجزائري، يتضح أن التجريم لا ينصرف إلى مجرد الاتصال التقني بالنظام في حد ذاته، وإنما يتعلق بالدخول أو البقاء فيه على نحو غير مشروع، بما يشكل اعتداءً على نظام معلوماتي لا يملك الفاعل حق الولوج إليه أو الاستمرار فيه. ومن ثم، يمكن التمييز بين صورتين للسلوك الإجرامي، تتمثل أولاهما في الدخول غير المشروع إلى النظام، وتتحقق عندما يلج الفاعل إلى النظام دون أن يكون مخولًا بذلك، في حين تتمثل الثانية في البقاء غير المشروع، وتتحقق عندما يكون الدخول في الأصل مشروعًا، ثم يستمر الفاعل في النظام رغم انتفاء السند الذي يجيز له ذلك

ولتحديد مدى خصوصية هذا التجريم في التشريع الجزائري، يمكن الاستئناس بالتشريع الفرنسي باعتباره من التشريعات التي عالجت مبكرًا الاعتداءات الواقعة على أنظمة المعالجة الآلية للبيانات، حيث نصت المادة 323-1 من قانون العقوبات الفرنسي المعدل بالمادة 06 من القانون رقم 22-2023 على تجريم فعل «الدخول» و «البقاء» بصورة احتيالية في كل أو جزء من نظام معالجة آلي للبيانات. ويُفهم من ذلك أن المشرع الفرنسي، شأنه في ذلك شأن المشرع الجزائري، يميز من الناحية السلوكية بين الولوج غير المشروع إلى النظام والاستمرار فيه دون سند مشروع

ويذهب جانب من الفقه الفرنسي، في تفسيره لهذه المادة، إلى التمييز بين حالتين: تتمثل الأولى في الولوج إلى النظام دون وجود ترخيص سابق، بينما تتمثل الثانية في الولوج الذي يكون مشروعًا في بدايته، ثم يتحول إلى بقاء غير مشروع بسبب تجاوز حدود الترخيص الممنوح أو انتهاء المدة أو الغرض الذي أجيز من أجله الاتصال بالنظام. وبذلك لا يكون محل التجريم في الحالة الثانية هو الدخول ذاته، وإنما استمرار الفاعل في النظام بعد زوال المشروعية التي كانت تبرر وجوده فيه[1]

1.1-حالة انعدام الترخيص كليا:

وهي الحالة التي لا يكون فيها للشخص أية علاقة بالنظام، كأن يكون من أحد العاملين الذين لا تدخل في وظيفتهم الاتصالات بهذا النظام أو معطياته.

في كلا الحالتين (عدم وجود الترخيص أو انقضائه) فإن الدخول إلى النظام يعد غير مشروع، من خلال تحديد مجال الترخيص الممنوح له، أي أن يكون عضو معين أو جهة معينة وقد يكون غير جائز

[1] خالد ممدوح إبراهيم، أمن المستندات الإلكترونية، الدار الجامعية، الإسكندرية، 2008، ص 148.

مطلق، فنجد من خلال المادة 1/323 من قانون العقوبات الفرنسي المعدلة بموجب المادة 06 من القانون رقم 22-2023 قد نلاحظ درجتين لتشديد العقوبة كالتالي:[1]

الدرجة الأولى (الولوج لأول مرة): تتحدد من طريقة الدخول، أي هل هو دخول إلى نظام المعالجة الآلية للمعطيات، أو أن هناك وسيلة تم استعمالها للدخول؟ فالمشرّع الجزائري لم يحدد الطريقة أو الوسيلة التي يتم بها الدخول، بل كل دخول غير مشروع يعتبر جريمة، مهما كانت الوسيلة التي يتم بواسطتها الدخول.[2]

***الدرجة الثانية (الولوج المتكرر أو المتعدد):** تتحدد من نية الفاعل، أي أن الدخول إذا كان بنية حسنة فإن الفاعل لا يعاقب على فعله، أما إذا كانت النية سيئة فإنه يعاقب، أي أن عنصر النية يلعب دوراً في تحديد الطابع الإجرامي للفعل، ومن ثم التأثير في عدم التقدير على الفاعل الذي يتجاوز النظام[3].

1_2حالة تجاوز حدود التصريح: في هذه الحالة قد يكون الدخول مصرح به، ولكن في حدود معيّنة، ولكن الفاعل يتجاوز هذه الحدود كان يكون التصريح لغايات محددة، فإذا به يتحول في النظام ويكون الفعل المادي للجريمة هو الدخول للبيانات التي يتجاوزها التصريح.

وحتى يتضح الأمر أكثر، نورد مثال موظف داخل مؤسسة له الحق في الدخول إلى قاعدة البيانات التي تخص القسم الذي يعمل فيه، إلا أنه تجاوز هذا الحد ودخل إلى أقسام أخرى لا تدخل ضمن نطاق اختصاصاته وعمليات كل قسم داخل المؤسسة، في هذه الحالة يكون فعله غير مشروع، لأن التصريح الذي بحوزته لا يتجاوز هذا الحد، فقد يكون الاختراق المادي تم بطريقة شرعية، ولكن التجاوز هو غير شرعي.

بذلك سنتكلم أولا على تجاوز المجال الذي حدده التصريح ثم الدخول القائم على أساس تجاوز النطاق والأهداف التي حددها التصريح[4].

---

[1] LEGISLATION BELGE, loi du 20-11-2000 sur la fraude informatique, 550 bis circonstances https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=01-02-03&numac=2001009035

[2] غنية باطلي، **مرجع سابق**، ص 156

[3] خليفة محمد، **مرجع سابق**، ص 149.

[4] نائلة عادل محمد فريد قورة، **مرجع سابق**، ص 346.

3-تجاوز النطاق المحدد للترخيص: في هذه الحالة يكون الشخص يملك تصريحًا بالدخول، لكن هذا التصريح ليس عاما، أي أنه غير مطلق لكل النظام، بل لقسم على بعض المناطق فقط، وعليه فإن الدخول إلى هذه المناطق بعد مرورها بالمناطق الأخرى يعد غير مشروع.[1]

فتحدد طبيعة الدخول حسب العلاقة بين العامل والقائم على النظام على النحو الذي يخول للعامل بالدخول يكون استخدامه مشروعاً، أما إذا تجاوز هذا العامل حدود منطقة معينة فإنه يكون بذلك قد تجاوز الحد المصرح له في النظام فيعتبر الدخول غير مشروع.

وهناك من يذهب إلى أن بعض المؤسسات تحدد للعمال مناطق معينة يمكنهم الدخول إليها ومناطق أخرى لا يمكنهم الدخول إليها، ويترتب عن ذلك أن الموظف أو العامل في حالة دخوله إلى نظام المعلومات للمناطق المصرح له بها، فإن فعله يكون مشروعاً، أما إذا تجاوز هذا الحد ودخل إلى مناطق غير مصرح له بها، فإن فعله يكون غير مشروع[2].

كما أن هناك حالات يكون فيها التصريح بالدخول عاماً أي دون تحديد الاختصاص، وهنا يجب التمييز بين النية السيئة والنية الحسنة للعامل، فإذا كانت النية سيئة، يكون الدخول غير مشروع، ويشكل بذلك تجاوزا لحدود التصريح الممنوح له، إلا أنه في النية الحسنة لا يمكن القول بذلك، إذ أن الفعل يكون غير معاقب عليه.

4-تجاوز الغرض المحدد للترخيص:

يثار تساؤل آخر في هذا السياق حول إذا ما كان الدخول قد استخدم لغير الذي مُنح لأجله الترخيص فهل يعتبر هذا تجاوزا للتصريح؟

تتخذ جريمة الدخول إلى أنظمة المعالجة الآلية للبيانات صورًا متعددة، ولا تقتصر على حالة الولوج إلى النظام دون الحصول على أي ترخيص مسبق، بل قد تتحقق كذلك عندما يكون الفاعل مرخصًا له بالدخول، ثم يتجاوز الحدود التي حددها له صاحب النظام، أو يستمر في البقاء داخله بعد زوال الترخيص.

وقد جرم المشرع الجزائري هذه الأفعال بموجب المادة 394 مكرر من قانون العقوبات، التي تعاقب كل من يدخل أو يبقى، بطريقة احتيالية، في كل أو جزء من نظام للمعالجة الآلية للبيانات. ويستفاد من

[1] غنية باطلي، **مرجع سابق**، نفس الصفحة.

[2] محمد خليفة، مرجع سابق، ص 149.

صياغة النص أن المشرع لم يحصر السلوك المجرّم في الدخول غير المرخص به ابتداءً، وإنما وسّع نطاق التجريم ليشمل كذلك حالة البقاء داخل النظام بصورة احتيالية[1]

وتظهر أهمية ذلك في الحالات التي يكون فيها الشخص حائزًا على ترخيص صحيح بالدخول إلى النظام، كالموظف الذي تمنحه المؤسسة التي يعمل بها صلاحية الاطلاع على قاعدة بيانات معينة في حدود المهام المسندة إليه، ثم يقوم بالدخول إلى بيانات أو ملفات أخرى لا يشملها نطاق الترخيص الممنوح له. ففي هذه الحالة، لا يكفي القول إن الفاعل كان يملك اسم مستخدم وكلمة مرور صحيحة لنفي الصفة غير المشروعة عن سلوكه، وإنما ينبغي تحديد نطاق الترخيص الذي مُنح له، وما إذا كان الدخول قد تم في حدود الغرض والصلاحيات التي حددها صاحب النظام

ومن ثم، نميز بين الدخول المشروع الذي يتم في حدود الترخيص الممنوح، وبين الدخول الذي يتجاوز حدود ذلك الترخيص. فإذا كان الموظف مخولًا بالدخول إلى جزء معين من النظام، ثم ولج عمدًا إلى جزء آخر غير مشمول بصلاحياته، فإن مشروعية الدخول الأصلي لا تمتد بالضرورة إلى الولوج الذي تم خارج نطاق الإذن. غير أن اعتبار هذا التجاوز جريمة وفق المادة 394 مكرر يظل رهينًا بتوافر جميع عناصر الجريمة، ولا سيما الطابع الاحتيالي والقصد الجنائي، إذ لا ينبغي أن يؤدي كل تجاوز إداري أو تقني للصلاحيات إلى قيام المسؤولية الجزائية بصورة آلية

أما إذا كان الدخول في بدايته مشروعًا، ثم انتهت مدة الترخيص أو سُحبت الصلاحية الممنوحة للشخص، واستمر رغم ذلك في الولوج إلى النظام أو البقاء فيه مع علمه بزوال الإذن، فإن الأمر يختلف، إذ يمكن أن ينصرف التجريم هنا إلى صورة البقاء بطريقة احتيالية التي نصت عليها المادة 394 مكرر. فالعبرة في هذه الحالة لا تكون فقط بمشروعية الدخول الأول، وإنما كذلك بالوضع القانوني للفاعل أثناء استمرار وجوده داخل النظام[2]

ولتوضيح ذلك في الواقع العملي الجزائري، يمكن تصور حالة موظف في مؤسسة مصرفية أو إدارية مُنح صلاحية محددة للدخول إلى نظام معلوماتي أثناء فترة عمله، ثم انتهت علاقته الوظيفية أو سُحبت منه صلاحية الدخول، ومع ذلك استعمل بيانات الدخول التي كانت بحوزته للولوج إلى النظام والاستمرار في

[1] أنظر: المادة 394 مكرر، المرجع نفسه

[2] أنظر: عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، ديوان المطبوعات الجامعية، الجزائر،2005، ص399.

الاطلاع على المعلومات المخزنة فيه. ففي هذه الحالة، فإن انتهاء الترخيص يمثل عنصرًا مهمًا في تقدير مشروعية البقاء، ويقتضي من جهة التحقيق والقضاء التحقق من تاريخ انتهاء الصلاحية، وطبيعة الإذن الممنوح، وعلم الفاعل بزواله، وكيفية استمراره في الولوج، والغاية التي كان يستهدفها من ذلك

وعليه، فإن موقف المشرع الجزائري يمكن تحليله على أساس التمييز بين أربع حالات: أولًا، الدخول إلى النظام دون أي ترخيص؛ ثانيًا، الدخول بترخيص صحيح وفي حدود الصلاحيات الممنوحة؛ ثالثًا، الدخول بترخيص صحيح مع تجاوز حدود الصلاحية؛ ورابعًا، الدخول المشروع في بدايته ثم الاستمرار في النظام بعد انتهاء الترخيص أو سحبه[1]

وفي تقديرنا، فإن الحالة الثالثة لا ينبغي أن تُكيف جزائيًا بصورة آلية لمجرد حصول تجاوز للصلاحيات، وإنما يجب التحقق من طبيعة التجاوز ومدى انصراف القصد إلى الولوج غير المشروع، فضلًا عن توافر العنصر الاحتيالي الذي يتطلبه النص. أما الحالة الرابعة فتقترب بصورة أوضح من صورة البقاء غير المشروع متى ثبت علم الشخص بزوال الترخيص واستمراره عمدًا في النظام رغم ذلك

ويكشف هذا التحليل أن المعيار لا يتمثل في مجرد امتلاك الفاعل لوسيلة تقنية تسمح له بالدخول، كاسم المستخدم أو كلمة المرور، وإنما في حدود الإذن الممنوح له ومداه من حيث الموضوع والأشخاص والمدة والغرض. ولذلك فإن الترخيص لا يُفهم باعتباره إذنًا مطلقًا بالدخول إلى جميع مكونات النظام، وإنما هو إذن محدد بحدود معينة، ويترتب على تجاوزها طرح مسألة المشروعية الجزائية وفقًا لظروف كل واقعة

وبعد تحديد موقف التشريع الجزائري، يمكن الاستفادة من التجارب المقارنة، ولا سيما الفرنسية والإنجليزية والأمريكية، في توضيح الإشكالات التي يثيرها تجاوز حدود الترخيص، غير أن هذه المقارنة ينبغي ألا تحجب خصوصية النص الجزائري، وإنما تستخدم للكشف عن أوجه التشابه والاختلاف وتقييم مدى كفاية القواعد الوطنية في مواجهة الصور المستحدثة للاعتداء على أنظمة المعالجة الآلية للبيانات

ومن ثم، فإن خصوصية التجريم في هذه الحالة تكمن في ضرورة تحقيق التوازن بين حماية الأنظمة المعلوماتية من الولوج غير المشروع، وبين عدم التوسع في التجريم إلى الحد الذي يجعل كل مخالفة داخلية لقواعد استعمال النظام جريمة معلوماتية، إذ يظل قيام المسؤولية الجزائية مرتبطًا بتوافر

[1] القانون رقم 09_04 مرجع سابق

اختلفت المواقف بين كل من القضاء الانجليزي الأمريكي وكذا الفرنسي، بحيث يرى القضاء الإنجليزي أنه فعل مشروع وامتنع عن تطبيق نص المادة 01 من قانون إساءة استخدام الكومبيوتر والمتعلقة بالدخول الغير مصرح به في حالة تجاوز الغرض، وأبرز القضايا التي جاءت في سياق هذه المسألة هي قضية DPPv Bingell بالإضافة إلى قضية Rv. Bow, magistrate and Allisan.

في القضية الأولى، قام شرطيان بالدخول إلى نظام الحاسب الآلي الذي يعود للإدارة التابعين لها بغرض الحصول على معلومات خارج نطاق العمل، فحكمت المحكمة أولى درجة واستنادا لنص المادة 01 من قانون إساءة استخدام الكومبيوتر لسنة 1991 السابق ذكره بتهمة الدخول الغير مصرح به، غير أن محكمة الاستئناف قضت بخلاف ذلك وقامت بإلغاء الحكم، وارتأت أن المتهمان لهما حق الدخول وأن استخدام هذا الحق في العمل الغير مشروع لا ينف أن الدخول كان مصرحا به.[1]

القضية الثانية: تتمثل هذه القضية في رفض القضاء الإنجليزي تسليم إحدى العاملات في شركة American Expressالأمريكية لاتهامها بالدخول إلى نظام الحاسب الآلي للشركة والاطلاع على بيانات العملاء لأسباب لا تتعلق بالعمل، وذلك بعد طلب الحكومة الأمريكية تسليمها.

وقد رأت محكمة الاستئناف الإنجليزية أن هذا الفعل لا يُشكل جريمة بموجب القانون الإنجليزي، لأن العاملة كانت تمتلك صلاحية الدخول إلى النظام بحكم طبيعة عملها، حتى وإن كان استخدام هذه الصلاحية لأغراض غير مشروعة[2].

فقد رأت المحكمة أيضاً أن أحكام المادة 17 من القانون ذاته لا تُطبَّق إذا كان الشخص الذي قام بالدخول إلى النظام يملك صلاحية الدخول بحكم وظيفته، حتى لو استعمل تلك الصلاحية لأغراض غير مشروعة، إلا إذا نص القانون صراحة على خلاف ذلك، إلا أن قرارها من جهة أخرى أثار هذا جدلاً واسعاً، لكونه يضيق من نطاق تطبيق المادة المتعلقة بإساءة استخدام الحاسب الآلي في القانون الإنجليزي.

أما موقف القضاء الأمريكي، فقد كان مغايراً لذلك، إذ اعتبر أن الجريمة قائمة لأن الفعل يمثل خروجاً عن الإذن الممنوح من جهة العمل، وأن الدخول إلى النظام لأغراض لا ترتبط بالعمل هو دخول غير مشروع. ويُطلق على هذا الاتجاه في الفقه الأمريكي مصطلح EMPLOYEE MISCONDUCTCASES.

---

[1] نائلة عادل محمد فريد قورة، **مرجع سابق**، ص 349.

[2] خليفة محمد، مرجع سابق، ص 153.

ومن أبرز القضايا التي تناولها القضاء الأمريكي في هذا السياق قضيةSHURGAND، حيث قام موظف الشركة المدعى عليه، ERICLELAND، بالدخول إلى خطط العمل السرية الخاصة بالشركة وأسرارها التجارية، ثم قام بإرسال هذه المعلومات عبر البريد الإلكتروني إلى أحد منافسي الشركة. وقد خلصت المحكمة عند النظر في القضية إلى أن فعله يشكل دخولاً غير مشروع إلى الحاسب الآلي، رغم أنه كان يمتلك صلاحية الدخول في الأصل.[1]

يرى القضاء الفرنسي أن تجاوز حدود التصريح بالدخول إلى النظام المعلوماتي يشكل خرقاً للقانون، لأن التصريح الممنوح للعاملين في المؤسسة لا يُعتبر مطلقاً، بل هو مقيد بحدود المهام الموكلة إليهم وبعلم الإدارة. فإذا استُخدم هذا التصريح لأغراض غير مشروعة أو لأهداف لا تتصل بالعمل، فإن ذلك يُعدّ استعمالاً غير مشروع لحق الدخول.

وقد استخدم القضاء الفرنسي مصطلح «Frauduleusement» (أي الدخول بطريقة احتيالية أو عن طريق الغش) للتعبير عن الحالة التي لا يكون فيها الشخص ممنوحاً حق الدخول إلى النظام المعلوماتي[2]، أو يكون قد تجاوزه رغم امتلاكه صلاحية محددة. فالمعيار المعتمد هو مدى احترام الشخص للقواعد التقنية والإجرائية التي تنظّم الدخول إلى النظام، سواء تم الدخول بتصريح أو بدونه.

ويطرح هنا تساؤل آخر حول ما إذا كان فعل الدخول غير المشروع وحده كافيا لقيام الجريمة، أم أن الأمر يتطلب تحقق نتيجة معينة، كالحصول على بيانات النظام أو العبث بها؟ ويبدو أن الفقه الفرنسي يميل إلى الرأي الأول، إذ يرى أن الجريمة تقوم بمجرد الدخول غير المشروع، حتى ولو لم يقم الجاني باستخدام البيانات أو الإضرار بها فعلياً، مادام لم يحترم القواعد الفنية المنظمة لاستعمال النظام[3].

ثانيا الركن المعنوي لجريمة الدخول غير المشروع

يتجلى الركن المعنوي لجريمة الدخول غير المشروع في الحالة النفسية للجاني والعلاقة القائمة بين ماديات الفعل وشخصية الفاعل، وهو ما يتحقق بتوافر القصد الجنائي .ويتضح ذلك من خلال المثال الآتي: إذا قام أحد القراصنة باختراق النظام المعلوماتي، وفك شفراته، ونسخ برامجه، أو تخريبه بهدف الحصول

[1] معاشي سميرة، مرجع سابق، ص95

[2] سميرة معاشي، **نفس المرجع**، ص106.

[3] محمد خليفة، **مرجع سابق**، ص 153.

على البرمجيات أو لإلحاق الضرر بصاحب الموقع، فإن هذا السلوك يجسد الركن المعنوي للجريمة، باعتبار أن هذه الأفعال لا تقع إلا عمداً[1].

وقد شدد المشرع العقوبة في الحالات التي يترتب عنها إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو حذفها، أو إفشاؤها، أو إتلافها، أو تدميرها، أو تغييرها، أو نقلها، أو التقاطها، أو نسخها، أو نشرها، أو إعادة نشرها. كما تشمل العقوبة الأفعال المتمثلة في إلحاق ضرر بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته، أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال صفة مالكه أو القائم على إدارته.

وعليه، فإن هذه الجريمة تقوم على القصد الجنائي العام، الذي يتجسد في عنصري العلم والإرادة[2].

أما عن الركن المعنوي للجريمة فهو يتمثل في الحالة النفسية للجاني، والعلاقة الترابطية بين ماديات الجريمة وشخصية الجاني ونجد أن المشرع الأمريكي قد أضاف تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فينتقل من استخدام الإرادة مثل ما هو موجود في قانون العلامة التجارية في القانون الفيديرالي الأمريكي، وفي بعض الأحيان يأخذ بالعلم كما هو قانون مكافحة الاستنساخ الأمريكي،[3] ومن أبرز ما ظهرت به هذه المشكلة في قضية موريس والذي كان محل اتهام في قضية دخول غير مصرح به على جهاز حاسب فيدرالي، ودفع المحامي بانتفاء الركن المعنوي، وكان رد المحكمة كالتالي: " هل يُلزم الادّعاء بإثبات القصد الجنائي في جريمة الدخول الغير مصرح به؟ بحيث تثبت نية المتهم في الولوج إلى الحاسب فيدرالي ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق خسائر، الأمر الذي يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح"، وفي هذا الصدد ارتأت المحكمة في هذا الصدد إلى تبني معيارين هما: الإرادة بالدخول غير المصرح به، وكذا معيار العلم بالخطر الوارد على استخدام نظم المعلومات الفيدرالية دون تصريح.[4]

---

[1] سليمان بن إبراهيم بن أمان العامري، **جريمة الدخول الغير المشروع على المواقع الالكترونية المتعلقة بأمن الدولة**، المجلة الأكاديمية للأبحاث والنشر العلمي، الإصدار الرّابع والأربعون، 05-12-2022، ص

[2] حسين طاهر، الجرائم الإلكترونية، مرجع سابق، ص 132.

[3] هدى قشوش، **جرائم الحاسب الإلكتروني في التشريع المقارن**، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص20.

[4] مروة زين العابدين، **الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني**، مركز الدراسات العربية للنشر والتوزيع، مصر، ص 460-461.

أ: القصد الجنائي العام

يقوم الركن المعنوي في هذه الجريمة على القصد الجنائي، إذ يتعين أن يتجه نشاط الجاني إلى القيام بفعل أو الامتناع عنه مع علمه بعدم مشروعيته، وبعبارة أخرى، يجب أن يدرك الفاعل أن الولوج إلى النظام أو الاستمرار داخله يتم دون عذر قانوني.

كما يقوم هذا الركن في جريمة الدخول أو البقاء غير المشروع على القصد الجنائي العام، الذي يعبر عن الحالة النفسية للجاني عند ارتكاب الفعل، والمتمثلة في الفعل والإرادة، فالجاني يجب أن يعلم أن دخوله إلى نظام المعالجة نتيجة للمعطيات أو استمراره فيه يتم دون إذن أو سند قانوني، ومع ذلك تتجه إرادته إلى القيام بهذا السلوك[1].

وعليه فان القصد الجنائي هنا لا ينصرف إلى تحقيق نتيجة معينة، وإنما يقتصر على العلم بمخالفة القانون واتجاه الإرادة إلى ارتكاب الفعل المجرم، باعتبار أن هذه الجريمة من جرائم السلوك لا جرائم النتيجة.[2]

وبالتالي، يتحقق القصد الجنائي متى كان الفاعل مدركا لعدم مشروعة الدخول أو البقاء، ومصرا على الاستمرار فيه، بغض النظر عن الدافع أو الباعث، في المقابل، ينتفي هذا القصد إذا وقع الدخول أو البقاء عن طريق الخطأ أو الجهل بمدى مشروعته، لغياب عنصر العلم، أو إذا اعتقد الجاني بحسن نية أن سلوكه مشروع ومسموح به[3]

ومنه فان الركن المعنوي في هذه الجريمة يجسد صورة من صور القصد الجنائي العام، القائم على إرادة واعية تتجه إلى السلوك الإجرامي مع العلم بطبيعته غير المشروعة[4].

ب-القصد الجنائي الخاص

بالتأمل في القصد الجنائي الخاص، فإنه لا يُفترض توافره في الجريمة إلا إذا اشترطه النص صراحة، أو أمكن استخلاصه بوضوح من طبيعة الجريمة وغايتها. ومن ثم، فإن مجرد الدخول غير المشروع لا يستلزم، في ذاته، إثبات غاية إضافية، كتحقيق منفعة أو إلحاق ضرر بالغير، ما لم تكن هذه الغاية مطلوبة لقيام صورة معينة من صور الجريمة أو لقيام جريمة أخرى مستقلة ترتبط بهذا الدخول

[1] أحسن بوسقيعة، **الوجيز في القانون الجزائي** العام، الطبعة الثانية والعشرون، دار بلقيس، الجزائر، 2025، ص 112.
[2] غنية باطلي، **نفس المرجع**، ص 166-167
[3] آمال قارة، **مرجع سابق**، ص 124.
[4] علي عبد القادر القهواجي، مرجع سابق، ص 136-137.

أما القصد الجنائي اللازم لقيام جريمة الدخول غير المشروع، فيتمثل أساساً في علم الجاني بعدم أحقيته في الولوج إلى النظام المعلوماتي، واتجاه إرادته إلى الدخول إليه رغم انتفاء الترخيص أو الحق في ذلك. ويترتب على ذلك أن ثبوت المسؤولية الجزائية يقتضي التحقق من أن الدخول قد تم عن علم وإرادة، بما يضمن عدم التوسع في التجريم ليشمل حالات الدخول التي تتم بطريق الخطأ أو دون إدراك لعدم مشروعيتها

وبذلك يسهم التحقق من توافر الركن المعنوي في تحقيق التوازن بين حماية الأنظمة والمعطيات المعلوماتية من الولوج غير المشروع، من جهة، وضمان عدم المساس بالاستعمال المشروع لوسائل الاتصال وتكنولوجيا المعلومات، من جهة أخرى.[1]

الفرع الثاني: جريمة البقاء غير المشروع

يقصد بجريمة البقاء غير المشروع استمرار الشخص داخل نظام المعالجة الآلية للمعطيات خلافا لإرادة من له حق السيطرة عليه، وذلك بعد زوال أو انعدام الترخيص، ويتحقق هذا البقاء سواء كان نتيجة دخول مشروع ثم فقد سنده القانوني، أو نتيجة دخول وقع بطريق الخطأ ثم استمر فيه الفاعل عن علم وإرادة لتحقيق مصلحة معينة.

كما يفهم البقاء غير المشروع بأنه مواصلة الوجود أو النشاط داخل نظام المعالجة الآلية للبيانات خلافا لإرادة صاحب الحق في السيطرة عليه، أو الاستمرار في استغلاله مع الاعتقاد بعدم مشروعية هذا السلوك ويتحقق البقاء غير المشروع عندما لا يقوم الفاعل بقطع اتصاله بالنظام رغم علمه بعدم مشروعية وجوده فيه، ومن صورة استمرار دخوله إلى النظام بعد انتهاء المدة المسموح له بها.

ولا يعد البقاء سلوكا مستقلا تماما عن الدخول، بل يرتبط به ارتباطا وثيقا، إذ قد يأتي امتدادا له أو نتيجة له، ومن ثم، فإن جوهر هذه الجريمة يقوم على الاستمرار غير المبرر داخل النظام رغم العلم بعدم مشروعية ذلك[2].

أولا: الركن الشرعي لجريمة البقاء غير المشروع

يتمثل الركن الشرعي لجريمة الدخول غير المشروع في وجود نص قانوني يجرّم هذا السلوك ويحدد العقوبة المقررة له، تطبيقًا لمبدأ شرعية الجرائم والعقوبات. وقد كرّس المشرّع الجزائري هذا النص في

[1] غنية باطلي، مرجع سابق، ص158

[2] عبد القادر القهوجي، **مرجع سابق**، ص 52.

مجال الجرائم المعلوماتية، فخصّ المشرّع الجزائري البقاء غير المشروع بنص جزائي صريح، يتمثل في المادة 394 مكرر من قانون العقوبات، المعدّلة بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024، كما تعاقب هذه المادة كل من يدخل ويبقى، عن طريق الغش، في كل أو جزء من منظومة المعالجة الآلية للمعطيات، أو يحاول ذلك

ثانيا: الركن المادي لجريمة البقاء غير المشروع

يتحقق الركن المادي لجريمة البقاء غير المشروع من خلال استمرار الجاني في الوجود داخل نظام معلوماتي دون حق، متى توافرت الشروط التي يتطلبها النص الجزائي، ولا سيما أن يتم ذلك عن طريق الغش، ويستند التجريم في التشريع الجزائري إلى المادة 394 مكرر من قانون العقوبات، التي تشمل فعلَي الدخول والبقاء غير المشروعين في منظومة للمعالجة الآلية للمعطيات.[1]

ويتخذ هذا السلوك صورتين أساسيتين؛ تتمثل الأولى في استمرار الجاني داخل النظام بعد دخوله إليه دون ترخيص، بينما تتمثل الثانية في مواصلة استخدامه رغم زوال الحق الذي كان يجيز له النفاذ إليه، كأن يستمر شخص في الولوج إلى نظام مهني بعد سحب صلاحياته، مع علمه بعدم أحقيته في ذلك، واستعماله وسائل احتيالية تسمح له بمواصلة النفاذ

كما يتميز هذا السلوك عن الأفعال التي قد يرتكبها الجاني أثناء وجوده داخل النظام، كحذف البيانات أو تغييرها أو تخريب النظام أو تعطيل عمله؛ إذ لا تُعد هذه الأفعال عناصر لازمة لقيام جريمة البقاء غير المشروع، وإنما قد تشكل أفعالًا إجرامية أخرى أو ظروفًا يترتب عليها تشديد العقوبة، بحسب طبيعتها والنص القانوني المنطبق عليها

وعليه، فإن مناط الركن المادي في هذه الجريمة هو استمرار النفاذ إلى النظام المعلوماتي على نحو غير مشروع، وليس مجرد وجود اتصال تقني به، كما لا يتوقف تحقق هذا الركن على إثبات وقوع تلف في البيانات أو تحقق خسارة مالية، متى استوفى السلوك شروط التجريم المقررة قانونًا.[2] طبقًا لما ورد في المادة 394 مكرر من قانون العقوبات الجزائري.

[1] مروة زين العابدين **صالح، مرجع سابق**، ص 459.

[2] حسين طاهري، الجرائم الإلكترونية، **مرجع سابق**، ص 124

ثالثا: العلاقة بين الدخول والبقاء

يتضح أن البقاء غير المشروع لا يفترض بالضرورة دخولا غير مشروع سابقا، ويتخذ عدة صور، يجمعها عنصر مشترك يتمثل في الاستمرار داخل النظام رغم انعدام أو زوال الحق في ذلك،

أ_ حالة استقلال فعل البقاء عن الدخول غير المشروع

يتمثل في دخول الشخص بصفة مشروعة (كموظف أو مستخدم) ثم يستمر الولوج بعد انتهاء مدة الترخيص أو سحب الصلاحية، ففي الوقت الذي ينبغي للشخص المغادرة والخروج من النظام يبقى داخله فيتحصل على المعلومات والمعطيات التي لا يحق له رؤيتها[1] ، كما يحدث الولوج إلى النظام المعلوماتي بصورة عرضية أو عن طريق الخطأ، دون توفر القصد الجنائي لدى الفاعل في البداية، غير أنه، متى أدرك هذا الأخير أنه يوجد داخل نظام غير مصرح له بالدخول إليه، واستمر رغم ذلك في التواجد داخله دون أن يبادر إلى مغادرته، فان فعله يتحول إلى بقاء غير مشروع [2].

ب حالة اجتماع كل من فعل البقاء والدخول

غالبا ما يتلازم فعل الدخول غير المشروع مع البقاء غير المشروع، كما في حالة ولوج شخص غير مرخص له إلى نظام معلوماتي ثم استمراره داخله خلافا لإرادة صاحب الحق في السيطرة عليه، وفي مثل هذه الحالة يتحقق الركن لكل من الجريمتين، مما يثير إشكالا مهما يتمثل في تحديد الحد الفاصل بينهما، أي متى ينتهي فعل الدخول وتبدأ حالة البقاء غير المشروع[3]؟

فيرى اتجاه فقهي أن جريمة الدخول غير المشروع تتحقق بمجرد الولوج إلى النظام، ولو كان ذلك لفترة وجيزة، بحيث يفترض أن البقاء لو كان قصيرا لا يؤثر في قيام الجريمة، غير أن هذا الرأي يؤخذ عليه عدم وضع معيار زمني دقيق يحدد بداية البقاء غير المشروع، مما يجعل التمييز بين الجريمتين غير واضح.

في حين يذهب اتجاه آخر إلى أن بداية البقاء غير المشروع تتحدد من اللحظة التي يدرك فيها الفاعل أن استمراره داخل النظام أصبح غير مشروع، إلا أن هذا الطرح يؤخذ عليه صعوبة إثبات العلم من الناحية العملية لارتباط بعنصر نفسي داخلي[4].

---

[1] غنية باطلي، مرجع سابق، ص 160.

[2] محمد خليفة، **مرجع سابق**، ص 154-155

[3] عبد القادر القهوجي، نفس المرجع، ص 133.

[4] محمد خليفة، **نفس المرجع**، ص 133.

كما يرى اتجاه اخر أن جريمة البقاء غير المشروع تبدأ من اللحظة التي يتم فيها تنبيه أو إنذار الفاعل بعدم مشروعية وجوده داخل النظام، غير أن هذا الرأي ينتقد لارتباطه بوجود وسائل تقنية للإنذار، وهو أمر قد لا يتوفر إلا لدى بعض المؤسسات الكبرى، مما يحد من إمكانية تطبيقه في جميع الحالات[1].

وما يمكن استخلاصه أن الحد الفاصل بين الدخول والبقاء غير المشروع يظل مسألة تقديرية، تتأرجح بين معيار مادي (زمني أو تقني) ومعيار معنوي (العلم بعدم مشروعية الإستمرار)، وهو ما يعكس تعقيد هذه الجرائم في البيئة الرقمية.

وعليه نرى أن بداية البقاء غير المشروع ترتبط، كم حيث الأصل، باللحظة التي يتوافر فيها لدى الفاعل العلم بزوال أو إنتفاء مشروعية وجوده داخل النظام المعلوماتي، بحيث يصبح استمرار وجوده رغم هذا العلم سلوكا مستقلا عن مجرد فعل الدخول

ثالثا: الركن المعنوي لجريمة البقاء

يتمثل الركن المعنوي في جريمة البقاء غير المشروع داخل النظام المعلوماتي في توافر القصد الجنائي العام، والذي يقوم على عنصرين أساسيين هما العلم والإرادة. ويقصد بالعلم أن يكون الشخص مدركاً أن استمراره أو بقاؤه داخل النظام المعلوماتي غير مسموح به قانوناً أو يتم دون ترخيص من صاحب النظام أو المسؤول عنه. أما الإرادة فتتحقق عندما يتجه قصد الفاعل إلى مواصلة البقاء داخل النظام رغم علمه بعدم مشروعية ذلك.

ولا يشترط لقيام هذه الجريمة توافر قصد جنائي خاص أو تحقيق نتيجة معينة، بل يكفي أن يستمر الجاني عمداً في التواجد داخل النظام المعلوماتي بصورة غير قانونية. وينتفي الركن المعنوي إذا كان البقاء ناتجاً عن خطأ أو جهل أو اعتقاد مشروع بأن وجوده داخل النظام مسموح به. كما لا يؤثر الباعث أو الدافع وراء البقاء، سواء كان بدافع الفضول أو التجربة أو الرغبة في إثبات المهارة التقنية، ما دام الفاعل يعلم بعدم مشروعية بقائه داخل النظام [2].

من خلال ما سبق يتضح لنا الإشكال الحالي: متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

يرى رأي في الفقه أن الدخول هو الخطوة الأولى لقيام الركن المادي لجرائم المتعلقة بأنظمة المعلومات، وله معنيان أحدهما مادي كالدخول مثلا لمحل أو غرفة معينة والمعنى الآخر هو معنى معنوي وهو ما

[1] غنية باطلي، **مرجع سابق**، ص 162

[2] أمال قارة، **مرجع سابق**، ص 123.

نقصده هنا، ويعبر عن النشاط الذهني الذي يقوم به الجاني بهدف الوصول للنظام، ويشبه الفقه هذا الدخول للنظام المعلوماتي بالدخول إلى ذاكرة الإنسان،[1]

والبعض الآخر يعرف الدخول بمجمله على أساس الأبعاد المكانية والزمنية، فمن ناحية المكان فيقصد بالدخول للنظام فعل التسلل داخله أما من حيث الزمان يُقصد به تجاوز الحد المرخص به[2].

ويرى رأي اخر أنه ان كان الدخول يفترض حتما البقاء ولو لفترة قصيرة من الزمن فهنا تنتهي جريمة الدخول وتبدأ جريمة البقاء التي تنتهي بانتهاء حالة البقاء [3]

وما يعاب على هذا الرأي انه لم يحدد تلك اللحظة بطريقة جدية وصارمة

وإذا كان الاتجاه الغالب في الفقه يعتبر جريمة الدخول أو جريمة البقاء لا تعتبر جريمة وقتية أو مستمرة وإنما الغرض من هذه التفرقة هو البحث في مسألة التقادم والاختصاص المكاني والعفو الا ان هذا التوجه ضعيف مقارنة بجريمة البقاء التي تستغرق وقتا فيمكن اعتبارها مستمرة ذات أثر او دون أثر.

ونلاحظ أن المشرع الجزائري لم يربط الدخول للأنظمة بالبقاء فيها بل اكتفى فقط بتحقق أن يتم الدخول لجزء منه، وهو ما أكدته المادة 394 مكرر أعلاه أن الدخول يتضمن" كل أو جزء من منظومة " للمعالجة الآلية للمعطيات، ويعني الدخول إلى جزء من النظام المعلوماتي الولوج إلى بعض مجالات النظام المعلوماتي أي بعض عناصر النظام المعلوماتي أو حتى عنصر واحد فقط من النظام، كالدخول مثلا إلى برنامج معلوماتي معين أو إلى المعطيات الرقمية المعالجة في النظام...، والهدف من التفريق هو تجريم المشرع لبعض الحالات التي يتم فيها الدخول إلى مجال ضيق من النظام فقط، كمن يلج إلى مجال من النظام يكون من حقه الدخول إليه ويستغل الفرصة ويقوم بالدخول لجزء آخر من النظام دون ترخيص بالدخول.[4]

---

[1] يرى البعض بأن فعل الدخول له طبيعة معنوية دفعت بالتشريعات كالتشريع التونسي مثلا لاستعمال عبارة النفاذ وليس عبارة الدخول فالعبارة الأولى تعتبر أكثر دقة مقارنة بالعبارة الثانية على اعتبار أنها تستعمل للتعبير على فكرة الوصول للشيء المعنوي وليس مادي.

[2] نسيمة بطيحي، **جريمة الدخول أو البقاء الغير المشروع إلى النظام المعلوماتي**، مجلة الفقه القانوني والسياسي، المجلد 01، العدد 01، ص 78، 77.

[3] فيصل بدري، **مرجع سابق**، ص 166.

[4] عشاش حمزة، حمزة خضري، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، العدد 2، 2020، ص185.

فنشير هنا بأن جريمة الدخول للنظام المعلوماتي هي جريمة شكلية، أي أنها تتحقق بمجرد الدخول للنظام المعلوماتي ولا يشترط البقاء، وقد أقر القضاء الفرنسي مجموعة القضاء الفرنسي مجموعة من المبادئ التي يجب إعمالها في حال دخول أحد الأشخاص للمواقع الالكترونية والاطّلاع على بياناتها تتمثل فيما يلي:

*استئذان أو إخطار صاحب الموقع المراد استغلال البيانات أو المعلومات الموجودة في موقعه.

*احترام القوانين واللوائح التي تحكم في حق الملكية الذهنية. [1]

الفرع الثالث: جريمة الاعتداء على النظام المعلوماتي

ويتحقق ذلك من خلال تصميم المعطيات أو البحث عنها أو جمعها أو إتاحتها أو نشرها أو تداولها أو الاتجار بها، سواء تعلق الأمر بمعطيات مخزنة أو معالجة أو مرسلة عبر نظام معلوماتي، كما يشمل حيازة أو إفشاء أو استعمال أو نشر المعطيات المتحصّل عليها نتيجة ارتكاب إحدى الجرائم الماسة بالأنظمة المعلوماتية، مهما كان الغرض من استخدامها[2].

أولا: الركن الشرعي لجريمة الاعتداء على النظام المعلوماتي

يستمد التجريم في هذه الصورة من الأحكام التي أقرها المشرع الجزائري لحماية أنظمة المعالجة الآلية للمعطيات، والتي تجرّم الأفعال التي من شأنها المساس بسلامة النظام أو معطياته أو عرقلة سيره، وذلك وفقًا للنصوص المقررة في قانون العقوبات ضمن الأحكام الخاصة بالمساس بأنظمة المعالجة الآلية للمعطيات

ويقتضي مبدأ الشرعية الجنائية أن يكون الفعل محل المتابعة منصوصًا عليه ومحددًا في القانون، بحيث لا يكفي مجرد كون السلوك ضارًا بالنظام المعلوماتي لقيام المسؤولية الجزائية، وإنما يجب أن تتوافر فيه العناصر التي حددها النص الجزائي.

ثانيا: الركن المادي لجريمة الاعتداء على النظام المعلوماتي

يتمثل الركن المادي للجريمة من خلال نص المادة 394مكرر 2 من قانون العقوبات في السلوك الإجرامي الذي يشمل أفعال الحيازة والإفشاء والنشر والاستعمال للمعطيات المتحصل عنها من جرائم

1حنان ريحان مبارك المضحكي، **مرجع سابق**، ص 102.

[2] امال قارة، مرجع سابق، ص 126.

معلوماتية الواردة في القسم السابع مكرر من قانون العقوبات، الأمر الذي جعل هذه المعطيات ترتبط بأعمال أخرى غير مشروعة[1]. وتتمثل صور الاعتداء العمدي على نظام المعالجة الآلية للمعطيات فيمايلي:

أ_ إفساد أو إتلاف النظام المعلوماتي:

لم يشترط المشرع الجزائري أسلوب خاصا لإفساد أو تعطيل أو توقيف النظام المعلوماتي فهو عامة كل فعل من شأنه إعاقة سير النظام، ومن وسائل التعييب أو الإفساد استخدام البرنامج الذي يحمل فيروسا من نوع" حصان طراودة" أو قنبلات إلكترونية أو برنامج الدودة

ويتضح مما سبق أن الفعل غير المشروع في هذه الجريمة يتمثل في كل فعل يتسبب في افساد نظام التشغيل مهما كانت نتيجته سواء ادى ذلك الى تعطيله كلية أو جزئيا[2].

ب_ عرقلة سير النظام أو تعطيل وظائفه:

تتحقق هذه الصورة عندما يؤدي السلوك المرتكب إلى الحيلولة، بصورة كلية أو جزئية، دون قيام النظام المعلوماتي بوظائفه بصورة طبيعية، أو إلى الحد من قدرته على معالجة البيانات أو تقديم الخدمات التي أعد من أجلها، وقد يكون التعطيل مؤقتًا أو مستمرًا، كليًا أو جزئيًا، بحسب طبيعة السلوك وآثاره. ولا يشترط بالضرورة أن يؤدي الفعل إلى تدمير النظام، إذ يكفي أن يترتب عليه اختلال في سيره أو انخفاض في قدرته على أداء وظائفه، متى توافرت العناصر التي يتطلبها النص الجزائي.

ومن ثم، يختلف تعطيل النظام عن إتلافه من حيث الأثر المباشر للسلوك؛ فالإتلاف ينصرف أساسًا إلى المساس بسلامة النظام أو المعطيات، في حين تنصرف العرقلة أو التعطيل إلى المساس بوظيفة النظام وقدرته على العمل بصورة طبيعية. ويتحقق التخريب كظرف مشدد دون اشتراط القصد المباشر، متى ترتب عن فعل الدخول أو البقاء غير المشروع ضرر بالنظام هو ما جاءت به المادة 394 مكرر الفقرة 02 من القانون 04_15 السالف الذكر[3].

---

[1] المادة 394 مكرر فقرة 2 قانون العقوبات

[2] دليلة خينش، نفس المرجع

[3] نص قانون العقوبات الجزائري لاسيما المواد من 394 مكرر إلى 394 مكرر 7 على تجريم: **فعل إدخال معطيات بطريقة احتيالية في نظام معلوماتي، حذف أو تعديل المعطيات، عرقلة سير نظام المعالجة الآلية للمعطيات**

[3] طاهري حسين، **الجرائم الإلكترونية**، مرجع سابق، **ص 154**.

ومن هذا المنطلق لابد من التمييز بين الإفساد والتعطيل، فالأول ينصرف إلى التأثير على سلامة البيانات أو النتائج، أما الثاني فيتعلق بإيقاف النظام وعرقلة سيره، غير أن هذا التمييز يبقى نظريا في كثير من الحالات، نظرا لتداخل الآثار الناجمة عن الأفعال الإجرامية في المجال المعلوماتي

وبذلك، فإن عمومية النص قد تؤدي إلى اتساع نطاق التجريم ليشمل حالات قد تفتقر إلى القصد الجنائي الواضح، مما يستدعي تفسيرًا دقيقًا من القضاء لضبط حدود المسؤولية الجزائية في هذه الجريمة.[1]

ثانيا: الركن المعنوي لجريمة الإعتداء على النظام المعلوماتي

جريمة الاعتداء الماسة بالأنظمة المعلوماتية هي جريمة عمدية يتوفر فيها القصد الجنائي بعنصريه العلم الإرادة، وقد نصت المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي تشترط لقيام الجريمة قيام الجاني بخرق النظام بهدف الحصول على المعطيات الموجودة بداخله.

الفرع الرابع: جريمة المساس العمدي بسلامة المعطيات المعلوماتية

تتميز جريمة المساس بالمعطيات المعلوماتية عن جريمة تعطيل نظام المعالجة الآلية للبيانات من حيث محل الاعتداء، فالجريمة الأولى تتعلق بالبيانات والمعلومات الموجودة داخل النظام، أما الثانية فتنصب على النظام المعلوماتي نفسه من خلال عرقلته أو تعطيل وظائفه[2]، ويقصد بالمعطيات أو البيانات المعلوماتية كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إلى ذلك[3].

أولا: الركن المادي لجريمة المساس العمدي بسلامة المعطيات المعلوماتية

يتمثل الركن المادي في السلوك الإجرامي لهذه الجريمة سواء كان بإدخال أو محو أو تعدي وقد نصت المادة 394 مكرر 2 من قانون العقوبات الجزائري على معاقبة كل من يقوم، بطريق الغش، بإدخال معطيات داخل نظام المعالجة الآلية، أو حذفها، أو تعديلها، بعقوبة الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية.

---

[1] بدري فيصل، **مرجع سابق**، ص 173

[2] شريفة كلاع، **الأمن السيبيراني وأشكال التهديد**، مرجع سابق، ص 166

[3] تنص المادة **394 فقرة 2 من قانون العقوبات**" يعاقب بالحبس من ستة أشهر إلى ثلاث وبغرامة من 500.000 دج إلى 2000000 دج، كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

حيث يتضح أن المشرّع يتجه إلى حماية مضمون المعطيات المعلوماتية نفسها وليس مجرد الجانب الوظيفي وعليه، فإن الاعتداء العمدي على المعطيات يتجسد في ثلاثة أشكال رئيسية هي:

أ-الإدخال غير المشروع لمعطيات جديدة داخل النظام[1] L'intrusion

يتمثل فعل الإدخال في إضافة معطيات أو معلومات جديدة إلى الدعامة المعلوماتية، سواء كانت فارغة أو تحتوي مسبقا على بيانات، ويتحقق ذلك الفعل بإدخال برامج خبيثة أو فيروسات

ب_ حذف المعطيات الموجودة L'effacement

يتمثل الفعل في محو جزء من المعطيات المسجلة أ إزالة البيانات وإتلافها بما يؤدي إلى فقدانها كليا أو جزئيا من الذاكرة المعلوماتية، كما قد يتحقق بنقلها أو تغيير مكان تخزينها داخل النظام على نحو يجعل الوصول إليها واستعمالها متعذرا[2].

ج- تعديل أو تغيير محتواها Modificatio

يقصد بتعديل أو تغيير محتوى المعطيات المعلوماتية إحداث تغيير غير مشروع في البيانات أو المعطيات محل الحماية، بما يؤدي إلى المساس بمضمونها أو محتواها أو قيمتها الوظيفية، سواء بإضافة معطيات جديدة، أو حذف معطيات موجودة، أو استبدالها أو تحويرها على نحو يجعلها مختلفة عن حالتها الأصلية. وقد يتحقق هذا السلوك باستعمال وسائل تقنية مختلفة، من بينها البرامج أو التطبيقات التي تسمح بالتلاعب بالمعطيات أو تغيير محتواها

ويقتضي تحديد هذه الصورة من صور الاعتداء الرجوع أولا إلى أحكام التشريع الجزائري ذات الصلة، ولا سيما الأحكام المنظمة لحماية المعطيات ذات الطابع الشخصي بموجب القانون رقم 18-07، المعدل والمتمم بالقانون رقم 25611 المؤرخ في 24 يوليو 2025 مع التمييز بينها وبين الأحكام الجزائية المتعلقة بالاعتداء على أنظمة المعالجة الآلية للمعطيات. ذلك أن نطاق الحماية يختلف باختلاف طبيعة المعطيات ومحل الاعتداء والنص الجزائي المنطبق عليها، فلا ينبغي الخلط بين المساس بالمعطيات في حد ذاتها وبين الاعتداء على النظام المعلوماتي الذي تتم فيه معالجتها

[1] خالد حسن أحمد لطفي، **الأمن المعلوماتي، التهديدات والتدابير التشريعية والتقنية لحمايته**، دار الفكر الجامعي، 2021، ص 70.

[2] فيصل بدري، مرجع سابق، ص 176.

ويتحقق السلوك المادي في صورة التعديل أو التغيير متى أقدم الجاني على فعل من شأنه تغيير الحالة الأصلية للمعطيات محل الحماية، سواء تم ذلك بإضافة بيانات جديدة، أو حذف بيانات قائمة، أو تحوير محتواها، متى توافرت الشروط التي يتطلبها النص الجزائي المنطبق. ومن ثم، لا يشترط اجتماع صور السلوك المادي في فعل واحد، وإنما يكفي . بحسب الصورة التي حددها النص . تحقق الفعل المجرّم الذي من شأنه إحداث التغيير أو المساس بالمعطيات

ولا يقف الركن المادي عند مجرد السلوك الإجرامي، وإنما يتعين التحقق كذلك من النتيجة التي يرتبها هذا السلوك، والمتمثلة في إحداث تغيير فعلي في المعطيات أو المساس بسلامتها أو مضمونها، فضلا عن قيام علاقة سببية بين فعل الجاني والنتيجة المتحققة. وبالتالي، لا يكفي مجرد استعمال وسيلة تقنية أو القيام بعملية على المعطيات لقيام الجريمة ما لم يكن الفعل قد أفضى إلى النتيجة التي يجرّمها النص، متى كانت الجريمة من الجرائم التي يتطلب القانون فيها تحقق نتيجة معينة.

أما من حيث محل الجريمة، فينبغي تحديده وفقا للنص القانوني الذي يجرّم الفعل، إذ لا يصح القول بصورة مطلقة إن الحماية الجنائية لا تمتد إلا إلى المعطيات الموجودة فعليا داخل النظام المعلوماتي أو أنها تستبعد المعطيات التي خرجت منه، وإنما يتحدد نطاق الحماية بحسب طبيعة المعطيات ومحل المعالجة والفعل الذي استهدفها، وبحسب الأحكام الخاصة الواردة في التشريع الجزائري

ثانيا: الركن المعنوي لجريمة المساس العمدي بسلامة المعطيات المعلوماتية

تتطلب جريمة المساس بسلامة المعطيات المعلوماتية، متى كانت من الجرائم العمدية الجريمة العمدية الماسة بسلامة المعطيات المعلوماتية صورة القصد الجنائي، الذي يقوم على عنصرين هما العلم والإرادة. فيتعين أن يكون الجاني عالما بطبيعة الفعل الذي يقدم عليه وبأنه يستهدف معطيات مشمولة بالحماية، وأن تتجه إرادته إلى ارتكاب السلوك المجرّم وإحداث الأثر الذي يرتبه فعله، متى كان تحقق هذا الأثر لازما لقيام الجريمة

وعليه، لا يكفي عند بحث الركن المعنوي مجرد القول إن إرادة الجاني اتجهت إلى القيام بفعل الإضافة أو الحذف أو التعديل، وإنما يجب بحث علمه بالعناصر التي يتطلبها النص لقيام الجريمة، واتجاه إرادته إلى ارتكاب السلوك المجرّم والنتيجة التي يمكن أن تترتب عنه، متى كانت هذه النتيجة عنصرا من عناصر الجريمة[1].

[1] فيصل بدري، مرجع سابق، ص 177.

ولا يشترط لقيام القصد الجنائي، من حيث الأصل، توافر نية خاصة في الإضرار بالغير ما لم يشترطها النص صراحة أو تستخلص من طبيعة الجريمة، إذ يكفي توافر العلم والإرادة بالنسبة للعناصر التي يتطلبها القانون. أما الضرر، فيتحدد أثره في قيام الجريمة بحسب ما إذا كان النص يجعله عنصرا لازما لتمامها أو نتيجة مترتبة عن السلوك الإجرامي

وبذلك، فإن دراسة الاعتداء على المعطيات المعلوماتية تقتضي عدم الوقوف عند مجرد وصف السلوك الإجرامي، وإنما تحليل عناصر الركن المادي في تكاملها، من سلوك ونتيجة وعلاقة سببية متى كانت النتيجة لازمة لقيام الجريمة، ثم بيان الركن المعنوي من خلال مدى توافر العلم والإرادة بالنسبة إلى مختلف عناصرها.

المطلب الثاني: المسؤولية الجزائية في جريمة القرصنة الالكترونية

من الإشكالات التي تطرحها جريمة القرصنة الالكترونية مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أحد دول الاتحاد الأوروبي باختراق جهاز خادم server في أحد بنوك الجزائر، باستخدام خادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة، وأيضا القانون الواجب التطبيق لوجود بعد دولي في هذا المجال، بمعنى على عاتق من تقع المسؤولية الجزائية[1].

فمن غير المشكوك فيه بأن قرصنة بيانات الغير يمثل جريمة يعاقب عليها القانون سواء في أحكام التشريعات التقليدية أم تشريعات الانترنت، ففي حالة ضبط شخصا في جريمة سطو وإثبات انتساب الفعل الإجرامي إليه، فإن فعله هذا يحمله المسؤولية الجنائية، التي يترتب عليها العقاب، الذي من شأنه أن يكف به الجاني عن ممارسة السلوك الإجرامي من جهة، ويعتبر به الغير من جهة أخرى.

غير أن تداول المعلومات ونشرها في الوسط الإلكتروني قد يطرح صعوبات تقنية تعيق الجهات المختصة بأعمال التتبع والتحليل أثناء ملاحقة جرائم القرصنة الإلكترونية.[2]

كما تثير المسؤولية الجزائية في مجال القرصنة الإلكترونية إشكالات تتعلق بتحديد الشخص الذي يُنسب إليه الفعل الإجرامي، ولا سيما عندما تتوزع عناصر النشاط المعلوماتي بين دول مختلفة، كأن ينفذ

[1] احسن بوسقعية، **الوجيز في القانون الجزائي العام**، الطبعة 22، دار بلقيس، الجزائر، 2025، ص212.

[2] **المادة 12 من معاهدة بودبست** تطرقت الى المسؤولية الجنائية في الجريمة المعلوماتية بأنها: التزام الشخص بتحمل النتائج القانونية المترتبة على الفعل الإجرامي الذي ارتكبه"، ويقصد بها مساءلة الجاني عن سلوكه المخالف للقانون وإخضاعه للعقوبة المقررة قانونا، كما تعد المسؤولية الجزائية من العناصر الأساسية لقيام الجريمة، لأنها ترتبط بإسناد الفعل إلى مرتكبه بصورة قانونية.

الجاني من دولة أجنبية اختراقًا لخادم تابع لبنك جزائري، مستعينًا بخادم موجود في دولة ثالثة. وتطرح هذه الصورة مسائل تتصل بتحديد مكان ارتكاب الجريمة، والقانون الواجب التطبيق، وإمكانية تحديد هوية الفاعل وإثبات صلته بالنشاط الإجرامي وتزداد صعوبة إسناد الجريمة في البيئة الرقمية بسبب إمكانية إخفاء الهوية الحقيقية للمستخدم، واستعمال وسائل تقنية متعددة لإخفاء مصدر الاتصال أو تمويه مساره، الأمر الذي يستلزم الاستعانة بالأدلة الرقمية ووسائل التحري والتحقيق المقررة قانونًا لتحديد مرتكب الفعل وإثبات مسؤوليتها، فيقصد بالمسؤولية الجزائية خضوع الشخص للمساءلة القانونية عن فعل يجرّمه القانون، متى توافرت شروط إسناده إليه وانتفت موانع المسؤولية. وفي مجال القرصنة الإلكترونية، يقتضي ذلك التمييز بين الشخص الطبيعي الذي ينفذ النشاط الإجرامي، والشخص المعنوي الذي قد تُرتكب الجريمة باسمه أو لحسابه، وفقًا للشروط التي يحددها التشريع الجزائري

الفرع الأول: المسؤولية الجزائية للشخص الطبيعي عن جرائم القرصنة الإلكترونية

تعد المسؤولية الجزائية نتيجة قانونية تترتب على ارتكاب فعل يجرمه القانون، وهي تعكس رابطة قانونية بين الجاني والفعل الإجرامي الذي صدر عنه، ولا تقوم هذه المسؤولية إلا إذا أمكن إسناد الفعل إلى شخص تتوافر فيه شروط الإدراك والاختيار، بحيث يكون سلوكه معبرا عن إرادة واعية ومعتبرة قانونا، فالمسؤولية لا تعد ركنا من أركان جريمة القرصنة الإلكترونية بل هي أثر قانوني يترتب عليه قيام الجريمة مكتملة الأركان، ومنه فان الجريمة تقع على ركنين أساسيين هما الركن المادي الذي يتمثل في السلوك الإجرامي ونتيجته وعلاقته السببية، وركن معنوي يعبر عن القصد الجنائي أو الخطأ[1].

تقوم المسؤولية الجزائية للشخص الطبيعي متى أمكن إسناد الفعل المجرّم إليه، وتوافرت الشروط القانونية اللازمة لمساءلته. وفي جرائم القرصنة الإلكترونية، لا يكفي إثبات وقوع اختراق أو اعتداء على نظام معلوماتي، بل يتعين تحديد الشخص الذي صدر عنه النشاط الإجرامي وإقامة الدليل على صلته به، مع مراعاة الضمانات القانونية المقررة في مجال الإثبات الجزائي.

وتكتسي عملية الإسناد أهمية خاصة بالنظر إلى إمكانية تنفيذ الهجوم المعلوماتي عن بُعد، أو استعمال حسابات وأجهزة وخوادم وسيطة لا تعود إلى الفاعل الحقيقي. لذلك، ينبغي أن يستند تحديد المسؤولية إلى مجموعة من القرائن والأدلة الرقمية التي يجري الحصول عليها وفحصها وفقًا للقانون، مع

[1] أحسن بوسقيعة، مرجع سابق، ص 200.

التحقق من سلامتها ومدى اتصالها بالفعل محل المتابعة، كما يشترط لمساءلة الشخص الطبيعي توافر الأهلية اللازمة لتحمل المسؤولية الجزائية، وفقًا للأحكام القانونية المتعلقة بالتمييز والإدراك وموانع المسؤولية. ويجب كذلك التحقق من توافر العنصر المعنوي الذي يتطلبه النص المجرّم، بحسب طبيعة الجريمة وصورتها، دون افتراض القصد الجنائي لمجرد ثبوت استعمال وسيلة تقنية أو حصول اتصال غير مشروع بنظام معلومات

وعليه، فإن خصوصية المسؤولية الجزائية للشخص الطبيعي في جرائم القرصنة الإلكترونية لا تتمثل في إنشاء أركان جديدة للجريمة، وإنما في صعوبة تحديد الفاعل الحقيقي وإثبات نسبة النشاط المعلوماتي إليه، فضلًا عن ضرورة التحقق من توافر الشروط القانونية للمساءلة[1].

الفرع الثاني: مسؤولية الشخص المعنوي جريمة القرصنة الإلكترونية

في حال ارتكاب الشخص المعنوي لأفعال غير مشروعة فانه يتحمل المسؤولية الجزائية متى ارتكبت الجريمة باسمه أو لحسابه من طرف أجهزته أو ممثليه الشرعيين، وذلك وفق الشروط التي يقرّرها قانون العقوبات الجزائري. فالمشرّع لم يعد يحصر المسؤولية الجنائية في الشخص الطبيعي فقط، بل وسع نطاقها لتشمل الشركات والمؤسسات والجمعيات وغيرها من الهيئات المعنوية، بالنظر إلى الدور المتزايد الذي أصبحت تؤديه خاصة في البيئة الرقمية[2].

كذلك مسؤولية الشخص المعنوي في الجرائم الإلكترونية عندما تستعمل الوسائل التقنية أو الأنظمة المعلوماتية التابعة له في تنفيذ أفعال مثل الاختراق غير المشروع، أو اعتراض المعطيات، أو تعطيل الأنظمة، أو الاستيلاء على البيانات الإلكترونية، بشرط أن يكون الفعل قد ارتكب لتحقيق مصلحة الشخص المعنوي أو لفائدته، كما قد تثور هذه المسؤولية إذا ثبت وجود تقصير تنظيمي داخل المؤسسة، كغياب الرقابة التقنية أو التساهل في استعمال الأنظمة المعلوماتية بما يسمح بوقوع الجريمة[3]

كرس المشرع الجزائري نظام المسؤولية الجزائية للأشخاص المعنوية لأول مرة في قانون العقوبات سنة 2004 بموجب المادة 51 مكرر منه[4].

---

[1] أمر فرج يوسف، **البلطجة الإلكترونية، كشكل من أشكال التهديد والابتزاز الإلكتروني ووسائل مكافحتها القانونية** دراسة قانونية مقارنة، مركز المحمود لتوزيع الكتب القانونية، الطبعة الأولى، 2024، ص57.

[2] أحسن بوسقيعة، **مرجع سابق**، 2025، ص 210

[3] محمد حزيط، الوجيز في قانون الاجراءات الجزائية الجزائري، الطبعة الاولى، دار بلقيس، 2025، ص 450.

[4] نفس المرجع.

ومن الناحية العملية، قد تظهر هذه المسؤولية في حالة شركة تستغل وسائل إلكترونية للتجسس على منافسيها، أو مؤسسة تسمح باستعمال خوادمها لشن هجمات معلوماتية، أو هيئة تستفيد من معطيات تم الحصول عليها بطرق غير مشروعة، وفي هذه الحالات لا يمنع قيام مسؤولية الشخص المعنوي من مساءلة الشخص الطبيعي الذي نفّذ الفعل، إذ يمكن أن تقوم المسؤوليتان معا.

المطلب الثالث: العقوبات المقررة لجريمة القرصنة الإلكترونية

تتحدد السياسة العقابية في مجال القرصنة الإلكترونية من خلال العقوبات التي رصدها المشرع للأفعال الماسة بالأنظمة المعلوماتية والمعطيات التي تحتويها، مع مراعاة اختلاف جسامة الاعتداء والنتائج المترتبة عليه وطبيعة الجهة المتضررة، ويقتضي بيان هذه السياسة التمييز بين العقوبات الأصلية المقررة للأفعال المجرّمة، والحالات التي يترتب عليها تشديد العقوبة، وفقًا للأحكام القانونية ذات الصلة[1].

ومن خلال نص المادة **394 مكرر** من قانون العقوبات الجزائري صراحة على أن جريمة الدخول أو البقاء غير المصرح بهما تعد جريمة عمدية، ويفهم ذلك من عبارتها" كل من يدخل أو يبقى عن طريق الغش"

فنجد أن هذه الجريمة تأخذ شكلين من العقوبة إما في صورتها البسيطة التي تتمثل في فعل الدخول أو البقاء غير المشروع دون أن يترتب عليه أي محو أو تغيير، أما الصورة الثانية فتتمثل في الدخول أو البقاء وأن يتسبب هذا الدخول في محو أو تغيير في المعطيات أو تعييب وظيفة تشغيل النظام، والصورة المشددة[2].

الفرع الأول: العقوبات الأصلية لجريمة القرصنة الإلكترونية

تتمثل العقوبات الأصلية المقررة لهذه الجريمة في الحبس والغرامة المالية، وفق الحدود التي يحددها المشرع الجزائري بموجب النصوص القانونية ذات الصلة، تبعًا لطبيعة الفعل المرتكب والصورة التي تتحقق بها الجريمة.

ولقد أوجبت المادة 13 من الاتفاقية الدولية المتعلقة بالإجرام المعلوماتي أن تكون العقوبات المقررة للجرائم المعلوماتية فعالة ورادعة، وأن تشمل العقوبات السالبة للحرية باعتبارها عقوبات أصلية، إلى جانب العقوبات التكميلية التي يمكن تطبيقها على الشخص الطبيعي والشخص المعنوي، وذلك وفق ما نصت عليه

[1] نصت **المادة 13 من اتفاقية بودبست** على ضرورة التزام الدول على اتخاذ تدابير تشريعية للردع من الجريمة الالكترونية وتقييد الحرية، بما فيها الأشخاص الاعتبارية.

[2] عبد القادر القهوجي، مرجع سابق، ص 129.

المادة 12 من الاتفاقية. وقد نهج المشرع الجزائري نفس النهج من خلال تعديل الأحكام الخاصة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات وتشديد العقوبات المقررة لها[1].

أولا: العقوبات المقررة للدخول والبقاء غير المشروعين في النظام المعلوماتي

وقد شهدت الأحكام الجزائية المتعلقة بالاعتداء على أنظمة المعالجة الآلية للمعطيات تعديلًا بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، وهو ما يستوجب مراعاة الصيغة الجديدة للنصوص عند تحديد نطاق التجريم والعقوبات المقررة للجرائم المعلوماتية.

ففيما يتعلق بجريمة الدخول أو البقاء غير المشروع داخل منظومة المعالجة الآلية للمعطيات، أصبحت المادة 394 مكرر تعاقب كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، بالحبس من ستة (6) أشهر إلى سنتين (2)، وبغرامة من 60.000 دج إلى 200.000 دج.

ثانيا: العقوبات المقررة للإعتداء على المعطيات وسير النظام المعلوماتي

كما شدد المشرع العقوبة إذا ترتب عن الفعل حذف أو تغيير لمعطيات المنظومة، وتكون العقوبة أشد إذا أدى الفعل إلى تخريب نظام اشتغال المنظومة، حيث تصبح الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000 دج إلى 300.000 ج

أما جريمة الاعتداء على المعطيات، فقد أعاد المشرع تنظيمها بموجب المادة 394 مكرر 1، التي تعاقب كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات، أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها، بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج

ويلاحظ من خلال هذه التعديلات أن المشرع الجزائري لم يقتصر على تجريم مجرد الولوج غير المشروع إلى المنظومة، وإنما ميز بين الاعتداء الواقع على الولوج إلى المنظومة وبين الاعتداء الذي ينصب على المعطيات ذاتها، كما أخذ بعين الاعتبار النتائج المترتبة عن الفعل، ولا سيما حذف أو تغيير المعطيات أو تخريب نظام اشتغال المنظومة، ورتب على ذلك تشديدًا في العقوبة

[1] المادة 13 من الاتفاقية الدولية المتعلقة بالإجرام المعلوماتي.

كما استحدث التعديل أحكامًا أخرى ضمن القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، من بينها المادة 394 مكرر 2، التي تتناول أفعالًا عمدية تتم عن طريق الغش، فضلًا عن أحكام خاصة عندما تستهدف الجرائم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام

وعليه، فإن دراسة صور الاعتداء على أنظمة المعالجة الآلية للمعطيات تقتضي عدم الاكتفاء بعرض النصوص السابقة للتعديل، وإنما يتعين بيان مضمون التعديل التشريعي وأثره في تحديد صور السلوك المجرّم والعقوبات المقررة له، باعتبار أن النص المعدل هو الذي يعبر عن السياسة الجنائية الجزائرية الحالية في مجال مكافحة الجرائم المعلوماتية.

وتطبق العقوبة نفسها على كل من يحتفظ أو يفشي أو ينشر أو يستعمل البيانات المتحصل عليها من الجرائم المعلوماتية المنصوص عليها في هذا القسم. كما تشدد العقوبات إذا استهدفت الأفعال أنظمة تخص الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وذلك دون المساس بتطبيق العقوبة الأشد عند الاقتضاء

وتطبق هذه العقوبة متى كان الفعل مجرد دخول أو استعمال غير مشروع دون إحداث ضرر جسيم أو ظروف مشددة، ففي حال ارتكبت الجريمة سواء في صورتها البسيطة أو المشددة ولم يترتب عنها تعطيل أو فساد لنظام المعالجة الآلية للمعطيات أو حذف أو تعديل لهذه الأخيرة فإن العقوبة الأصلية تتمثل في الحبس من ثلاثة أشهر إلى سنة وبغرامة مالية تتراوح بين 50000 دج خمسين ألف دينار إلى مائة ألف 100000 دينار جزائري[1].

الفرع الثاني: تشديد العقوبات المقررة لجريمة القرصنة الإلكترونية

بالرجوع لنص المادة 394 مكرر من ق. ع. ج في فقرتها الثانية أن " تضاعف العقوبة إذا ترتب على ذلك – فعل البقاء الغير مشروع – حذف أو تغيير لمعطيات المنظومة، كما نصت ذات المادة في الفقرة الثالثة على أنه" إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون الحبس من ستة أشهر إلى سنتين وبغرامة مالية تُقدر من 50.000 دج إلى 150.000دج، بالإضافة للظرف الذي أقرته المادة 394 مكرر 03 من قانون العقوبات والمتعلق بالمساس بمؤسسات الدولة، وسنفصل في هذه الظروف المشددة في التالي[2]:

[1] سميرة معاشي، مرجع سابق، ص 104.

[2] المادة 394 مكرر فقرة 03 من قانون العقوبات الجزائري.

أولا: جريمة المساس بالمعطيات (حذف أو تغيير معطيات النظام الآلي)

وهي أكثر الصور رواجا ويقصد بها كل فعل ينتج عنه جعل المعطيات غير موجودة أو غير متاحة لمستعملي النظام الشرعيين، أما التغيير فهو تعديل للمعطيات الموجودة، ويرى الفقه صعوبة التمييز بين فعلي الحذف والتغيير، ذلك أنه لإجراء التغيير فلا مفر من الإلغاء أي الحذف. [1]

وقد نصت المادة 394 مكرر 1 على معاقبة كل من يقوم بإضافة بيانات أو إزالة بيانات من نظام المعالجة الآلية للمعطيات باستعمال طرق احتيالية، بالحبس من سنة إلى 3 سنوات وبغرامة من 500.000 دج الى 2.000000 دج

والتشديد يهدف لحماية سلامة المعطيات التي يحويها النظام المعلوماتي، هذه المعطيات تمثل في الوقت الراهن قيما مستحدثة يتعين حمايتها إلى جانب ما تتمتع به الأشياء المادية من حماية.

غير أن ما يعيب النص أنه لم يحدد نوع المعطيات المعنية بالحماية، بما معناه أن كافة أنواع المعطيات تشملها الحماية دون تخصيص، عكس المشرع الجزائري فالمشرع الفرنسي نجده قد خص المعطيات ذات الطابع الشخصي بالحماية واعتبرها ظرفا مشددا، ويتجلى هذا في الفقرة الثالثة من المادة 323-3 من ق ع الفرنسي، فعندما تكون جريمة الدخول أو البقاء الغير مشروع داخل النظام ضد نظام معالجة المعطيات ذات الطابع الشخصي التي تقوم بها الدولة[2].

ثانيا: جريمة المساس بسلامة النظام (تخريب نظام اشتغال النظام المعلوماتي)

ويمكن أن نشير بأن أفعال التغيير لمعطيات النظام المعلوماتي والتخريب لنظام اشتغال النظام المعلوماتي هي مجموعة أفعال لاإرادية خلاف الأفعال الأساسية المتمثلة في فعل الدخول أو البقاء داخل النظام التي تفترض نية الغش، وهذا في أنه في الفرض التي تتم فيه هذه الأفعال عمدا لا يكون هناك مجال لتطبيق نص المادة، بل وإن النص القانوني الواجب تطبيقه هو المادة 394 مكرر 01 من قانون العقوبات، والتي تجرم فعل المساس العمدي بمعطيات النظام المعلوماتي[3].

---

[1] Papa Assante Touré, le traitement de la cybercriminalité, le traitement de la cybercriminalité de vante le juge, (exemple du Sénégal), paris, le Harmattan, 2014, p 115.

[2] المادة 323 فقرة 3 من ال
قانون الفرنسي.

[3] المادة **394 مكرر** 1 قانون العقوبات.

ثالثا: جريمة المساس بمؤسسات الدولة

تضاعف العقوبة إذا كان الطرف المستهدف من طرف الهاكر في جريمة الدخول أو البقاء الغير مشروع للنظام المعلوماتي هو الدفاع الوطني أو أحد مؤسسات الدولة، حيث نصت المادة 394 مكرر3 من ق ع "تضاعف العقوبات المنصوص عليها في هذا القسم، حيث استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام،[1] دون الإخلال بتطبيق عقوبات أشد"، فاختراق المواقع الخاصة بمؤسسات الدولة الحساسة من شأنه أن يهدد أمنها واستقرارها[2]، وقد ورد تعديل في القانون لاقم 24_06 المؤرخ في 28 أفريل 2024 أين أقر عقوبة المساس بالهيئات والمؤسسات الخاضعة للقانون العام بالحبس من سنتين إلى عشر سنوات وغرامة مالية من 700.000 دج إلى 2.000.000 دج.

الفرع الثالث: عقوبة الاشتراك والشروع في الجريمة

نتطرق أولا إلى عقوبة الاشتراك ثم إلى عقوبة الشروع

أولا: عقوبة الاشتراك

الاشتراك هو الاتفاق الجنائي بغرض ارتكاب الجريمة الإلكترونية حيث تطبق عليه عقوبة الجريمة الأشد عند تعدد الجرائم محل الاتفاق، وقد نصت المادة 394 مكرر 5 من قانون العقوبات على تجريم هذا الاتفاق متى توفر قصد التحضير لارتكابها مع توفر الركن المادي الذي يثبت المشاركة في هذا الفعل.

ومن خلال استقراء النصوص القانونية، يتضح أن المشرع لم يخرج عن القواعد العامة المتعلقة بمسؤولية الشريك، إذ أخضعه لنفس عقوبة الفاعل الأصلي، وتتميّز جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات بأنها غالبًا ما تُرتكب بصورة جماعية، حتى وإن لم يثبت وجود اتفاق صريح بين الجناة، إذ قد يستدل على الاتفاق الضمني من خلال تعاون أفراد المجموعة وتحقيقهم لنتيجة إجرامية واحدة كما أن قيام الاتفاق الجنائي في هذا النوع من الجرائم لا يشترط اجتماع الأشخاص في مكان واحد أو وجود تنسيق مباشر بينهم، بل قد يتحقق بمجرد انتقال كلمة السر أو تبادل وسائل الدخول غير المشروع بين عدة أشخاص. ويمكن أن يضم الاتفاق أشخاصا طبيعيين أو معنويين[3]، مثال ذلك الدخول والبقاء غير المشروعين الحبس من ستة أشهر إلى سنتين، وغرامة من 60.000 إلى 200.000 دج

---

[1] غنية باطلي، **مرجع سابق**، ص 170.

[2] نسيمة بطيحي، **مرجع سابق**، ص83.

[3] فقد نصت **المادة 44 من قانون العقوبات في فقرتها الأولى:** «يعاقب الشريك في جناية أو جنحة بالعقوبة المقررة للجناية أو الجنحة"، فعملا بهذه القاعدة يخضع الشريك للعقوبة المقررة للجريمة التي ارتكبها الفاعل سواء من حيث الطبيعة أو من

إذا ترتب على الدخول حذف معطيات المنظومة أو تغييرها، تضاعف العقوبة وفق المادة 394 مكرر، وإذا ترتب تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة إلى ثلاث سنوات، وغرامة من 100.000 إلى 300.000 دج

ثانيا: عقوبة الشروع

يقصد بالشروع البدء في القيام بالشيء وفي الجريمة فيقصد به البدء في تنفيذها وقد جاءت الاتفاقية الدولية للإجرام المعلوماتي لتؤكد على المعاقبة على الشروع وهو النهج الذي تبناه المشرع الجزائري من خلال نص المادة 394 مكرر 7 من قانون العقوبات التي تنص على معاقبة الشروع في ارتكاب الجنح بالعقوبة المقررة للجنحة ذاتها، وعليه، فإذا تعلق الشروع بجنحة الدخول و البقاء غير المشروعين، تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 60.000 إلى 200.000 دج، وفق العقوبة المقررة للجريمة المعنية، مع مراعاة الأحكام الخاصة التي قد تنطبق على الفعل المرتكب.

من هنا يظهر سعي المشرع الجزائري الى تعزيز المنظومة الجنائية من خلال توسيع نطاق العقوبة ليجعل الشرع في الجرائم الماسة بالأنظمة المعلوماتية تخضع لنفس العقوبة المقررة للجريمة التامة على عكس المشرع الفرنسي الذي لم يأخذ بنفس المبدأ وراح الى تبني فكرة الشروع كأحمال تحضيرية أو التهيئة لم يصل بعد الى مرحلة التنفيذ[1].

الفرع الرابع: العقوبات التكميلية

إلى جانب العقوبات الأصلية، يمكن للقاضي الحكم بعقوبات تكميلية تهدف إلى تعزيز الردع ومنع تكرار الجريمة، وهو ما جاء به نص المادة 394 مكرر 6 ومن أهمها الغلق والمصادرة [2]، كما تنص على إمكانية الحكم بعقوبات تكميلية تتمثل في الحرمان من بعض الحقوق السياسية والمدنية والعائلية لمدة قد تصل إلى خمس سنوات ، كما يجوز منع المحكوم عليه من تولي الوظائف العامة أو ممارسة نشاط مهني أو اجتماعي ارتبط ارتكاب الجريمة به، إضافة إلى باقي العقوبات التكميلية الأخرى[3].

حيث المدة، وتطبق أيضا على الشريك العقوبات التكميلية التي تطبق على الجريمة التي ارتكبها الفاعل الأصلي، غير انه يسأل على الاشتراك إذا كان الفعل الأصلي جناية أو جنحة فقط أما إذا كانت مخالفة فلا يسأل على الاشتراك.

[1] نصت المادة **30 من قانون العقوبات الجزائري** على أن كل محاولات لارتكاب جناية تبتدئ بالشروع إذا لم تتوقف أو يخب أثارها

[2] انظر المادة **394 مكرر 6 قانون العقوبات الجزائري والمادة 323-فقرة 5** من القانون الفرنسي.

[3] حسين طاهري، جرائم القرصنة الإلكترونية، **مرجع سابق** ص 210.

أولا: المصادرة

وتشمل مصادرة الأدوات والأجهزة المستعملة في ارتكاب الجريمة (حاسوب، برامج اختراق...)، مصادرة البيانات أو الوسائل الرقمية محل الجريمة إذا أمكن ذلك قانونا

ثانيا: غلق المحل أو مكان الاستغلال

بالرجوع إلى نص المادة 394 مكرر 6 من قانون العقوبات الجزائري، نجد أن المشرع الجزائري قرر عقوبة الغلق في حالة ارتكاب جريمة الدخول أو البقاء ويتمثل في غلق المحل أو المؤسسة أو النظام المعلوماتي إذا كان قد استعمل كوسيلة لارتكاب الجريمة، أو تعليق نشاط الموقع الإلكتروني في بعض الحالات

الفرع الخامس: العقوبات المقررة للشخص المعنوي

إذا ارتكبت الجريمة باسم أو لحساب شخص معنوي (شركة، مؤسسة)[1]، فإن المسؤولية الجزائية تمتد إليه وفقا للقانون، وتعاقب المادة 394 مكرر و394 مكرر 3 و394 مكرر 4 من قانون العقوبات الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى لغرامة الشخص الطبيعي[2]، كما حددت المادة 18 مكرر من قانون العقوبات المسلطة على الشخص المعنوي وهي:

أولا: الغرامة المالية

تُعدّ الغرامة العقوبة الأصلية المقررة للشخص المعنوي، بالنظر إلى عدم قابلية تطبيق العقوبات السالبة للحرية عليه. ويُحدَّد مقدارها وفقًا للقواعد التي أقرّها المشرع الجزائري في المادة 18 مكرر من قانون العقوبات، إذ يتراوح بين مرة وخمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي عن الجريمة ذاتها، متى توافرت شروط تطبيق هذا النص، وذلك بما يتناسب مع طبيعة الشخص المعنوي وخطورة الفعل المرتكب.

ثانيا: العقوبات التكميلية

إلى جانب الغرامة، أجاز المشرع الجزائري إخضاع الشخص المعنوي لعقوبات تكميلية ترمي إلى الحد من قدرته على تكرار النشاط الإجرامي، ومن أبرزها:

[1] حسين طاهري، **الجرائم الإلكترونية**، مرجع سابق، ص 175.
[2] المادة 394 مكرر 4 من قانون العقوبات الجزائري

_حلّ الشخص المعنوي، متى توافرت الشروط القانونية المقررة لذلك.

_غلق المؤسسة أو أحد فروعها لمدة لا تتجاوز خمس سنوات.

_المنع من ممارسة نشاط مهني أو اجتماعي، بصورة مباشرة أو غير مباشرة، نهائيًا أو لمدة لا تتجاوز خمس سنوات.

_الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

_مصادرة الأشياء التي استُعملت في ارتكاب الجريمة أو نتجت عنها، وفقًا للشروط القانونية

_نشر حكم الإدانة أو تعليقه، بحسب ما يقرره الحكم القضائي

_الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، على أن تنصب الحراسة على النشاط الذي أدى إلى ارتكاب الجريمة

وعليه، تتحدد العقوبات المطبقة على الشخص المعنوي بحسب النص القانوني الذي يجرّم الفعل المرتكب، وطبيعة العقوبة المقررة له، ومدى توافر شروط مسؤولية الشخص المعنوي. وتكتسي هذه المسألة أهمية خاصة في جرائم القرصنة الإلكترونية التي تستهدف الأنظمة المعلوماتية ذات الطابع الحساس، متى نص القانون على ظروف مشددة أو عقوبات خاصة بشأنها.

خاتمة الفصل الثاني

من خلال دراسة الأحكام الموضوعية لجريمة القرصنة الإلكترونية، تم التطرق إلى طبيعتها القانونية وصورها المختلفة، مع بيان العناصر اللازمة لقيامها وفقًا للتشريع الجزائري، والمتمثلة في العنصر المادي الذي يتجسد في السلوك الإجرامي، والعنصر المعنوي الذي يعكس الحالة الذهنية للجاني واتجاه إرادته نحو ارتكاب الفعل المجرّم.

كما تناولت الدراسة المسؤولية الجزائية المترتبة عن ارتكاب هذه الجريمة، والعقوبات المقررة لها، مع مراعاة اختلاف الأحكام بحسب طبيعة الفعل المرتكب والظروف المحيطة به.

وتأسيسًا على ما سبق، فإن تحديد الأحكام الموضوعية لجريمة القرصنة الإلكترونية يمثل أساسًا لفهم خصوصية التعامل الإجرائي معها، الأمر الذي يستدعي الانتقال إلى دراسة إجراءات التحري والإثبات، وما تثيره من إشكالات قانونية وعملية في مجال الكشف عن هذه الجرائم وإقامة الدليل على ارتكابها.

الباب الثاني

الأحكام الإجرائية لجريمة القرصنة الإلكترونية في التشريع الجزائري

أصبحت وسائل الإعلام تتناول يوميا أخبارا تتعلق بأمن الشبكات وأنظمة الحاسوب، وهو ما يعكس استمرار الصراع بين القراصنة المعلوماتيين الذين يسعون إلى اختراق الأنظمة الرقمية، وبين المختصين في أمن المعلومات الذين يعملون على حماية البنية التحية الرقمية، وتتعدد هذه الأخبار بين الكشف عن عمليات اختراق الأنظمة الحساسة، أو الإعلان عن إحباط هجمات إلكترونية استهدفت شبكات معلوماتية ذات طابع استراتيجي، وهو ما يؤكد أن الفضاء المعلوماتي أصبح ساحة جديدة لمواجهة متواصلة بين طرفين: المعتدين على الأنظمة الرقمية من جهة ، وخبراء الأمن المعلوماتي من جهة أخرى[1].

بالرغم من أن الإجرام المعلوماتي في الواقع الجزائري، وكذا في العديد من الدول العربية ، لم يبلغ المستوى الذي وصلت إليه هذه الظاهرة في الدول المتقدمة، إلا أن ذلك لا يقلل من أهمية التنبه إلى بوادره الأولى والتصدي له في مراحل مبكرة، حتى لا تتفاقم مع التوسع السريع في استخدام تكنولوجيا المعلومات والاتصال، فمع انتشار الأنظمة المعلوماتية في مختلف القطاعات، وما صاحب ذلك من مظاهر العولمة الرقمية، ظهرت مخاطر جديدة تمس خصوصية البيانات الشخصية، وقد تمتد أثارها إلى المساس بالأمن الوطني والسيادة الرقمية للدول[2] .

فتبعا للتحول الحديث في الجرائم المعلوماتية التي أصبحت أكثر تعقيدا من الجرائم التقليدية نظرا لخصوصيته، وباعتبار أن القانون الجنائي يخضع في تطبيقه لمبدأ شرعية الجرائم والعقوبات، فلا يجوز للقاضي الجزائي تجريم الأفعال التي لم ينص عليها المشرع مهما بلغت درجة خطورتها ومن أبرزها القرصنة الإلكترونية التي تشير إلى جملة الأفعال غير المشروعة التي ترتكب باستخدام الوسائل المعلوماتية أو الشبكات الرقمية، بقصد التسلل إلى الأنظمة المعلوماتية أو استغلالها بطريقة غير قانونية، وتتمثل هذه الأفعال غالبا في اختراق أنظمة المعالجة الآلية للبيانات أو شبكات الحاسوب بهدف الوصول إلى المعلومات المخزنة فيها، وكذا الاطلاع على البيانات السرية، أو تعديلها أو إتلافها، أو حتى تعطيل عمل الأنظمة المعلوماتية وإرباك سيرها الطبيعي.[3]

---

[1] مناصرة يوسف، **الدليل الالكتروني في القانون الجزائي، الطريق إلى التحول أدلة الإثبات في المادة الجزائية**، دراسة مقارنة، دار الخلدونية، 2021، ص 13.

[2] مال قارة، مرجع سابق، ص 7.

[3] وائل رمضان، **القرصنة الإلكترونية بين الجريمة المنظمة والجهاد المشروع**، مجلة الفرقان الكويتية منشورة على الموقع الإلكتروني، http/www.alforquan.net/avile2954hlmt ، 2025/07/07، 10.00 سا.

من خلال استغلال ثغرات أمنية أو تقنيات اختراق تكون في الأغلب متطورة تسمح للقرصان المعتدي عليها بتجاوزها من خلال اتخاذ العديد من السلوكيات من بينها التجسس المعلوماتي، سرقة البيانات، العبث بالمعلومات المخزنة، أو تعطيل الخدمات الإلكترونية، وهي ممارسات تمس بشكل مباشر عناصر أمن المعلومات المتمثلة في السرية وسلامة البيانات وتكاملها، ،وعلى هذا الأساس فان الغرض الرئيسي لهذا النوع من الجرائم لا يقتصر على الاعتداء على الجهاز المادي للحاسوب، وإنما ينصب على النظام المعلوماتي وما يتضمنه من بيانات وبرامج وقواعد ومعلومات، فالبيانات المخزنة داخل الأنظمة أصبحت تمثل قيمة اقتصاديه واستراتيجية ذات أهمية كبيرة، الأمر الذي جعلها هدفا رئيسيا لمرتكبي جرائم القرصنة الإلكترونية، الذين يسعون إلى الوصول إليها بطرق غير مشروعة عبر استغلال الثغرات التقنية[1].

ومن ثم يثور التساؤل حول مدى كفاية القواعد القانونية التقليدية لمواجهة هذه الأفعال المستحدثة، خاصة أن أغلب النصوص الجزائية وضعت في إطار قانوني يرتبط بالاعتداءات المادية الملموسة، الأمر الذي يجعل تطبيقها على القيم غير المادية التي أفرزتها البيئة الرقمية أمرا يثير العديد من الصعوبات[2]، هذا ما جعلنا نستعرض في هذا الجزء من الدراسة النماذج القانونية المستعملة في مواجهة جريمة القرصنة الإلكترونية مع تحليلها حتى تسمح بتسهيل فهم طريقة التعامل مع هذا النوع من الجرائم ومدى وملاءمتها للطبيعة البيئة الرقمية،

وفي هذا السياق، جاء القانون رقم 09_04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، ليشكل الإطار التشريعي الأساسي الذي ينظم الأحكام الجزائية الخاصة بجريمة القرصنة الإلكترونية، من خلال تجريم مختلف الأفعال التي تستهدف الأنظمة المعلوماتية، كالدخول غير المشروع، والبقاء غير المصرح به، والاعتداء على سلامة البيانات، مع تقرير عقوبات تتناسب وخطورة الأفعال، كما عمل المشرع الجزائري على تدعيم هذه الأحكام من خلال إدخال تعديلات على قانون العقوبات، بما يضمن التكامل بين القواعد العامة والنصوص الخاصة.

غير أن هذه الأحكام الجزائية لا تتوقف عند مجرد النص القانوني، بل تمتد إلى آليات مكافحتها، سواء من خلال الإجراءات الوقائية التي تهدف إلى الحد من وقوع الجريمة، أو عبر الوسائل الإجرائية التي تمكن من كشفها ومتابعة مرتكبيها، خاصة في ظل ما تتميز به هذه الجرائم من طابع عابر للحدود وصعوبة

[1] حنان ريحان مبارك المضحكي، **مرجع سابق**، ص 101.

[2] مناصرة، يوسف، مرجع سابق، ص15.

الإثبات. وعليه فقد أولى المشرع الجزائري أهمية خاصة لتعزيز قدرات أجهزة الضبطية القضائية والجهات القضائية المتخصصة، من خلال استحداث أقطاب جزائية متخصصة وتبني وسائل تقنية حديثة في التحري والتحقيق.

وعلى هذا الأساس تطرقنا في هذا الباب إلى دراسة الأحكام الإجرائية المقررة لجريمة القرصنة الإلكترونية في التشريع الجزائري، وكذا الحماية الجزائية للمعلوماتية،[1] من خلال تناول خصوصية الإجراءات الجزائية من إجراءات البحث والتحري والمتابعة والإثبات الرقمي، أي الإطار الإجرائي لجريمة القرصنة الالكترونية في التشريع الجزائري **(الفصل الأول)** وكذا التحقيق والمحاكمة واليات مكافحة الجريمة في القانون الدولي والوطني **(الفصل الثاني)**.

[1] أمال قارة، مرجع سابق، ص 63.

الفصل الأول

خصوصية الإجراءات الجزائية

في جريمة القرصنة الإلكترونية

استعرضنا في الباب الأول من هذا البحث جريمة القرصنة الالكترونية بمفهوم عام وارتكزنا في تفصيل أركانها بوجه خاص كنوع من الجرائم المستحدثة التي أفرزتها التحولات العميقة التي يمر بها العالم في ظل الثورة الرقمية والتي أسفرت بدورها عن واقع إجرامي جديد، تجاوز الإطار التقليدي للجريمة ليشمل أنماطا مستحدثة، في مقدمتها جرائم القرصنة الإلكترونية التي تستهدف أنظمة المعالجة الآلية للمعطيات.

إن القواعد التقليدية المنصوص عليها في قانون الإجراءات الجزائية الجزائري، رغم أهميتها، لم تعد كافية لوحدها لمواجهة هذا النوع من الإجرام، الذي يعتمد أساسا على الدليل الرقمي ويستوجب وسائل تقنية متطورة في البحث والتحري والإثبات، والذي سنعطيه حقه في الشرح في هذا الباب. ومن ثم، كان لزاما على المشرع التدخل بإقرار آليات إجرائية خاصة تتلاءم مع طبيعة هذه الجرائم، من خلال توسيع صلاحيات الضبطية القضائية، وإقرار تفتيش الأنظمة المعلوماتية، واعتراض المراسلات الإلكترونية، والاستعانة بالخبرة الفنية، من خلال التعديل الجديد الذي طرأ على ق.إ.ج.ج المعدل والمتمم وفق القانون رقم 25-14 المؤرخ في 3 أوت 2025،[1] الذي ارتأى فيه المشرع الجزائري ضرورة التعديل في مواده بما يتلاءم مع هذه الجريمة.

غير أن هذا التطور الإجرائي يثير إشكالية دقيقة تتمثل في مدى قدرة هذه الإجراءات الخاصة على تحقيق التوازن بين فعالية المتابعة الجزائية من جهة، وضمان احترام الحقوق والحريات الأساسية، وعلى رأسها الحق في الخصوصية من جهة أخرى، خاصة في ظل خطورة المساس بالبيانات الشخصية.[2]

تركز الدعوى العمومية في قانون الإجراءات الجزائية الجزائري لسنة 2025 على كونها الأداة القانونية التي تمكّن الدولة من حماية النظام العام ومتابعة مرتكبي الجرائم، فهي تعبّر عن حق المجتمع في ملاحقة الجاني وتوقيع العقوبة عليه، وتتولاها النيابة العامة باعتبارها ممثلة للمصلحة العامة، وذلك وفقاً للإجراءات والضوابط التي يحددها القانون، وتكتسي الدعوى العمومية أهمية خاصة لارتباطها بتحقيق العدالة الجنائية، إذ تمر بعدة مراحل تبدأ بتحريكها، ثم مباشرتها، وصولاً إلى الفصل فيها بحكم قضائي، كما تتميز بخصائص تجعلها مختلفة عن غيرها من الدعاوى، من حيث أطرافها وطبيعتها والغاية منها، فضلاً عن القواعد التي تحكم انقضاءها أو وقفه[3]،

فيعود الأصل في تحريك هذه الدعوى إلى النيابة العامة، باعتبارها ممثلة للحق العام، غير أنه قد تتدخل جهات أخرى على سبيل الاستثناء في حالات محددة، وتستمر صفة المتهم قائمة إلى غاية صدور

---

[1] القانون رقم **25-14** المؤرخ في 3 أوت 2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 504، الصادرة بتاريخ 13 أوت 2025

[2] القانون **18-07** المتعلق بحماية البيانات ذات الطابع الشخصي، مرجع سابق.

[3] خليفي عبد الرحمان، مرجع سابق، ص 163

حكم قضائي نهائي يفصل في الدعوى، سواء بالإدانة أو البراءة أو بأي سبب آخر من أسباب انقضائها.

ومن المهم التمييز في هذا السياق بين مرحلتين أساسيتين، تختلف فيهما المراكز القانونية للأشخاص، ففي مرحلة البحث والتحري يكون الشخص محل شبهة فقط، يسمى بالمشتبه فيه حيث تباشر الضبطية القضائية إجراءات أولية للكشف عن الجريمة وجمع المعلومات، وغالباً ما تتم هذه الإجراءات تحت إشراف النيابة العامة، مع توفر قدر محدود من ضمانات الدفاع. أما في المرحلة القضائية، فيكتسب الشخص صفة المتهم، بعد توجيه الاتهام إليه رسمياً، وتتميز هذه المرحلة بقدر أكبر من الضمانات، مثل حق الدفاع وعلنية الإجراءات، إضافة إلى خضوعها لرقابة القضاء واستقلاله[1].

وبالنظر إلى خصوصية جرائم القرصنة الإلكترونية، فإنها تتسم بتقنية خاصة من إجراءات البحث والتحري إلى تحريك الدعوى العمومية والتحقيق فيها ثم متابعتها أمام الجهات القضائية وصولا إلى المحاكمة، أين تكتسي طابعا تقنيا يستوجب تكييف القواعد العامة مع طبيعة الدليل الرقمي. وهو ما سيتم التطرق إليه في هذا الفصل المتضمن **خصوصية الإجراءات الجزائية في جرائم القرصنة الالكترونية (المبحث الأول)، خصوصية الإثبات والدليل الرقمي في جرائم القرصنة الإلكترونية (مبحث ثاني).**

المبحث الأول: خصوصية الإجراءات الجزائية في جرائم القرصنة الإلكترونية

تتعدد الاختصاصات التي تمارسها الشرطة القضائية في إطار مهامها العادية، وتختلف عن الاختصاصات الاستثنائية التي تباشرها في حالات خاصة، كحالة اللجوء إلى أساليب التحري الخاصة، وتُعد إجراءات البحث والتحري المنصوص عليها في قانون الإجراءات الجزائية من الوسائل التي خولها المشرع لضباط الشرطة القضائية بهدف الكشف عن الحقيقة، والتحقق من وقوع الجريمة، وتحديد هوية مرتكبيها، وتقديمهم أمام وكيل الجمهورية، مع الالتزام بمبدأ الشرعية الإجرائية واحترام الحقوق والحريات الأساسية.

فمرحلة الاستدلال تعد مرحلة سابقة على تحريك الدعوى العمومية، ولا يشكل مرحلة من مراحلها القانونية، وإنما تهدف إلى جمع المعلومات والقرائن الأولية التي تساعد النيابة العامة على اتخاذ قرار المتابعة، وبخلاف التحقيق القضائي، فإن أعمال الاستدلال لا ترتب في الأصل أدلة بالمعنى القانوني الكامل، ولا يجوز أن تكون وحدها أساسًا لحكم القاضي، إلا في الحالات التي يقرر فيها القانون خلاف ذلك على سبيل الاستثناء. ويرجع ذلك إلى أن هذه المرحلة لا تتوافر فيها جميع ضمانات الدفاع اللازمة لإضفاء المشروعية الكاملة

[1] بلارو كمال، **الشرطة القضائية في التشريع الجزائري**، أطروحة دكتوراه، جامعة الإخوة منتوري، قسنطينة 1، 2001-2021، ص 63.

على الأدلة المستخلصة منها، بخلاف التحقيق القضائي الذي يتم تحت إشراف السلطة القضائية وتحيط به ضمانات قانونية أوفر[1].

غير أن المشرع الجزائري منح ضباط الشرطة القضائية اختصاصات استثنائية تقترب في طبيعتها من بعض إجراءات التحقيق، أوردها في القانون 06-22 المؤرخ في 20 ديسمبر سنة 2006، المعدل والمتمم لقانون الإجراءات الجزائية ثم أعاد تعزيزها بموجب القانون الجديد لسنة 2025، حيث خول لهم اتخاذ تدابير تمس الحرية الشخصية، كالتفتيش والحجز واعتراض المراسلات والتقاط الصور، المراقبة، مراقبة الاتصالات الإلكترونية، التسرب، وذلك استجابة لضرورات السرعة و الفعالية في مواجهة بعض الجرائم الخطيرة، كما تناول قانون الوقاية من الفساد ومكافحته أساليب أخرى في نص المادة 56 من القانون رقم 06-01 المؤرخ في 20 فبراير 2006 المعدل والمتمم بالقانون 11-15 المؤرخ في 2 أوت 2011 وهي تسليم المراقب، مع ذكر نفس الصور التي جاءت ضمن قانون الإجراءات الجزائية بتسميات مختلفة تتمثل في الترصد والاختراق[2].

وتتجلى خصوصية إجراءات البحث والتحري بصورة أوضح في جرائم القرصنة الإلكترونية، بالنظر إلى طبيعتها التقنية وتعقيد وسائل ارتكابها وسرعة زوال آثارها الرقمية. فقد فرضت هذه الخصوصية على المشرع تبني آليات إجرائية حديثة تتجاوز الوسائل التقليدية، مثل تفتيش الأنظمة المعلوماتية، وحجز البيانات الرقمية، واعتراض المراسلات الإلكترونية، واللجوء إلى الخبرة الفنية المتخصصة، فضلا عن اعتماد أساليب التحري الخاصة كالمراقبة الإلكترونية والتسرب الرقمي عند الاقتضاء. ومن ثم، فإن خصوصية هذه الإجراءات لا تكمن فقط في اتساع سلطات الضبط القضائي، وإنما أيضًا في ضرورة التوفيق بين فعالية البحث عن الأدلة الرقمية واحترام الضمانات القانونية المرتبطة بحماية الحياة الخاصة وحرمة المعطيات الشخصية[3].

المطلب الأول: إجراءات البحث والتحري في الجرائم المعلوماتية

يتحدد الإطار القانوني لاختصاصات الشرطة القضائية من خلال الأحكام الواردة في قانون الإجراءات الجزائية، فقد منح المشرع للشرطة القضائية صلاحية البحث والتحري عن الجرائم، وجمع الأدلة والقرائن المتعلقة بها، وكشف مرتكبيها والمساهمين فيها، فألزمت المادة 27 ضباط الشرطة القضائية بتحرير محاضر

---

[1] عبد الرحمان خلفي، **مرجع سابق**، ص 97

[2] القانون 06-01 المؤرخ في 20 فبراير 2006، **المتعلق بالوقاية من الفساد ومكافحته**، (ج.ر.ج.ج: عدد 14) المعدل والمتمم بالقانون 11-15 المؤرخ في 2 أوت 2011 (ج.ر.ج.ج.عدد44)

[3] خليفي عبد الرحمان، **مرجع سابق**، ص 126.

تتضمن مختلف الأعمال والإجراءات التي يباشرونها، مع إخطار وكيل الجمهورية المختص إقليمياً، بما يضمن خضوع أعمالهم لرقابة النيابة العامة واحترام الشرعية الإجرائية[1].

كما يشمل هذا الاختصاص تلقي البلاغات والشكاوى، ولو بوسائل إلكترونية، وسماع الأطراف بالوسائل التقليدية أو عبر وسائل الاتصال الحديثة متى توافرت الموافقة الصريحة وتم إثباتها بمحضر رسمي[2]، وهو ما يعكس تأثر التشريع الجزائري بالتطورات التقنية الحديثة في مجال الإثبات والإجراءات الجزائية.

ولا تقف اختصاصات الشرطة القضائية عند حدود الإجراءات المنصوص عليها صراحة، وإنما تمتد إلى كل إجراء يسمح به القانون ويهدف إلى الوصول إلى الحقيقة، شريطة احترام الضمانات القانونية وحقوق الأفراد.

وقد كرس المشرع الجزائري هذا التوجه منذ سنة 2017، من خلال اعتماد مصطلح «الشرطة القضائية» بدلًا من مصطلح «الضبطية القضائية»، بما يعكس التوجه نحو توحيد المصطلحات القانونية المتعلقة بهذه الهيئة. وتتمثل مهام الشرطة القضائية أساسًا في البحث عن الجرائم، وجمع الاستدلالات بشأنها، والكشف عن مرتكبيها، وذلك وفقًا للاختصاصات والإجراءات المحددة قانونًا. وعند افتتاح التحقيق القضائي، تتولى تنفيذ الإجراءات التي تكلفها بها جهة التحقيق في حدود الإنابات والأوامر الصادرة عنها، وتحت إشرافها، بما يضمن التكامل بين مرحلة البحث والتحري ومرحلة التحقيق القضائي.[3]

الفرع الأول: اختصاص الشرطة القضائية المختصة في الجرائم المعلوماتية

ينشأ حق الدولة في العقاب مباشرة بعد وقع الجريمة، ولا تملك الدولة توقيع هذا العقاب إلا عن طريق الدعوى العمومية طبقا لقاعدة " **لا عقوبة بغير دعوى**".

لكن قبل عرض الدعوى العمومية على القضاء لابد من الحديث عن مرحلة تسبقها وهي مرحلة تمهيدية يتم فيها ضبط المجرم والتحري عن الجريمة وجمع الأدلة، ويسيطر على هذه المرحلة جهاز يعرف في قانون الإجراءات الجزائية بالشرطة القضائية، وتسمى هذه المرحلة عند البعض بالمرحلة الشبه قضائية قياسا على

---

[1] تنص المادة 20 فقرة 3 من قانون الإجراءات الجزائية" **ويناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في التشريع الجزائري وجمع الأدلة عنها والبحث عن مرتكبيها والمساهمين فيها مادام لم يبدأ فيها تحقيق قضائي**"

تنص المادة 21"**وإذا ما افتتح تحقيق قضائي، يجب على الضبط القضائي تنفيذ تفويضات جهات التحقيق وأوامرها وتسخيراتها**"

[2] المادة 26 فقرة 1 "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 20 و21 أعلاه، ويتلقون الشكاوى والبلاغات بأي وسيلة كانت بما فيها **الطريق الإلكتروني** ويقومن بجمع الاستدلالات وإجراء التحقيقات الابتدائية.

[3] خليفي عبد الرحمان، مرجع سابق، ص 97.

مرحلة لاحقة عليها تسمى بالمرحلة القضائية وهي مرحلة مهمة لا يمكن الاستغناء عنها لأنها ممهدة للعمل القضائي وسبيل النيابة العامة في اتخاذ قرار مناسب كما أنها جامعة للدليل المؤسس للدعوى.[1]

أولا: صلاحيات الشرطة القضائية المنصوص عليها في المواد 20 إلى 28 من قانون الإجراءات الجزائية.

تتولى الشرطة القضائية، في إطار الاختصاصات التي حددها قانون الإجراءات الجزائية، مجموعة من المهام المرتبطة بالبحث والتحري عن الجرائم والكشف عن مرتكبيها وجمع الأدلة اللازمة لإثباتها. وقد حدد المشرع الجزائري هذه الصلاحيات، لاسيما ضمن المواد 20 إلى 28 من قانون الإجراءات الجزائية، بما يضمن مباشرة أعمال الاستدلال والتحري تحت إشراف السلطة القضائية وفي الحدود التي رسمها القانون

وتتمثل أهم هذه الصلاحيات في تلقي الشكاوى والبلاغات المتعلقة بالجرائم، وجمع الاستدلالات وإجراء التحريات اللازمة للكشف عن الجرائم ومرتكبيها، والانتقال إلى أماكن وقوعها ومعاينتها، والمحافظة على الأدلة والآثار المتصلة بها، وتحرير المحاضر المتعلقة بالإجراءات التي يباشرونها، فضلا عن تنفيذ ما يندرج ضمن اختصاصهم من أوامر وتعليمات السلطة القضائية. كما يخول القانون للشرطة القضائية، متى توافرت شروط ذلك، مباشرة بعض الإجراءات التي تمس حقوق الأفراد وحرياتهم وفقا للضوابط والشكليات المقررة قانونا.

وتتخذ هذه الصلاحيات أهمية خاصة في مجال جرائم القرصنة الإلكترونية، إذ لا يقتصر عمل الشرطة القضائية فيها على البحث التقليدي عن الأدلة، وإنما يمتد إلى التعامل مع الأدلة الرقمية والكشف عن مصدر الأفعال الإجرامية وتحديد مستخدمي الأنظمة والحسابات والأجهزة محل الجريمة، مع ضرورة احترام الضمانات القانونية المقررة لجمع هذه الأدلة وحفظها.

وعليه، فإن دراسة صلاحيات الشرطة القضائية في مجال جرائم القرصنة الإلكترونية تقتضي التمييز بين الصلاحيات العامة في البحث والتحري التي تمارسها الشرطة القضائية في مختلف الجرائم، وبين الإجراءات ذات الطبيعة التقنية أو الخاصة التي يقررها القانون لمواجهة خصوصية الجريمة المعلوماتية، وهو ما سيتم بيانه تباعا.

[1] استبدل المشرع الجزائري مصطلح الضبطية القضائية بالشرطة القضائية وفقا للقانون رقم 17-07 المؤرخ في: 27 مارس سنة 2017 المعدل والمتمم للأمر رقم 66-155 المؤرخ في: 08-يونيو سنة 1966 (ج.ر.ج.ج. عدد20) (الملغى)، ليتمسك بمصطلح الشرطة القضائية، في قانون الإجراءات الجديد تحت رقم 25-14 المؤرخ في: 03غشت 2025(ج.ر.ج.ج.عدد 54).

ثانيا: صلاحيات البحث والتحري في البيئة الرقمية

تشكل إجراءات البحث والتحقيق الإطار الذي يتم من خلاله تكوين صورة واضحة للجريمة وظروفها المحيطة، مما يسمح للسلطات بكشف الغموض وملاحقة الجناة والقبض عليهم. هذه تدابير تمهيدية وتحضيرية مصممة لتسهيل جمع الأدلة ودعم كل من التحقيق الأولي وإجراءات المحاكمة في البحث عن الحقيقة .من هذا المنظور، تمثل مرحلة التحقيق التمهيدي حجر الزاوية في الإجراءات الجنائية، حيث إنها تشكل الأساس الجوهري الذي تُبنى عليه الملاحقة القضائية بأكملها. وبناءً على ذلك، سنتناول أهم التعديلات التي تم إدخالها في هذه المرحلة.

ثالثا: توسيع نطاق تشكيل الشرطة القضائية وضباطها

نظراً للزيادة الأخيرة في الجرائم المنظمة العابرة للحدود مثل الاتجار بالبشر وغسل الأموال والاتجار بالمخدرات والهجرة غير الشرعية عن طريق البحر، سعى المشرع الجزائري إلى معالجة الثغرات المؤسسية من خلال توسيع فئات الأشخاص المخولين بصلاحيات الشرطة القضائية .أدخلت المادة 23 (الفقرتان 7 و8) من القانون رقم 25_14 فئتين جديدتين من ضباط الشرطة القضائية :الضباط الإداريون في الشؤون البحرية وقادة الوحدات العائمة التابعة لجهاز خفر السواحل الوطني؛ مفتشو الملاحة البحرية والعمل، بالإضافة إلى عملاء خفر السواحل الذين خدموا لمدة ثلاث سنوات على الأقل ويتم تعيينهم بشكل مشترك من قبل وزير الدفاع الوطني ووزير العدل .وبالمثل، وسعت المادة 29 من القانون رقم 25-14 فئات مساعدي الشرطة القضائية لتشمل الشؤون البحرية.[1]

الفرع الثاني: وسائل التحري

نسعى في هذا الفرع للتعرف على السياسة الإجرائية المتبعة للبحث والتحري في مسرح الجريمة الالكترونية في ضوء قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين المعدل والمتمم بالقانون

25-11 في مجال المعطيات الشخصية ذات الطابع الشخصي التي تهدف لحماية حق الفرد في حماية معلوماته الشخصية من أي اعتداء، خاصة وأن الفرد لا يمكن الاستفادة من الخدمات الالكترونية إلا بعد أن يدرج بياناته الشخصية على منصات افتراضية، وهذه الأخيرة قد أثبت الواقع أنها ليست في مأمن من

[1]Abd-el-Kader FELLAH, **Procedural Development sin the Stages of Preliminary Investigation and Trial (A Study in Light to flaw 25-14)**,ZAOULIN°11, Vol. 8, November 2025, pp 138.

الاختراق والقرصنة[1]. لذلك تهدف الدراسة للتعرف على الأحكام التي تخص الأدلة الالكترونية، وكيفية استخلاصه وجمعه من حيث جمع الاستدلالات من ضبط وتفتيش وإجراءات الاستعانة بالخبرة، وبيان مدى حجية هذه الأدلة التي تحوزها كوسائل للإثبات أمام القضاء[2].

أولا: تفتيش الأنظمة المعلوماتية وحجز المعطيات

يكتسي التفتيش أهمية بالغة في البحث عن الأدلة والكشف عن الحقيقة لكنه يبقى في أساسه إجراءً خطيراً لما قد يثيره من حساسية فيما يتعلق بحرية الأشخاص وكرامتهم وممتلكاتهم، وعلى هذا فقد نظم المشرع الجزائري إجراءات التفتيش وأخضعه لضوابط صارمة، فهو يعتبر من إجراءات التحقيق ولا يكون من أعمال التحري إلا استثناء في الجريمة المتلبس بها.[3] وسنتعرف على إجراء التفتيش فيما يتعلق في الجرائم المعلوماتية وكذا التعرف على الاستثناءات الواردة عليها والتمييز بينها وبين الطرق التقليدية للتفتيش.

أ: السلطة المختصة بالتفتيش عن طريق التسخير القضائي

إن مشكلة التحري في الجرائم الرقمية تتمحور حول طبيعة هذا النوع من الجرائم كونها تتعلق ببيانات معالجة الكترونيا وكيانات غير مادية يصعب الكشف عنها، ويصعب في الغالب جمع الأدلة بشأنها بالطرق المألوفة، في الجرائم التقليدية، وتزداد الصعوبة إذا تعلق الأمر بتفتيش البيانات والأنظمة المعلوماتية الموجودة خارج النطاق الوطني (الجرائم العابرة للحدود) لأن الأمر قد يصطدم بسيادة الدول وعليه فإن إسناد مهمة التفتيش في الجرائم المعلوماتية وكيفيات إجراءها تحتاج الدقة وهو ما سنتعرف عليه في النقاط التالية:

1_ مفهوم التفتيش الالكتروني:

لم تتضمن مختلف التشريعات تعريفا دقيقا للتفتيش، مما ترك المجال للفقه والقضاء للاجتهاد في تحديد مفهومه. وقد تعددت التعريفات الفقهية لهذا الإجراء.

---

[1] سي حاج محند أرزقي، مرجع سابق، ص .48

[3] القانون 18-07 المؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، صادر في الجريدة الرسمية رقم 34 المؤرخ في 10 يناير 2018، . المعدل والمتمم بالقانون رقم 25-11 ، أين أدركت الجزائر أهمية تقنين إستعمال المعطيات ذات المؤرخ في 28 محرم عام 1447 الموافق 24 يوليو سنة 2025 الطابع الشخصي عملا بالتعديل الدستوري الصادر في سنة 2016 المتبوع بالتعديل سنة 2020 الجريدة الرسمية عدد 14 بتاريخ 7 مارس 2016، المؤكد بمقتضى تعديل سنة 2020.

[3] أحمد فتحي سرور، **مرجع سابق**، ص 135.

فقد عرفه بعض من الفقه على أنه إجراء من إجراءات التحقيق، تقوم به سلطة يحددها القانون، يهدف إلى البحث عن الأدلة المادية لجناية أو جنحة، والتي قد توجد في مكان خاص يتمتع بالحماية القانونية، بغض النظر عن إرادة صاحبه.

ومن جهة أخرى، يعرف التفتيش بأنه :البحث داخل الأماكن أو الأشخاص عن دليل يفيد في كشف الحقيقة بشأن جريمة معينة، وهو من الإجراءات التي يباشرها قاضي التحقيق أو من يفوضه القانون بذلك[1]، كضباط الشرطة القضائية.كما يرى بعض الفقه أن التفتيش هو :عملية البحث والتحري داخل نطاق معين عن أدلة مادية تثبت ارتكاب جريمة، ويعد من أهم إجراءات التحقيق الجنائي[2].

أما بالنسبة لتفتيش الأنظمة المعلوماتية، فقد عرّف بعض الفقه التفتيش الالكتروني على أنه: البحث في مكونات النظام المعلوماتي أو داخله عن بيانات أو معطيات ذات صلة بجريمة معينة، بهدف كشف الحقيقة[3].

ويشمل ذلك:

- البحث والتفتيش في أجهزة الحاسوب
- أو في أي نظام معلوماتي
- سواء كان متصلًا بشبكة الإنترنت أو غير متصل

ويهدف هذا النوع من التفتيش إلى ضبط الأدلة الرقمية، مثل:

- البرامج المعلوماتية
- الملفات المخزنة
- المعطيات الإلكترونية

وذلك قصد استخدامها في إثبات الجريمة.

---

[1] لامية مجدوب، **إجراءات التفتيش في التزوير الإلكتروني**، مجلة التواصل في الاقتصاد والادارة والقانون، جامعة باجي مختار، عنابة، المجلد 25، العدد 3، سبتمبر 2019، ص 110.

[2] بكري يوسف بكري، التفتيش عن المعلومات في الوسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2011، ص57.

[3] رضا همسي، **تفتيش المنظومات المعلوماتية في القانون الجزائري**، مجلة العلوم القانونية والسياسية، عدد 05، جوان 2012، ص 160.

عندما يتعلق الأمر، بجرائم المعلوماتية، يمكن قاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك[1].

لذلك، يجب أن يتوافر في التفتيش شرطان أساسيان:

1.1-الشروط الموضوعية

وتتمثل في وجود جريمة (جناية أو جنحة) وقعت بالفعل، ووجود دلائل أو قرائن تشير إلى ارتباط شخص أو مكان بالجريمة، وأن يكون الهدف من التفتيش هو البحث عن أدلة تساعد في كشف الحقيقة.

2.1_الشروط الشكلية للتفتيش في جرائم المعلوماتية

وأهمها صدور إذن بالتفتيش من الجهة القضائية المختصة وأن يكون هذا الإذن محددًا بدقة، سواء من حيث المكان أو الأشياء المراد ضبطها[2] .

أن يكون محل التفتيش مشروعًا (فلا يجوز مثلًا تفتيش مقرات تتمتع بحصانة كالمقارات الدبلوماسية وفي مجال الجرائم المعلوماتية، تبرز صعوبة عملية، وهي أن تحديد محل التفتيش بدقة يتطلب معرفة تقنية متخصصة (مثل تحديد ذاكرة الحاسوب أو وسائط التخزين)، وهو ما قد يتجاوز في بعض الأحيان المعرفة الفنية لرجال الضبط القضائي[2].

وبناءً على ذلك، يمكن القول أن التفتيش في الجرائم الإلكترونية ينصبّ على محورين رئيسيين : المكونات المادية للحاسوب (الأجهزة ووسائط التخزين)، المكونات غير المادية (البيانات والبرامج)، وذلك بشكل غير مباشر عبر الوسيط المادي أو من خلال وسائل تقنية خاصة.

وعلى هذا الأساس فان التفتيش في الأصل يبحث عن أشياء ملموسة، لكن في الجرائم الإلكترونية الأدلة غير ملموسة (بيانات). لذلك، يتم تفتيش الأجهزة التي تحتوي هذه البيانات بدلًا من البيانات نفسها، مع ضرورة احترام شروط قانونية دقيقة، رغم صعوبة ذلك تقنيًا في بعض الحالات [3].

نتيجة الخصوصية التي تتميز بها الجرائم الالكترونية فإن إجراءات التفتيش المتعلقة بها تتسم بخصوصية إجرائية تفرقها عن غيرها وهو ما نتناوله في النقاط التالية:

2_ خصوصية الميقات الزمني لإجراء التفتيش الالكتروني

إن فرض القيود الزمنية على إجراء التفتيش يعد وسيلة فعالة للحد من حالات التعسف في استعمال السلطة، إذ يساهم في تحقيق التوازن بين ضرورات المصلحة العامة، كما يُعد ضمان الاحترام الحياة الخاصة

---

[1] المادة 78 / الفقرة الأخيرة، القانون 25-14، **مرجع سابق.**

[2] سامي حسين الحسيني، **النظرية العامة للتفتيش في القانون المصري والقانون المقارن**، دار النهضة العربية، القاهرة، 1972، ص 210.

[3] خالد أحمد لطفي، **جرائم الإنترنت**، مرجع سابق، ص 164.

للأفراد. ومن هذا المنطلق، أوجب المشرع الجزائري على السلطات المختصة الالتزام بميقات محدد لإجراء التفتيش، يمتد من الساعة الخامسة صباحا إلى غاية الثامنة مساء، مراعاة لحرمة الحياة الخاصة.[1]

غير أن هذا المبدأ لم يكن مطلق بل وردت عليه استثناءات منها ما يتعلق بالجرائم المعلوماتية، والتي أطلق عليها وصف "الجرائم الماسة بالمعالجة الآلية"، لما تتميز به من خطورة بالغة، وسرعة في محو أو إتلاف آثارها، إضافة إلى إمكانية ارتكابها في أي وقت، وبناءً على ذلك خول المشرع للسلطات المختصة صلاحية مباشرة لإجراء التفتيش في هذا النوع من الجرائم في أي وقت دون التقيد بالقيود الزمنية المعتادة لفعالية التحقيق ومواكبة خصوصية هذا النمط من الجرائم.[2]

1.2 _إجراء التفتيش بحضور المتهم أو من ينوب عنه

اشترط المشرع الجزائري لإجراء عملية التفتيش في المعطيات المخزنة في المنظومة المعلوماتية، إعمال قاعدة الحضور تطبيقا لأحكام المادة 05 من القانون 09-04 التي تُحيل إلى الأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية بحيث يشترط ضرورة حضور صاحب مسكن المشتبه في ارتكاب الجريمة أو صاحب مسكن شخص من الغير يحوز أوراقا أو أشياء تتعلق بالجريمة لعملية التفتيش أو من ينوبها أو حضور شاهدين إذا تعذر حضورهما بحس ما ينص عليه ق,إ,ج،[3] لكن الاستثناء في الجرائم الإلكترونية بموجب التعديلات التي جاء بها قانون 25-14:

يمكن لضابط الشرطة القضائية إجراء التفتيش دون حضور المتهم أو الشهود في الحالات التالية:

إذا تعلق الأمر بجرائم تكنولوجيا الإعلام والاتصال.

وعليه، يتضح أن المشرّع الجزائري من خلال القانون 25-14 قد سعى إلى تحقيق توازن دقيق بين متطلبات حماية الحقوق والحريات الفردية من جهة، وضرورة تعزيز فعالية البحث والتحري في الجرائم

---

[1] المادة فقرة 01، ق إ. ج. ج، مرجع سابق.

[2] حسب الاستثناء الذي ورد في نص **المادة 78/ 3** " وعندما يتعلق الأمر بجرائم القتل العمدي، والمخدرات والمؤثرات العقلية، والجريمة المنظمة عبر الحدود الوطنية، والجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع لخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد، وجرائم التهريب، وجرائم الاتجار بالبشر، وجرائم الاتجار بالأعضاء، وجرائم تهريب المهاجرين، وجرائم اختطاف الأشخاص، فإنّه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مكتوب مسبق من وكيل الجمهورية المختص.

[3] رضا هميسي، **المرجع السابق، ص** 169.

الإلكترونية من جهة أخرى، من خلال إقرار قواعد مرنة تراعي خصوصية هذا النوع من الجرائم دون الإخلال بالضمانات الأساسية للمحاكمة العادلة.

2.2 التفتيش والضبط الإلكتروني

يعد التفتيش في معناه الفني إجراء من إجراءات التحقيق ووسيلة من وسائل الإثبات الجنائي، فهو يهدف أساسا إلى ضبط أشياء مادية لها صلة بالجريمة أو تساعد في كشف الحقيقة. غير أن هذا المفهوم التقليدي يصطدم بطبيعة الأدلة الرقمية، التي تتمثل في برامج وبيانات إلكترونية غير ملموسة، ولا وجود مادي محسوس لها في العالم الخارجي[1].

وعلى هذا الأساس، لا يمكن إخضاع البيانات الرقمية بذاتها للتفتيش أو الضبط بالمفهوم التقليدي، لأنها ليست أشياء مادية. لهذا، اتجه الفقه والقانون إلى معالجة هذا الإشكال من خلال اعتبار أن التفتيش في الجرائم المعلوماتية ينصبّ على الوعاء المادي الذي يحتوي هذه البيانات، مثل الحواسيب، الأقراص الصلبة، الأقراص الممغنطة، ووسائط التخزين المختلفة. ومن ثم، فإن ضبط هذه الوسائط يعد في حقيقته وسيلة غير مباشرة للوصول إلى الأدلة الرقمية.

ويعد تفتيش أنظمة المعلومات، سواء تعلق بالحاسوب أو بالشبكات، نوعا من التفتيش القانوني يخضع لنفس الأحكام العامة، مع ضرورة مراعاة خصوصيته التقنية.

3_التفتيش الإلكتروني في التشريع الجزائري:

خول المشرع الجزائري للسلطات المختصة بمهام التفتيش، بموجب نص المادة 5 في الفقرة الأخيرة من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، صلاحية الاستعانة بأي شخص يمتلك خبرة في تشغيل الأنظمة المعلوماتية محل التحقيق، أو لديه دراية بالإجراءات الأمنية المتبعة لحماية البيانات التي تتضمنها هذه الأنظمة، وذلك من أجل تسهيل تنفيذ عمليات التفتيش وتوفير المعطيات الضرورية لضمان نجاعة المهمة[2].

في السابق، لم تكن البيانات الرقمية تعامل كدليل مستقل، بل من خلال الجهاز الذي يحتويها، لذلك، كان يتم التعامل معها بطريقة غير مباشرة، من خلال اعتبارها مرتبطة بالدعامة المادية التي تخزن عليها، مثل الأقراص أو الحواسيب، فيتم حجز هذه الوسائط واستغلال ما تحتويه من بيانات كدليل في الإثبات ومع تطور الجرائم المعلوماتية، برزت الحاجة إلى إيجاد توازن بين الإجراءات التقليدية (كالتفتيش

[1] سيد على السيد محمد، مرجع سابق، ص 97.

[2] حليم رامي، **مرجع سابق**، ص140.

والحجز) والطبيعة الخاصة للبيانات الرقمية، التي تتميز بسرعة الانتشار وسهولة التعديل أو الإتلاف[1]. ولهذا جاء القانون رقم 09-04 ليُدخل نوعًا من التكييف القانوني، حيث أقرّ بإمكانية إخضاع المعطيات الإلكترونية لإجراءات شبيهة بتلك المطبقة على الأشياء المادية، مع مراعاة خصوصيتها التقنية، وقد استحدث هذا القانون وسائل حديثة تمكن من الحفاظ على الأدلة الرقمية، مثل الإسراع في تأمين البيانات ومنع ضياعها أو تغييرها، وذلك بسبب طبيعتها غير المستقرة وإمكانية انتقالها داخل أنظمة معلوماتية مترابطة عبر الشبكات، كما سمح بجمع المعطيات الإلكترونية أثناء عملية التفتيش، بما يتلاءم مع البيئة الرقمية[2]

وفي هذا السياق، جاءت الأحكام المتعلقة بالتفتيش الإلكتروني لتمنح السلطات المختصة صلاحيات في العالم الافتراضي تعادل تلك الموجودة في العالم المادي، بحيث يمكن البحث عن البيانات المخزنة وضبطها كما هو الحال بالنسبة للوثائق التقليدية. فبعد أن كان التفتيش ينصبّ على مستندات مكتوبة أو أشياء ملموسة، أصبح يشمل أيضًا البيانات الإلكترونية التي تُجمع وتُحفظ بطرق تقنية خاصة.

غير أن جمع هذه المعطيات يبقى خاضعًا لضوابط قانونية صارمة، إذ يجب أن يتم أثناء فترة التفتيش المحددة قانونًا، وإلا اعتبر هذا الإجراء باطلًا، كما يشترط الحصول على إذن مسبق من الجهة القضائية المختصة[3].

ومنه فان المشرع الجزائري من خلال سنه للمادة 05 من القانون 09-04 سعى إلى إرساء سلطات في العالم الافتراضي تتماشى مع السلطات الموجودة في عالم الأشياء المادية في إطار التفتيش الكلاسيكي

---

[1] مناصرة يوسف، **الدليل الإلكتروني في القانون الجزائي**، مرجع سابق، ص 354.

[2] مناصرة يوسف، **مرجع سابق**، ص 355

[3] تنص **المادة 05 من القانون 09-04** "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من نفس القانون، الدخول بغرض التفتيش ولو عن بعد إلى:

أ _ منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها

ب_ دعامات تخزين معلوماتية تسمح بتخزين المعطيات المعلوماتية، في الحالات المنصوص عليها في الفقرة أ من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة، إلى هذه المنظومة أو جزء منها بعد الإخبار المسبق للسلطة القضائية المختصة.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

الخاص بالوثائق والمستندات، تضمنت المادة حالات تمديد التفتيش عن بعد وكذا المساعدة الدولية في إطار الاتفاقات الدولية بالنسبة للجرائم التي تقع خارج إقليم الدولة[1].

ثانيا: حجز البيانات الرقمية والنسخ الإلكتروني للمعطيات

يعد الهدف الأساسي من تفتيش المنظومة المعلوماتية هو وضع اليد على الأدلة الرقمية التي من شأنها المساهمة في كشف الحقيقة وتحديد هوية الفاعل، وهو ما يستلزم اتخاذ تدابير خاصة لحجز هذه المعطيات، بالنظر إلى طبيعتها التقنية التي تُمكّن من محوها أو تعديلها في وقت وجيز وبوسائل بسيطة. وفي الحالات التي يتعذر فيها الحجز لأسباب تقنية، أجاز المشرع للسلطات المختصة اتخاذ إجراءات بديلة، كمنع الوصول إلى هذه المعطيات أو تقييد استعمالها. [2]

1_ تدابير الحجز

تتميز المعطيات المعلوماتية بكونها غير مادية، إذ تخزن في ذاكرة الحاسوب أو ضمن برامجه على شكل إشارات أو نبضات إلكترونية، وهو ما أثار جدلا فقهيا حول قابليتها للحجز.

غير أن المشرع الجزائري حسم هذا الإشكال من خلال إضفاء حماية قانونية على قواعد البيانات، واعتبارها من المصنفات المحمية، وفق ما نصت عليه المادة 5 الفقرة 2 من الأمر رقم 05-03 المتعلق بحقوق المؤلف والحقوق المجاورة[3].

كما نصت المادة 6 الفقرة 1 من القانون 09-04 على ضرورة نسخ المعطيات اللازمة على دعامة تخزين إلكترونية قابلة للحجز والوضع في أحراز، مثل الأقراص الصلبة، والأقراص المضغوطة، والذاكرة الوميضية، وغيرها من الوسائط، مع إبقاء المجال مفتوحًا أمام استيعاب التطورات التقنية الحديثة في وسائل التخزين.

ويتم الحجز وفقا للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، لا سيما بعد تعديله بموجب القانون 25-14، مع ضرورة احترام الضمانات الأساسية، كسرية المعلومات وحقوق الدفاع، بما

---

[1] مناصرة يوسف، **نفس المرجع**، ص 358.

[2] يزيد بولحيط، **تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري**، مجلة التواصل في الاقتصاد والإدارة والقانون، عدد48، ديسمبر 2016، ص 90.

[3] يزيد بولحيط، **نفس المرجع**، 91.

يضمن سلامة المعطيات وعدم المساس بمحتواها. كما يمكن إعادة تشكيل هذه المعطيات بما يخدم مصلحة التحقيق، شريطة الحفاظ على مضمونها الأصلي، تحت طائلة العقوبات المنصوص عليها قانونًا.

وإلى جانب الحجز، أجاز المشرع اتخاذ تدابير تكميلية، كالمصادرة وغلق المواقع الإلكترونية المستعملة في ارتكاب الجريمة، وذلك وفقًا لما تضمنه قانون العقوبات.

2_الحجز عن طريق منع الوصول إلى المعطيات وحدود استعمالها

نظرا للصعوبات التقنية التي قد تعترض عملية الحجز، نصت المادة 7 من القانون 09-04 على إمكانية اللجوء إلى وسائل تقنية تحول دون الوصول إلى المعطيات أو نسخها، وذلك في حالة استحالة الحجز المباشر.

ويشمل ذلك منع الدخول إلى المنظومة المعلوماتية أو تقييد استعمال النسخ المتاحة للمستخدمين المرخص لهم[1].

غير أن المشرع لم يحدد على وجه الدقة ماهية الأسباب التقنية التي تحول دون الحجز، وهو ما يفهم منه ترك المجال لتقدير الجهات المختصة بحسب طبيعة كل حالة، أو إذا تعلق الأمر بوجود أنظمة حماية معقدة، أو صعوبات تقنية في نسخ البيانات. وهذا يبرز أهمية توفير الإمكانيات التقنية والتكوين المستمر لأعوان الضبطية القضائية، بما يُمكّنهم من التعامل مع هذا النوع من الجرائم بفعالية.

ويبقى الهدف من هذه التدابير هو منع الجاني من الوصول إلى المعطيات أو استغلالها أو إتلافها، نظرا لكونها تمثل محل الجريمة ومصدرا أساسيا للإثبات.

كما قيد المشرع استعمال المعلومات المتحصل عليها من هذه الإجراءات، بحيث لا تُستخدم إلا في إطار التحريات والتحقيقات القضائية، وذلك تحت طائلة العقوبات، وفقًا لما نصت عليه المادة 9 من القانون 09-04[2].

ثالثا: المعاينة

تعتبر المعاينة من أهم إجراءات البحث التحري والإثبات، إذ تتمثل في الانتقال إلى مكان الجريمة أو فحص شخص أو شيء معين لإثبات حالته والكشف عن الآثار المرتبطة بالفعل الإجرامي، ويهدف هذا الإجراء إلى جمع العناصر المادية من أدوات مستعملة التي تساعد في إظهار الحقيقة مع وضع الأختام على الأماكن التي تحتوي على أدلة مهمة، وإخطار النيابة العامة بكامل الإجراءات المتخذة

[1] لامية مجدوب، **مرجع سابق**، ص 111.

[2] تنص المادة 09 من القانون رقم 09-04 على أنه: تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات والتحقيقات القضائية، **مرجع سابق**، ص07.

وفي الجرائم المعلوماتية والقرصنة الإلكترونية تبرز خصوصية المعاينة بسبب الطبيعة التقنية للجريمة فها لابد من التمييز بين الجرائم التي تمس المكونات المادية للحاسب، كجهاز الحاسوب أو الكابلات وشاشة العرض ومفاتيح التشغيل وغيرها وبين الجرائم التي تستهدف المكنات غير المادية كالبرامج والبيانات والمعطيات الرقمية[1].

ففي الحالة الأولى لا تثير المعاينة صعوبة كبيرة، إذ يمكن لمأموري الضبط القضائي معاينة الأجهزة وحجزها والتحفظ على أدواتها على أساس أنها أدلة مادية ملموسة، أما في الجرائم التي تقع على البيانات والبرامج فان المعاينة هنا تصبح أكثر تعقيدا بسبب ضعف الآثار المادية وسهولة محو البيانات أو تعديلها، إضافة إلى كثرة الأشخاص الذين قد يستعملون النظام المعلوماتي مما يؤدي إلى اختلاط الآثار الرقمية أو العبث بها قبل كشفها[2].

فيظهر أن المعاينة الرقمية لها صعوبات أهمها طول الفترة الفاصلة بين ارتكاب الجريمة واكتشافها مما قد يؤدي إلى التشكيك في سلامة الأدلة[3] مما يستدعي ضرورة إخضاع هذه المعاينة إلى إرشادات فنية دقيقة منها:

أ_ توثيق مكان الجريمة رقميا، وتصوير الأجهزة وملحقاتها قبل فحصها

ب_ تسجيل تاريخ ووقت ومكان المعاينة

ج_ تثبيت حالة النظام قبل أي تدخل تقني

د_ عدم نقل الأجهزة قبل التأكد من سلامة البيانات

و_ تجنب تشغيل أو تعديل النظام المعلوماتي دون ضرورة

هـ_ فحص وسائط التخزين والأقراص التالفة أو المحطمة والتحفظ على المستندات والمخرجات الورقية المرتبطة بالنظام

ن_ رفع البصمات والآثار المادية الموجودة على الأجهزة والوثائق

ي_ الاستعانة بالخبرة التقنية المتخصصة أثناء المعاينة[4].

بالرغم من الإجراءات الموصي باتخاذها في مواجهة الدليل الرقمي عن طريق المعاينة الرقمية إلا أن الأمر يظل نسبيا فقط فلابد من وضع تنظيم إجرائي خاص يراعي طبيعة المعطيات الإلكترونية المتغيرة.

المطلب الثاني: إجراءات المتابعة الجزائية في جرائم القرصنة الإلكترونية

---

[1] بدري فيصل، مرجع سابق، ص 204.

[2] طاهري حسين، جرائم القرصنة الإلكترونية، **مرجع سابق**، ص 172-173.

[3] أمير فرج يوسف، **العالم ما وراء التقليدي ميتا فيرس ومستقبل العالم الافتراضي** وتطور الجريمة الرقمية والمعلوماتية الالكتروني، مركز المحمود لتوزيع الكتب القانونية، الطبعة الأولى، 2024، 147.

[4] طاهري حسين **نفس المرجع**، ص 174

تعد جريمة القرصنة الإلكترونية من الجرائم المستحدثة في مجال البيئة الرقمية، تدخل المشرع الجزائري لتكييف المنظومة القانونية مع هذا النوع المستحدث من الجرائم، من خلال وضع قواعد إجرائية خاصة تتعلق بكيفية تحريك الدعوى العمومية، بما يضمن فعالية المتابعة الجزائية من جهة، واحترام الحقوق والحريات الأساسية من جهة أخرى.

تنشأ عن الجريمة آثار قانونية متعددة، تختلف باختلاف الجهة التي أصابها الضرر، فإذا كان الفعل المرتكب يمس بالنظام العام، تتدخل الدولة عن طريق النيابة العامة لمتابعة الجاني والمطالبة بتطبيق العقوبة المنصوص عليها قانوناً، ويتم ذلك من خلال تحريك الدعوى العمومية وإحالتها إلى القضاء للفصل فيها، وفي المقابل، قد يترتب عن الجريمة ضرر يلحق بالأفراد، سواء كان ماديا كالإضرار بالممتلكات، أو معنويا كالمساس بالشرف والاعتبار. وفي هذه الحالة، يكون للمتضرر الحق في رفع دعوى مدنية تابعة، هدفها المطالبة بالتعويض عن الضرر الذي أصاب الضحية.

كما يمكن أن تفرز الجريمة نوعا آخر من المسؤولية إذا كان مرتكبها مرتبطا بوظيفة أو بهيئة معينة، حيث يعد الفعل إخلالاً بالواجبات المهنية أو التنظيمية، وهنا قد تبادر الجهة المستخدمة إلى تحريك دعوى تأديبية بغرض مساءلة الفاعل وفرض الجزاءات المناسبة وفقاً للأنظمة الداخلية[1]

وانطلاقاً من ذلك، سيتم التطرق إلى مفهوم الدعوى العمومية وبيان مراحلها، ثم تناول باقي أنواع الدعاوى المرتبطة بالجريمة، مع إبراز خصائص كل منها بشكل مبسط ومنظم تعتبر مرحلة تحريك الدعوى العمومية أهم مرحلة باعتبارها العنصر الأساسي لمتابعة الجريمة، إضافة إلى إجراءات التحقيق التي تليها باعتبارها اليد المساعدة في الكشف عن الحقيقة وجمع أدلة الإثبات، خاصة في ظل التقنية الحديثة في ارتكاب الجريمة.

وفي نفس السياق جاء قانون الإجراءات الجزائية الجزائري الجديد بإضافة مهمة في كل المراحل التي تمر عليها الدعوى العمومية، ولدى كافة السلطات المساهمة في محاربة الجريمة فقام بتعزيز عمل الشرطة القضائية على مستوى التحقيق الابتدائي، كما أدرج بدائل جديدة للدعوى العمومية،[2] خاصة ما يتعلق منها

[1] عبد الرحمان خليفي، الإجراءات الجزائية في القانون الجزائري والمقارن، دراسة تأصيلية تحليلية مقارنة، وفق القانون 25-14، المؤرخ في 9 صفر عام 1447، الموافق ل 3 غشت سنة 2025(ج. ر.ج.ج عدد54)، دار بلقيس، الجزائر، سبتمبر 2025، ص159.

[2] عبد الرحمان خلفي، **نفس المرجع**، ص 08.

بالدعاوى التي تخص الجرائم المعلوماتية وقد خصصت هذا الفصل لتحديد الإجراءات التي تمر بها الدعوى العمومية والتحقيق في هذا النوع من الجرائم.

الفرع الأول: خصوصية تحريك الدعوى العمومية في جرائم القرصنة الإلكترونية

وبما أن القانون يمنح النيابة العامة صلاحيات تحريك الدعوى العمومية متى تبين لها ذلك لازما لتحقيق حماية للمجتمع ومتى رأت أي تجاوز للقانون، إلا أن القانون يمنح أيضا أشخاص آخرين إمكانية تحريك الدعوى طبقا لما يحدده من شروط، غير أن مباشرة الدعوى وممارستها تبقى من اختصاص النيابة العامة وحدها دون سواها، سواء بالنسبة للدعاوى التي تحركها هي أو تلك التي يحركها أشخاص آخرون.

تعرف الدعوى العمومية حسب بعض الفقه بأنها" المطالبة بالحق العام أمام القضاء الجنائي، أو مطالبة النيابة العامة –نيابة عن المجتمع–بتوقيع العقاب على المتهم في جريم بواسطة القضاء الجنائي"، وقد جاءت المادة 39 من قانون الإجراءات الجزائية لتحديد هذا المفهوم وسبب إنشائها[1]، باعتبارها وسيلة لتوجيه الاتهام من طرف النيابة العامة بهدف مطالبة القضاء بتطبيق القانون، ولاقتضاء حق المجتمع في العقاب، فالنيابة العامة هي طرف من أطراف الدعوى العمومية وتمارس إجراءاتها باسم المجتمع ونيابة عنه.[2]

تتميز الدعوى العمومية بعدة خصائص تختلف باختلاف الأنظمة الإجرائية التي تأخذ بها التشريعات، فبعضها يغلب عليه الطابع الاتهامي حيث يكون للضحية دور أساسي في تحريك الدعوى، أول بينما يعتمد النظام الإجرائي الجزائري على الطابع التنقيبي، الذي يمنح للدولة، ممثلة في النيابة العامة، الدور الأساسي في تحريك ومباشرة الدعوى العمومية[3]. وتزداد أهمية هذه الخصائص في مجال جرائم القرصنة الإلكترونية، خاصة بعد تعديل سنة 2025 الذي جاء لمواكبة التطور التكنولوجي من خلال ما سوف نتطرق إليه من خصائص.

---

[1] تنص المادة 39 من قانون الإجراءات الجزائية على انه "**تباشر النيابة العامة الدعوى العمومية باسم المجتمع وتطالب بتطبيق القانون، وهي تمثل أمام كل جهة قضائية، ويحضر ممثلها أمام جهات التحقيق والحكم ويتعين أن ينطق بالأحكام في حضوره، كما تتولى العمل على تنفيذ أحكام القضاء ولها في سبيل مباشرة وظائفها أن تلجأ إلى القوة العمومية، كما تستعين بضباط وأعوان الشرطة القضائية**".

[2] بوحجة نصيرة، **سلطة النيابة العامة في تحريك الدعوى العمومية فيا لقانون الجزائري**، مذكرة ماجستير، كلية الحقوق –بن عكنون، جامعة الجزائر، 2001–2002، ص 34،35.

[3] أسامة عبد الله قايد، **شرح قانون الإجراءات الجنائية**، دار النهضة العربية، القاهرة، 2007، ص 247.

أولا: خصوصية الدعوى العمومية لجرائم القرصنة الإلكترونية

لقد عمل المشرّع الجزائري، في إطار قانون الإجراءات الجزائية لسنة 2025، على تكييف قواعد البحث والتحري مع خصوصية الجرائم المرتكبة باستعمال تكنولوجيات الإعلام والاتصال، بما يسمح بتعزيز فعالية الكشف عنها وجمع أدلتها. ويظهر ذلك من خلال إقرار وتنظيم جملة من الآليات الإجرائية ذات الصلة بالبيئة الرقمية، بما يتيح للجهات المختصة مباشرة إجراءات البحث والتحري وفق الضوابط القانونية المقررة.[1]

وهو ما يعكس خصوصية هذه الجرائم مقارنة بالجرائم التقليدية، ويؤثر بشكل مباشر على كيفية تحريك الدعوى ومباشرتها، فالدعوى العمومية في جرائم القرصنة الإلكترونية لا تقتصر على حماية مصلحة فردية، بل تمتد لحماية الأمن المعلوماتي والاقتصادي للدولة، نظرا لخطورة هذه الجرائم العابرة للحدود وتأثيرها الواسع.

أ_ خضوعها لمبدأ الشرعية مع توسيع سلطة النيابة العامة

يقوم نظام الشرعية الإجرائية على إلزام النيابة العامة بتحريك الدعوى العمومية كلما توافرت لديها معطيات جدية تثبت وقوع جريمة مستوفية لأركانها القانونية، مع وجود أدلة أو قرائن كافية تسمح بإسنادها إلى مرتكب معلوم أو مجهول الهوية. غير أن خضوع الدعوى العمومية لمبدأ الشرعية لا يعني مباشرة المتابعة بصورة آلية أو شكلية، وإنما يفرض على النيابة العامة التحقق مسبقا من التكييف القانوني للوقائع ومدى انطباق النص الجزائي عليها، إضافة إلى التأكد من إمكانية مباشرة المتابعة قانونا في ظل انتفاء الموانع التي تحول دونها، كوفاة المتهم أو انقضاء الدعوى العمومية بالتقادم أو قيام سبب قانوني يمنع السير فيها، فضلا عن ضرورة استيفاء القيود الإجرائية التي قد يشترطها القانون، كالشكوى أو الطلب أو الإذن في بعض الجرائم[2].

وفي الجرائم المعلوماتية برز اتجاه تشريعي حديث نحو تدعيم فعالية النيابة العامة في تحريك الدعوى العمومية، بالنظر إلى خصوصية هذا النوع من الجرائم وما يتميز به من سرعة التنفيذ وسهولة محو الأدلة وصعوبة الكشف عن مرتكبيه. لذلك جاء التعديل الإجرائي لسنة 2025 ليعزز من سلطات النيابة العامة في مباشرة المتابعة التلقائية متى تعلق الأمر بجرائم تمس أمن الأنظمة المعلوماتية أو المعطيات الإلكترونية، دون التقيد في بعض الحالات بانتظار شكوى المتضرر، وذلك تكريسا لفكرة الحماية الاستباقية للمصلحة العامة وضمانا لفعالية السياسة الجنائية في مواجهة الإجرام الرقمي .

ب_ اعتماد وسائل تحقيق تقنية خاصة

تتميز الدعوى العمومية في هذا المجال باعتماد وسائل مستحدثة، مثل:

التفتيش الإلكتروني، اعتراض الاتصالات، التسرب الإلكتروني، المراقبة الرقمية، وهو ما يعكس

[1] ايت حمودة كهينة، البحث والتحري الجنائي في مسرح الجريمة الإلكترونية، **مرجع سابق**، ص 5.

[2] خليفي عبد الرحمان، **مرجع سابق**، ص 173.

خصوصية الإثبات في هذه الجرائم مقارنة بالجرائم التقليدية[1]، الذي تم التطرق إليه في الباب الأول

ج_ المرونة الإجرائية لمواكبة الطبيعة الرقمية للجريمة

أقر المشرع نوعًا من المرونة في الإجراءات، كإمكانية إجراء التفتيش عن بعد والدخول إلى الأنظمة المعلوماتية، وهو ما يشكل استثناءً على القواعد التقليدية، بهدف الحفاظ على الدليل الرقمي من الضياع أو التلاعب.

د_ الطابع العابر للحدود

تتميز الدعوى العمومية في جرائم القرصنة الإلكترونية بكونها قد تتجاوز الإقليم الوطني، مما يستدعي التعاون القضائي الدولي، وهو ما أخذ به المشرع ضمنيًا من خلال توسيع آليات المتابعة[2]

ثانيا: الجهات المختصة بتحريك الدعوى في جرائم القرصنة الالكترونية

لم يعد من الممكن الاعتماد فقط على الوسائل الكلاسيكية في البحث والتحري، بل أصبح من الضروري تدخل جهات مختصة تمتلك تكوينا قانونيا وتقنيا يسمح لها بالكشف عن الأدلة الرقمية وتتبع مرتكبي هذه الجرائم.

إن النيابة العامة جهاز يعمل ويضمن عدم إفلات مرتكبي الجرائم من العقاب، وذلك بتوجيهها الاتهام لهم عن الأفعال المجرمة التي يقدمون على ارتكابها بتحريكها للدعوى العمومية. وهذا من اجل المطالبة بحسن تطبيق القانون وبهدف تسليط العقوبة على منتهكيه ومخالفيه[3]، ولذلك تمارس مهامها واختصاصاتها خلال مختلف الإجراءات الجزائية ومراحل الدعوى العمومية بناء على السلطة المخولة لها والصلاحيات الممنوحة من قبل القانون، بهدف قيامها بالدور المعهود إليها على أكمل وجه[4].

---

[1] ايت حمودة كهينة، **نفس المرجع**، ص 6-7

[2] لخاز صلاح بوقاني، **الحماية الجنائية الموضوعية للمعلوماتية**، دراسة مقارنة، الفكر الجامعي، الإسكندرية، الطبعة الأولى، ص 50.

[3] تنص المادة **02 من قانون الإجراءات الجزائية** على أن "الدعوى العمومية لتحريك العقوبات يحركها ويباشرها القضاة أو الموظفون المعهود إليهم بما يقتضي القانون" وبالتحليل الفقهي والقضائي، فان المقصود أساسا من القضاة أو الموظفون ، النيابة العامة (الادعاء العام) الممثلة في وكيل الجمهورية والنائب العام وهي الجهة الأصلية المختصة بتحريك الدعوى العمومية وأكدت الدراسات الحديثة حول القانون 25-14 أن النيابة العامة تبقى صاحبة الاختصاص الأصيل في تحريك الدعوى العمومية وتقدير ملائمة المتابعة ، أما القانون الجديد فلم يغير الجهة المختصة ، لكنه أدخل قيودا أهمها تعزيز سلطة النيابة العامة في تقدير ملائمة المتابعة .

[1] خلفي عبد الرحمان، **مرجع سابق**، ص 160.

فخول المشرع الجزائري مهمة متابعة الجرائم المعلوماتية والتحقيق فيها إلى عدة جهات، تتقدمها النيابة العامة باعتبارها صاحبة الاختصاص في تحريك الدعوى العمومية، إلى جانب مصالح الشرطة القضائية المختصة التي تتولى إجراءات البحث والتحري وجمع الأدلة الرقمية، فضلا عن قاضي التحقيق الذي يمارس سلطاته في الجرائم التي تستوجب فتح تحقيق قضائي. كما عمل المشرع على توسيع صلاحيات هذه الجهات ومنحها آليات خاصة تتلاءم مع طبيعة الإجرام الإلكتروني، بهدف تحقيق فعالية أكبر في مكافحة هذا النوع من الجرائم وحماية الأنظمة المعلوماتية والمعطيات الإلكترونية من مختلف الاعتداءات .

وعليه، سوف نتطرق من خلال هذه العناصر إلى دور النيابة العامة مع إبراز اختصاصها المستحدث في الجرائم المعلوماتية:

أ: دور النيابة العامة في تحريك جرائم القرصنة الالكترونية وفق المادة 39 من قانون إ.ج.ج

جعل المشرع من النيابة العامة سلطة الادعاء العام بغرض الحفاظ على حقوق المجتمع وملاحقة المجرمين، وأعمالا لذلك خصها بمبدأ الملائمة بحيث يكون لها الحق في تحريك الدعوى العمومية ومباشرتها كَمَا يُمكنها أن تقرر حفظها حتى مع توافر أركان الجريمة ومعرفة فاعلها[1]، ولكن قد يرى المشرع في بعض الحالات أن الضرر الذي نشأ عن الجريمة أكثر مساسا بمصلحة المجني عليه من المصلحة العامة، وقد يرى هذا الأخير أن من صالحه – ووفقا لتقديره الشخصي والعائلي – ألا تحرك الدعوى العمومية ضد الفاعل، وامتناعه هذا يغل يد النيابة العامة على تحريك الدعوى، في أحوال أخرى يعلق المشرع تحريك الدعوى العمومية على طلب من إدارة معينة أو إذن من جهة مختصة بذاتها، ونفس الشيء يكون من حقهما رفع القيد أو إبقائه حتى ترجع للنيابة العامة سُلطتها في تحريك الدعوى، وهذه الأحوال تعرف عند الفقه بقيود تحريك الدعوى العمومية، وسوف نخصص لها فرع مستقل، في أحوال أخرى كذلك نجد أن المشرع الجزائري ولحكمة خاصة لا يجعل تحريك الدعوى العمومية حكرا على النيابة العامة وحدها تحريك الدعوى[2].

بموجب المادة 310 وما يليها من قانون الإجراءات الجزائية الجديد، يمتد الاختصاص الإقليمي لوكيل الجمهورية لدى الأقطاب الجزائية المتخصصة ليشمل كامل الإقليم المحدد لها بموجب التنظيم المعمول به. وفيما يخص الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مَنح المشرّع بموجب المادتين 337 و338

[1] المادة 39 من ق.إ.ج.ج.

[2] محمد حزيط، **مرجع سابق**، ص 17.

من ذات القانون اختصاصاً نوعياً وإقليمياً موسعاً وحصرياً لنيابة القطب الجزائي الوطني لمكافحة الجرائم المعلوماتية، مما يخولها مباشرة إجراءات المتابعة والتحري عبر كامل التراب الوطني دون التقيد بحدود الدوائر القضائية الكلاسيكية، وذلك استناداً إلى المادة 339 التي تكرس مرونة تمديد الاختصاص بالنظر للطبيعة الافتراضية والعابرة للحدود لهذه الجرائم، وهو ما عززته الأحكام المستحدثة الخاصة بالقواعد الإجرائية والتحري الرقمي والمعاينة الإلكترونية الواردة في هذا القانون.

وفيما يخص الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، نص المشرع الجزائري في المواد 335 إلى 340 من القانون رقم 25-14 المؤرخ في 3 أوت 2025، المتضمن قانون الإجراءات الجزائية، على تنظيم اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث نصت المادة 336 على ممارسة وكيل الجمهورية لدى هذا القطب وقاضي التحقيق ورئيسه صلاحياتهم في كامل الإقليم الوطني، فيما حددت المادتان 337 و338 حالات الاختصاص الحصري للقطب، ونظمت المادتان 339 و340 الإجراءات المتعلقة بهذا الاختصاص والاختصاص المشترك.

ب: الاختصاص المستحدث للنيابة العامة في الجرائم المعلوماتية[1]

تنص المادة 39 من قانون الإجراءات الجزائية الجديد (القانون رقم 25-14 المؤرخ في 3 أوت 2025) صراحة على أن "**تمثل نيابة الجمهورية المجتمع لدى المحكمة التي تمارس فيها وظائفها، وهي تباشر الدعوى العمومية باسم المجتمع وتطلب تطبيق القانون.**" وطبقا لنص المادة فقد توسع المشرع الجزائري في قانون الإجراءات الجزائية الجديد (القانون 25-14 المؤرخ في 3 أوت 2025) في مفهوم "**الاختصاص الموسع**" ليتجاوز القواعد التقليدية (مكان وقوع الجريمة، موطن المتهم، مكان القبض عليه)، وذلك لمواجهة الطبيعة "العابرة للحدود" و"الرقمية" للجرائم المعقدة.

بموجب القانون الجديد، تم تكريس القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

1_المعيار النوعي: الاختصاص لا يتحدد بالجغرافيا بل بنوع الجريمة (الإرهاب الإلكتروني، المساس بالأنظمة الحساسة للمعالجة الآلية للمعطيات التابعة للدولة، التجسس الرقمي).

1-تحدد المادة 39 من قانون الإجراءات الجزائية رقم 25-14 المؤرخ في 3 أوت 2025 مهام النيابة العامة، من خلال مباشرتها الدعوى العمومية باسم المجتمع، والمطالبة بتطبيق القانون، وتمثيلها أمام الجهات القضائية، فضلاً عن العمل على تنفيذ الأحكام والاستعانة بضباط وأعوان الشرطة القضائية.

2_تمديد الاختصاص بقوة القانون: بمجرد تكييف الجريمة كجريمة معلوماتية معقدة، يمتد اختصاص وكيل الجمهورية لدى هذا القطب ليشمل كامل التراب الوطني دون الحاجة لإجراءات تمديد تقليدية.

ثالثا: الاختصاص الإقليمي لوكيل الجمهورية.

حددت المواد 37 إلى 40، و329، من ق.إ.ج، الاختصاص الإقليمي للجهات القضائية، فيستلزم تسيير القضاء وسرعة الفصل في القضايا وفض النزاعات، تعدد المحاكم وانتشارها لتكون بقدر من الإمكان قريبة من موطن الخصوم أو من محل تواجد موضوع النزاع القائم يتم هذا بالنسبة للقضاء العادي، أما بالنسبة للقضاء الجزائي فيتحدد الاختصاص المحلي أو الإقليمي على أساس مكان وقوع الجريمة أو مكان إقامة المشتبه فيه[1]، هذا ما سنتناوله من خلال **تعريف الاختصاص المحلي للنيابة العامة (أولا)، وحدود هذا الاختصاص(ثانيا)**

أ: الاختصاص المحلي للنيابة العامة

وهذه القواعد تخص المحاكم والمجالس القضائية فحسب لأنه لا توجد سوى محكمة عليا واحدة لها اختصاص يشمل كامل التراب الوطني، فنظرا لأهمية تحديد الاختصاص الإقليمي نتطرق من خلال هذا الفرع إلى تعريفه حيث يعرف بأن:" الاختصاص الإقليمي هو ولاية الجهة القضائية بالنظر في

الدعاوى المرفوعة أمامها استنادا إلى معيار جغرافي يخضع للتقسيم القضائي". وبمعنى آخر الحيز الجغرافي الذي تختص كل محكمة النظر والفصل في القضايا والدعاوى التي تثار فيه والذي يتم تحديده عن طريق التنظيم، فدور الاختصاص الإقليمي إذن هو تحديد محكمة معينة بالجهات القضائية التابعة لها لكي تنظر في الدعاوى وتعمل في حدودها.[2]

[1] بموجب **القانون 25-14** تم توسيع الاختصاص لبعض الجهات القضائية خاصة في الجرائم المعقدة مثل الجرائم المعلوماتية مثل الأقطاب المتخصصة فيتميز الاختصاص بازدواجية خاصة، حيث يخضع من جهة لقواعد الاختصاص الإقليمي التقليدية القائمة على مكان ارتكاب الجريمة أو لإقامة الفاعل، مع التوسع فيها بالنظر إلى تعدد أماكن تحقق الفعل الإجرامي في البيئة الرقمية، ومن جهة أخرى يمتد الاختصاص الإقليمي الجزائري ليشمل الجرائم المرتكبة خارج الإقليم متى كان لها أثر داخله أو مست مصالحه ، وهو ما يعكس خصوصية الجرائم المعلوماتية ذات الطابع العابر للحدود .

[2]– سعيد بوحملة، الاختصاص النوعي والإقليمي

30 09 2025، 07:18 صباحا. - 2-fr.scribd.com-document-627885147

ب_ تعريف الاختصاص المحلي للنيابة العامة

تنص المادة 310 من قانون الإجراءات الجزائية "يجوز تمديد الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق والمحكمة إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والمؤثرات العقلية، وجرائم التهريب، وجرائم الاتجار بالبشر، وجرائم الاتجار بالأعضاء، وجرائم تهريب المهاجرين واختطاف الأشخاص، والمضاربة غير المشروعة، وتدعى هذه الجهات القضائية في صلب النص "الأقطاب القضائية المتخصصة".

ونشير هنا إلى أن ما يلاحظ على النصوص الجديدة هو اعتماد المشرع على المصطلح الإقليمي بدلا من المحلي وذلك للانسجام مع أحكام الدستور من الناحية الاصطلاحية، أما الاختصاص المحلي للنيابة العامة يعني أن النيابة كجزء من النظام القضائي في دولة معينة، لها سلطة محددة لمتابعة الجرائم وملاحقة المتهمين داخل نطاق جغرافي محدد وهذا النطاق يشير إلى المنطقة الجغرافية التي تخضع لسلطة القانون فتتخذ النيابة العامة الإجراءات القانونية وتمارس اختصاصاتها وصلاحياتها داخل نطاق جغرافي محدد، وهذا المبدأ يهدف إلى ضمان سير القانون وتسيير القضاء بطريقة منظمة مما يساهم في تحقيق العدالة والتوازن في نظام العدالة الجنائية[1].

الفرع الثالث: امتداد الاختصاص الإقليمي إلى كامل الإقليم الوطني

إذ وسع المشرع بمقتضى المادة 24 فقرة 7 من قانون الإجراءات الجزائية الاختصاص الإقليمي لضباط الشرطة القضائية التتابعين للأمن الوطني والدرك الوطني ليمتد إلى كامل الإقليم الوطني إذا تعلقت أعمال البحث والتحري بجرائم القتل العمدي والمخدرات والمؤثرات لعقلية والجريمة المنظمة عبر الحدود الوطنية والجرائم المتصلة بتكنولوجيات الإعلام الاتصال وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف حركة رؤوس الأموال من وإلى الخارج وجرائم الفساد وجرائم التهريب وجرائم الاتجار بالبشر جرائم الاتجار بالأعضاء وجرائم تهريب المهاجرين وجرائم اختطاف الأشخاص.

أما ضباط الشرطة القضائية التابعين للمصالح العسكرية للأمن أو للمصالح المركزية للشرطة القضائية فلهم الاختصاص الوطني على كافة الإقليم الوطني، بصفة أصلية أيا كانت الجريمة محل البحث والتحري وهذا بمقتضى الفقرة 6 من المادة 24 [2]،

[1] المادة 310 من القانون 25-14.

[2] المادة 24 من القانون 25-14.

كما جعل المشرع الاختصاص لضباط الشرطة القضائية التابعين للديوان الوطني لقمع الفساد يمتد في الجرائم المرتبطة بها إلى كامل الإقليم الوطني بمقتضى المادة 24 مكرر من القانون الوقاية من الفساد ومكافحته على أن يعمل هؤلاء تحت إشراف النائب العام المختص إقليميا واعلام وكيل الجمهورية المختص إقليميا بذلك بمقتضى الفقرة الأخيرة من المادة 24 من قانون الإجراءات الجزائية.

أولا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

في إطار مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أنشأ المشرع الجزائري على مستوى مجلس قضاء الجزائر قطبا جزائيا وطنيا متخصص في مكافحتها، وقد تم استحداث هذا القطب بموجب الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021 (الملغى)، وقد أبقى قانون إ.ج.ج الجديد على هذا القطب المختص بالمتابعة والتحقيق في هذا النوع من الجرائم وكذا الجرائم المرتبطة بها، [1]كما يختص بالحكم في ذات الجرائم إذا كانت تشكل جنحا[2].

ثانيا: النقل الوجوبي للملف من المحكمة المختصة إقليميا للقطب الجزائي

يتم التخلي وجوبا عن الملف الجزائي من المحكمة المختصة إقليميا سواء كان على مستوى التحريات الأولية أو المتابعة أو التحقيق القضائي إلى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إذا طلب هذا الأخير الملف أي بمعنى تمسك الأخير باختصاصه على النحو الوارد في المواد 317-329 من ق،إ،ج،ج.

إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام الاتصال مع اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مع اختصاص القطب الجزائي الوطني الاقتصادي والمالي يؤول الاختصاص وجوبا لهذا الأخير طبقا لنص المادة 341 من ق إ.ج.ج، أما إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا

[1] أمر 21-11 مؤرخ في غشت 2021، المعدل والمتمم للأمر رقم 66-155المؤرخ في 08يونيو سنة 1996، المتضمن قانون إ.ج.ج (ج.ر.ج.ج) **الملغى**.

[2] أنشأ المشرع الجزائري الأقطاب المتخصصة، منها القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بموجب قانون الإجراءات الجزائية، المعدل والمتمم لا سيما بعد التعديلات التي وسعت الاختصاص النوعي والإقليمي لهذه الأقطاب لتشمل الجرائم المعلوماتية ذات الطابع المعقد والعابر للحدود

الإعلام والاتصال مع اختصاص القطب الجزائي الوطني لمكافحة الإرهاب والجريمة المنظمة عبر الوطنية يؤول الاختصاص وجوبا لهذا الأخير وفقا لنص المادة 342 ق إ.ج.ج.[1]

المبحث الثاني: النظام القانوني للإثبات في جرائم القرصنة الالكترونية

تتسم جرائم القرصنة الإلكترونية، باعتبارها أحد أخطر الجرائم المعلوماتية، بطابعها العالمي وبخصوصية أركانها، خاصة من حيث وسائل ارتكابها وطبيعة أثارها، وهذا ما يجعلها تختلف جوهريا عن الجرائم التقليدية التي تقوم على أدلة ملموسة، إذ أن هذه الجرائم تتم في بيئة رقمية غير مرئية، مما يفرض الاعتماد على نوع خاص من الأدلة يعرف بالأدلة الرقمية Digital Evidences.

وتتميز هذه الأدلة بأهمية بالغة في مجل الإثبات، باعتبارها الوسيلة الأساسية لكشف الحقيقة وتحديد هوية الجناة، خاصة في ظل صعوبة تتبع الأفعال الإجرامية التي ترتكب عبر الأنظمة المعلوماتية الشبكات[2].

يرتكز إثبات الجريمة المعلوماتية أساسا على الدليل الجنائي الرقمي، باعتباره الوسيلة الأكثر فعالية في كشف هذا النوع من الإجرام المستحث، ويقصد بالدليل الرقمي كل معطى ذي طبيعة رقمية، يستخرج من أنظمة أو وسائط إلكترونية، ويكون قابلا للتجمع والتحليل باسطة تقنيات وبرمجيات متخصصة، بهدف استخلاص معلومات يمكن الاستناد إليها في ربط الفعل الإجرامي بمرتكبه وإثبات علاقته بالمجني عليه.

كما يأخذ هذا الدليل أشكالا متعددة، كالرسائل والنصوص المكتوبة، والصور، والتسجيلات الصوتية، والبيانات الرسومية، وغيرها من المخرجات الرقمية التي تخزن أو تنقل عبر وسائط إلكترونية، ومن مميزاته أنه ذو طبيعة غير مادية، ما يجعله عرضة للتغيير أو المحو، وهو الأمر الذي يتطلب إجراءات تقنية دقيقة للحفاظ على سلامته وضمان حجيته أمام جهات إنفاذ القانون[3].

يقصد بالدليل الرقمي كل معطى أو أثر يتم استخراجه من أجهزة الحاسوب أو الوسائط الإلكترونية المستعملة في مختلف مراحل الجريمة، حيث يكون في شكل بيانات أو إشارات أو نبضات رقمية يمكن تجميعها وتحليلها باستخدام تقنيات وبرامج متخصصة[4].

إلا أن التعريف الضيق لمفهوم الدليل الرقمي على ما لم يتم استخراجه من الحاسوب يعد تضييقا غير مبرر لنطاقه، إذ يمكن الحصول عليه من مختلف الأجهزة الرقمية، كالهاتف الذكي، وأجهزة التصوير ،

---

[1] عبد الرحمان خلفي، **مرجع سابق**، ص 206.

[2] محمود الرشيدي، **العنف في جرائم الإنترنت، الدار المصرية**، لبنان، 2011، ص43

[3] المنظمة العالمية لأدلة الحاسوب IOCE، تعرف الدليل الرقمي بانه" المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمي.

[4] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، مرجع سابق، ص 253.

ووسائط التخزين، وغيرها من الوسائل التي تعتمد المعالجة الإلكترونية للبيانات، مما يوسع من دائرة مصادر الإثبات في الجرائم المعلوماتية[1]، ناهيك عن فعاليته لا تكتمل إلا في إطار منظومة متكاملة من الآليات القانونية والتقنية الرامية إلى مكافحة الجريمة والحد من انتشارها، فالإثبات رغم أهميته، يبقى مرحلة من مراحل المواجهة الجنائية، تسبقه إجراءات وقائية تحريات تقنية، كما تليه تدابير ردعية وتنظيمية، وهو ما يقتضي دراسة مختلف الآليات المعتمدة لمكافحة جرائم القرصنة الإلكترونية[2]، وذلك على الصعيد الإجرائي أو الفني أو المؤسساتي.

ويأتي قانون الإجراءات الجزائية الجزائري الجديد رقم 25- 14لسنة 2025 ليضع إطارا قانونيا حديثا لمواجهة هذه التحديات، من خلال تنظيم إجراءات اعتراض المراسلات، تسجيل المحادثات، واستخدام الوسائل التقنية لجمع الأدلة الرقمية، مع فرض الرقابة القضائية والتوثيق القانوني لكل خطوة. هذه المستجدات التشريعية تعكس إدراك المشرع لأهمية تكييف القانون مع طبيعة الجرائم الرقمية، بما يحقق التوازن بين الفاعلية القضائية وحماية حقوق الأفراد[3].

ووفقا للقانون السابق ذكره والقانون 09-04المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها فإننا سنخصص هذا المبحث لما يلي: (المطلب الأول) خصوصية الإثبات في جريمة القرصنة الإلكترونية، (المطلب الثاني) حجية الدليل الرقمي وشروط قبوله.

المطلب الأول: خصوصية الإثبات في جرائم القرصنة الإلكترونية

إن الإثبات هو الأداة التي يستعين بها القاضي لتكوين اقتناعه والفصل في النزاعات المعروضة عليه تحقيقاً للعدالة، فالقواعد التي تنظّم الإثبات لا تهدف فقط إلى عرض الوقائع، بل تسعى أساساً إلى كشف الحقيقة التي تتجسد في النهاية في الحكم القضائي. ومن ثم، فإن الحق الذي لا يجد سبيلا إلى الإثبات يظل عديم الأثر، إذ أن قوة الحق لا تقوم إلا بالدليل الذي يسنده[4].

وتتخذ وسائل الإثبات أهمية بالغة، لأن فعاليتها هي التي تحدد مدى إمكانية الوصول إلى الحقوق، كما أن الأسلوب الذي يعتمده المشرع في تنظيم هذه الوسائل يؤثر مباشرة في تحقيق التوازن بين حماية

[1] أمير فرج يوسف، **البلطجة الإلكترونية**، مرجع سابق، ص 151.
[2] أمير فرج يوسف، **العالم ما وراء التقليدي ميتافيرس**، مرجع سابق، ص 161.
[3] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، مرجع سابق، ص 253
[4] سيد علي السيد محمد، **مرجع سابق**، ص 77

الحقوق وضمان استقرار المعاملات، فإذا كان هذا الأسلوب سليما، سهل على الأفراد الوصول إلى حقوقهم، أما إذا كان معيبا، فإنه قد يشكل عائقا يحول دون ذلك.

وكون الجرائم الإلكترونية، من الجرائم المعقدة وصعبة الاكتشاف فإن هذا المفهوم يتراجع بشكل واضح، إذ لا تخلف الجريمة في الغالب آثاراً مادية مباشرة، بل تترك بصمات رقمية يصعب اكتشافها أو تفسيرها دون وسائل تقنية متخصصة[1].

ويضاف إلى ذلك عامل الزمن، حيث قد تمرّ فترة طويلة بين ارتكاب الجريمة واكتشافها، مما يمنح الجاني فرصة لمحو أو إخفاء الآثار الرقمية. كما أن نقص الخبرة الفنية لدى جهات الضبط القضائي والادعاء، وأحياناً حتى لدى القضاء، يُعد من أبرز التحديات التي تعيق عملية الإثبات في هذا النوع من الجرائم [2].

الفرع الأول: مفهوم الإثبات الجزائي

يقصد بالإثبات في الجريمة إقامة الدليل على وقوع الجريمة ونسبته إلى المتهم بارتكاب الفعل الإجرامي[3].

أولا: مفهوم الاثبات الجزائي في اللغة

من الفعل "ثبت"، وتدل على المعرفة والدوام والاستقرار، والمصدر ثبات وثبوت وثبت، وأثبت حجته بمعنى أنه أقامها والإثبات في اللغة هو: إقامة الحجة على أمر ما.[4]

ثانيا: مفهوم الاثبات الجزائي اصطلاحا

تداول الفقهاء استعمال مصطلح الإثبات بمعناه اللغوي، والذي هو إقامة الحجة غير أنه يؤخذ من استعمالاتهم أنهم يطلقونه على معنى عام ومعنى خاص، فالمعنى العام يقصد به إقامة الحجة مطلقا سواء كان ذلك حق أو كان على واقعة، وإن كان أمام القاضي أم غيره، وسواء كان عند التنازع أم قبله، حتى أطلقوه على توثيق الحق وتأكيده عند إنشاء الحقوق والديون، وبمعناه الخاص فيُقصد به إقامة الحجة أمام القضاء بالطرق التي حددتها الشريعة على حق أو واقعة تترتب عليها آثار شرعية.

---

[1] **نفس المرجع**، ص 76-77.

[2] خالد حسن أحمد لطفي، **مرجع سابق**، ص 147.

[3] جميل عبد الباقي الصغير، **دراسة مقارنة، دار النهضة العربية**، القاهرة، 2011، ص 11.

[4] الجوهري، إسماعيل بن حماد-الصحاح-تاج **اللغة العربية**، الجزء الأول، الطبعة الرابعة،1990، ص 245.

ثالثا: مفهوم الإثبات قانونيا

يقصد بالإثبات في المجال القانوني إقامة الدليل أمام القاضي بالطرق التي يحددها القانون، بهدف تأكيد وجود واقعة قانونية ترتبت عنها أثار معينة[1]، أما وسائل الإثبات فهي الأدوات التي يعتمدها الخصوم لإقناع القاضي بصحة ما يدعونه من حقوق أو وقائع، وفي الإطار الشرعي يفهم الإثبات على أنه تقديم الحجة لإثبات حق أو واقعة يترتب عليها أثر معتبر، بما يؤدي إلى إقناع القاضي بصحة الادعاء[2]، ومنه فان الإثبات هو عملية قانونية تهدف إلى إظهار الحقيقة أمام القضاء، من خلال تقديم أدلة مشروعة تؤكد صحة الوقائع المدعى بها.

الفرع الثاني: خصائص الإثبات في الجرائم المعلوماتية

من أبرز خصائص الإثبات في الجرائم المعلوماتية أنه إثبات تقني يعتمد بدرجة كبيرة على وسائل علمية حديثة، كبرمجيات التحليل الجنائي الرقمي، مما يتطلب الاستعانة بخبراء مختصين لفهمه وتفسيره، كما يتسم هذا الإثبات بسهولة التغيير أو الإتلاف، وهو ما يحتم ضرورة التدخل السريع لضبط الأدلة قبا ضياعها أو التلاعب بها

وعليه فان الإثبات يتميز بجملة من الخصائص نتطرق إليها فيمايلي:

أولا: الطابع القضائي للإثبات

يقصد بالإثبات في معناه العام أنه إثبات ذو طبيعة قضائية، أي لا يتحقق إلا أمام جهة قضائية مختصة، سواء تعلق الأمر بقضاء الدولة أو بهيئات التحكيم التي يختارها الخصوم في الحالات التي يجيز فيها القانون ذلك. ويعد هذا الطابع القضائي من أهم خصائص الإثبات، إذ لا تكتسب الوقائع حجيتها القانونية إلا إذا عرضت على القضاء وثبتت أمامه وفق الإجراءات المقررة. [3]

ثانيا: مبدأ تقيد الإثبات بضوابط قانونية

كما يتميز الإثبات بكونه إثباتًا مقيدًا، حيث يخضع لجملة من القواعد القانونية التي تحدد وسائل الإثبات المقبولة، وتضع لكل وسيلة شروطًا وضوابط معينة يتعين احترامها، ويشكل هذا التقييد ضمانة لتحقيق التوازن بين مصلحة الأطراف ومتطلبات العدالة، ويحول دون التعسف في استعمال وسائل الإثبات.

---

[1] خالد حسن أحمد لطفي، **جرائم الإنترنت**، مرجع سابق، ص 146.

[2] سيد علي السيد محمد، **مرجع سابق**، ص 86.

[3] خالد حسن أحمد لطفي، جرائم الإنترنت، **نفس المرجع**، ص 147.

ثالثا: حجية الأمر المقضي

ومن خصائص الإثبات أيضًا أنه يهدف إلى إقرار الحقيقة القضائية، وهي الحقيقة التي يتوصل إليها القاضي بناء على ما يعرض عليه من أدلة، فتكتسب حجية ملزمة ولو لم تتطابق تمامًا مع الحقيقة الواقعية. وبالمقابل، فإن الوقائع التي لا تُثبت أمام القضاء تبقى مجرد ادعاءات قابلة للنقاش والإثبات بوسائل أخرى.

رابعا: مبدأ حرية الإثبات في المواد الجزائية

أما في المجال الجزائي، فإن الإثبات يتميز بخصوصية أساسية تتمثل في مبدأ حرية الإثبات، حيث يجوز إثبات الجريمة بكافة الطرق، دون التقيد بوسائل محددة، وذلك سعيًا للوصول إلى اليقين القضائي وفق معيار الحقيقة الواقعية. غير أن هذه الحرية ليست مطلقة، بل تقيد بضرورة مشروعية الوسيلة المستعملة، احترامًا لمبدأ الشرعية الإجرائية وضمانات حقوق الإنسان[1].

الفرع الثالث: الصعوبات التي تواجه جريمة القرصنة الإلكترونية في الإثبات

إن صعوبات الإثبات في جريمة القرصنة الإلكترونية لا ترتبط فقط بطبيعة الدليل الرقمي، بل تمتد لتشمل الجوانب التقنية والقانونية والدولية، ويرجع السبب في ذلك كونها تعود إلى عدة عوامل مترابطة يمكن تقسيمها على النحو الآتي:

أولا: صعوبات مرتبطة بطبيعة الجريمة نفسها

تتميز جريمة القرصنة بإمكانية ارتكابها عن بعد، وباستعمال وسائل تقنية متطورة تسمح بإخفاء الهوية أو تغييرها، بالإضافة إلى سهولة محو الآثار الرقمية أو تعديلها، مما يجعل الدليل الإلكتروني سريع الزوال وصعب التتبع.[2]

ثانيا: صعوبات الاثبات تواجه جهات التحقيق الابتدائي

تواجه السلطات المختصة تحديات تقنية وقانونية أثناء البحث والتحري، من بينها الحاجة إلى خبرة تقنية متخصصة لفهم الأدلة الرقمية وتحليلها، إضافة إلى صعوبة الوصول إلى كثير من حالات القرصنة لا يتم

[1] خالد حسن لطفي، **نفس المرجع**، ص 150.

[2] عبد الكريم أبو الفتوح درويش، **الإدارة الاستراتيجية لمكافحة الجرائم المستحدثة**، أكاديمية شرطة دبي، الإمارات العربية المتحدة، 2003، ص 64.

الإبلاغ عنها، إما بسبب جهل الضحايا أو خشيتهم على سمعتهم أو خسائرهم، مما يؤدي إلى ارتفاع نسبة الجرائم غير المكتشفة، ويضعف من فعالية الردع الجنائي. [1]

ثالثًا: صعوبات ذات بعد قانوني ودولي

كون البيانات المخزنة في أنظمة محمية أو موزعة عبر خوادم متعددة، قد تكون خارج الإقليم الوطني، فتتسم بطابع عابر للحدود، حيث قد يقع الفعل في دولة، وتخزن البيانات في دولة أخرى، ويكون الجاني في دولة ثالثة، مما يخلق إشكاليات تتعلق بالاختصاص القضائي والتعاون الدولي، ويؤثر على فعالية إنفاذ القانون.

رابعا: ضعف الإبلاغ وصعوبة المتابعة

بالنظر إلى طبيعة جريمة القرصنة الإلكترونية التي تتميز بالتعقيد وصعوبة الاكتشاف أو استحالة ذلك كليا يجعل من التبليغ عن هذه الجريمة صعب بل وقد يرفض أغلب الضحايا ذلك بالرغم من أن الدعوى العمومية في مثل هذا النوع من الجرائم تحرك اما من طرف النيابة العامة ممثلة الحق العام او من طرف الأشخاص الضحايا المتضررين سواء كانوا موظفين أو ضباط عموميون[2]، كما انه توجد حالات يكون فيها التبليغ عن الجريمة واقعا على عاتق كل من علم بوقوع الجريمة وهو ما نصت عليه المواد 31 من قانون العقوبات الجزائري[3].

وفي إطار جرائم القرصنة الإلكترونية، يكتسب الإثبات طابعا تقنيا مميزا، إذ يعتمد على وسائل علمية وفنية متطورة في جمع الأدلة وتحليلها، مثل التفتيش الإلكتروني الذي تم التطرق إليه سابقا، واستخراج البيانات، وتحليل الأنظمة المعلوماتية، بالإضافة الى الدليل الرقمي الذي يعتبر من أهم وسائل الإثبات في هذا المجال، نظرًا لخصوصيته المتمثلة في كونه غير مادي، سريع الزوال، وقابل للتلاعب، مما يفرض

---

[1] نعيم سعيداني، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة مقدمة لنيل شهادة الماجستير، في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة لخضر، باتنة، الجزائر 2012-2013، ص43.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المجلة الكبرى، مصر، 2002، ص 84

[3] فيصل بدري، **مرجع سابق**، ص 236

قانون العقوبات الجزائري المادة 31 منه تنص على " مع عدم الإخلال بالواجبات التي يفرضها سر المهنة يعاقب بالسجن المؤقت لمدة لا تقل عن 10 سنوات ولا تتجاوز 20 سنة في وقت الحرب وبالحبس من 5 سنوات وغرامة مالية من 3 ألاف إلى 30 ألف دج في قت السلم لكل شخص علم بوجود خطط أو أفعال لارتكاب جرائم الخيانة أو التجسس أو غيرها من النشاطات التي يكن من طبيعتها الإضرار بالدفاع الوطني ولم يبلغ عنها السلطات العسكرية أو الإدارية أو القضائية فور علمه بها"

التعامل معه وفق قواعد تقنية وقانونية دقيقة، ويجعله يحتل مكانة محورية في إثبات جرائم الإنترنت بصفة عامة وجرائم القرصنة الإلكترونية بصفة خاصة وهو ما سوف نعرضه من خلال المطلب التالي.

المطلب الثاني: خصوصية الدليل الرقمي كوسيلة إثبات

لقد أدى ظهور الجريمة الإلكترونية كنمط جديد من الإجرام له خصوصيته التقنية والمعقدة إلى إسراع المشرعين في مختلف الدول إلى مواكبة هذا التطور من خلال سن قواعد قانونية جديدة أو تعديل تلك التي لم تعد تستجيب من الناحية الموضوعية أو الإجرائية لمكافحة الظاهرة الإجرامية[1]، ومن أحدث مستجدات الإثبات في العصر الحديث، الدليل الرقمي الذي يعتبر وسيلة أساسية في الإثبات فيشمل كل البيانات أو المعلومات ذات الطابع الرقمي التي يمكن استخراجها من الأجهزة أو الأنظمة المعلوماتية وتقديمها أمام القضاء لإثبات واقعة معينة، فيتميز هذا الدليل بكونه غير ملموس، وقابل للنسخ والتعديل[2]، مما يثير إشكالات تتعلق بمدى مصداقيته وسلامته من التلاعب، وبالرغم من هذه الخصائص، فقد أصبح الدليل الرقمي يحتل مكانة مهمة في الإثبات الجنائي، خاصة في جرائم القرصنة الإلكترونية، كونه يعكس النشاط الإجرامي في بيئته[3].

في هذا الفرع نفصل في إعطاء مفهوم الدليل الالكتروني وحجته في الإثبات.

الفرع الأول: مفهوم الدليل الرقمي

تحظى نظرية الإثبات باهتمام بالغ من طرف الفقه على الصعيد المدني والجنائي وإن كان في المسائل المدنية تبدو قيمة الإثبات واضحة وجلية خاصة إذا كان من المستقر أن موضع التقاضي يشترط أن يتجرد من كل قيمة إذا لم يقم الدليل على الحادث الذي يستند إليه، وأن الدليل وحده الذي يحيي الحق ويجعله مفيدا.[4]

أولا: الدليل في اللغة

الدليل ما يستدل به، وهو مفرد جمعه أدلة ودلائل، وهو البينة، والحجة، والبرهان، والشاهد، والعلامة، يقال: أقام الدليل على براءته، وقال تعالى: " **ثم جعلنا الشمس عليكم دليلا**" الفرقان 45. والدليل أيضا ما

[1] القانون رقم 25-14 المؤرخ في 3 غشت 2025.

[2] ايت حمودة كهينة، **مرجع سابق**، ص 5.

[3] أمير فرج يسف، البلطجة الإلكترونية، مرجع سابق، ص 168.

[4] عبد الرحمان خلفي، **مرجع سابق**، ص 542.

يعبر عن شيء أو يثبت وجود شيء آخر مرتبط به، فالدليل هو المرشد وهو الناصب والذاكر وما به الإرشاد، والدليل عند الأطباء هو العلامة التي يهتدي بها الطبيب إلى المرض. [1]

ثانيا: التعريف الاصطلاحي للدليل الإلكتروني

يقصد بالدليل الإلكتروني ذلك النوع من الأدلة المستمدة من البيئة الرقمية، والذي ارتبط ظهوره بالتطور التكنولوجي المتسارع في مجال تكنولوجيات الإعلام والاتصال. ومن الناحية اللغوية، يُشتق مصطلح "الإلكتروني" من لفظ "إلكترون"، ويُستعمل لوصف كل ما هو مرتبط بالمجال الإلكتروني، كالحاسب الإلكتروني، والبرمجيات، والبطاقات الإلكترونية، والبريد الإلكتروني، والفضاء الرقمي، وغيرها من التطبيقات التي تعتمد على المعالجة الآلية للمعطيات[2].

وقد تعددت تعريفات الدليل الإلكتروني واختلفت باختلاف الزاوية التي يُنظر منها إليه، حيث اتجه بعض الفقه إلى التوسع في مفهومه ليشمل كل المعطيات الرقمية، في حين ذهب اتجاه آخر إلى تضييقه ليقتصر على ما يصلح منها للإثبات في المجال القضائي. كما يُستعمل أحيانًا مصطلح "**الدليل الرقمي**" كمترادف له، نظرا لارتباطه بالبيانات التي تُعالج وتُخزن في شكل رقمي.

وفي المجال الجنائي، يعرف الدليل الإلكتروني بأنه مجموعة المعطيات أو المعلومات التي يتم تخزينها أو نقلها أو معالجتها بوسائل إلكترونية، والتي يمكن الاعتماد عليها في الكشف عن الجريمة وإثبات وقوعها أو نسبتها إلى مرتكبها. ويتميز هذا النوع من الأدلة بخصائص فنية خاصة، من بينها قابليته للتغيير أو الإتلاف بسهولة، واعتماده على وسائط تقنية، مما يفرض ضرورة التعامل معه وفق ضوابط إجرائية دقيقة تضمن سلامته وحجيته في الإثبات[3].

وعليه، فإن الدليل الإلكتروني يعد اليوم من أهم وسائل الإثبات الحديثة في القضايا الجنائية، خاصة في الجرائم المستحدثة المرتبطة بالبيئة الرقمية، الأمر الذي يستدعي تطوير الإطار القانوني والتقني لضمان فعاليته دون المساس بالضمانات الأساسية للمحاكمة العادلة.

---

[1] خالد ضو، **حجية الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي، مجلة الأبحاث الأكاديمية في العلم القانونية والسياسية، المجلد 05، العدد01، 23-03-2022، ص 202.**

[2] أحمد مختار عمر وآخرون، **معجم اللغة العربية المعاصرة**، عالم الكتب، القاهرة، الطبعة الأولى، ج، 1، ص 764

[3] خالد ضو، **مرجع سابق**، ص 203.

الفرع الثاني: أنواع الدليل الرقمي

تتغير أدلة الإثبات في الجرائم الالكترونية عن الأدلة التقليدية المعروفة قديما والتي تبين كيفية كشف الجريمة والملابسات المحيطة بها، والتي تعتبر أدلة بسيطة مقارنة بالأدلة الحديثة التي تتعلق بموضوع الجريمة الالكترونية وهو ما يطلق عليه بالأدلة الرقمية والالكترونية.[1] وتتصل هذه الأدلة مباشرة بالكومبيوتر فتكون في صورة مجالات أو نبضات مغناطيسية أو كهربائية.

كما لأن هذه الأدلة أنواع مختلفة نذكرها:[2]

أولا: أدلة أُعدت لتكون وسيلة إثبات (أدلة رقمية مباشرة)

يمكن إجمال هذا النوع من الأدلة فيما يلي:

التسجيلات التي تم إنشاؤها بواسطة الآلة تلقائيا، وتعد هذه السجلات من مخرجات الآلة والتي ليس للإنسان دخل في إنشاءها مثال ذلك السجلات الموجودة في الهاتف وفواتير التابعة لأجهزة الحاسب الآلي.

السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الأدلة ومن أمثلتها: البيانات التي يتم إدخالها إلى الآلة وتتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

ثانيا: أدلة لم تعد لتكون وسيلة إثبات (أدلة رقمية غير مباشرة):

ينشأ هذا النوع من الأدلة دون إرادة الشخص، أي هي عبارة عن أثر يتركه الجاني دون أن يكون راغبا في تركه ويسمى هذا النوع من الأدلة بالبصمة الرقمية[3]، وهي ما يمكن تسميته أيضا بالآثار المعلوماتية الرقمية والتي تتجسد في الآثار إلي يرتكبها مستخدم الشبكة المعلوماتية نتيجة تسجيل الرسائل منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات[4].

الفرع الثالث: خصائص الدليل الرقمي

يعد الدليل الرقمي دليلاً غير ملموس، إذ لا يتمتع بوجود مادي محسوس كالأدلة التقليدية، بل يتمثل في بيانات ومعطيات ذات طبيعة إلكترونية. وعليه، فإن إخراج هذا الدليل في شكل مادي (كالطباعة أو النسخ) لا يُغير من طبيعته، وإنما يُعد مجرد وسيلة لعرضه وتمكين الجهات المختصة من الاطلاع عليه. وينتمي الدليل الرقمي إلى طائفة الأدلة الفنية أو العلمية، كونه مستمداً من أنظمة المعالجة الآلية، ولا يمكن فهم مضمونه أو الاستفادة منه إلا باستخدام وسائل تقنية متخصصة لتحليله واستخلاص المعلومات منه.

---

[1] حسين طاهري، **مرجع سابق**، ص253.

[2] خالد حسن أحمد لطفي، **مرجع سابق**، ص 153.

[3] كهينة ايت حمودة، **مرجع سابق**، ص 6.

[4] حسين طاهري، **نفس المرجع**، ص 295.

لذلك، فإن أي معطى رقمي لا يمكن تحليله أو تفسيره بواسطة هذه الوسائل، يفقد قيمته كدليل، لعدم صلاحيته للاستدلال على واقعة معينة أو نسبتها إلى الجاني[1]. ومن خصائصه:

أولا: الدليل الرقمي قابل للتغيير أو الإتلاف

يتسم الدليل الرقمي بكونه سريع التأثر، إذ يمكن تعديله بسهولة وبوسائل تقنية بسيطة، دون أن يترك في بعض الحالات أثرا ظاهرا، وهو ما يفرض ضرورة اتخاذ تدابير تقنية وقانونية صارمة أثناء جمعه وحفظه أو حذفه في لحظات أو إخفائه أو تشفيره.

ثانيا: الدليل الرقمي دليل عابر للحدود

لا يرتبط الدليل الرقمي بمكان جغرافي محدد، إذ يمكن تخزينه في دولة ومعالجته في دولة أخرى وارتكاب الجريمة من دولة ثالثة وهو ما يطرح مشكل الاختصاص القضائي والتعاون الدولي

ثالثا: الدليل الرقمي يعتمد على الخبرة التقنية

منذ بروز الجرائم الإلكترونية المرتبطة بأنظمة الحاسب الآلي، أصبح اللجوء إلى الخبرة الفنية ضرورة أساسية في مراحل التحقيق والمحاكمة، فلا يمكن فهم الدليل الرقمي بالعين المجردة، بل يحتاج إلى خبراء مختصين، إضافة إلى برامج تحليل وأجهزة تقنية مثل تحليل قرص أو استرجاع بيانات محذوفة يتطلب أدوات خاصة[2].

ويستعين القاضي أو المحقق بالخبراء المختصين في مجال المعلوماتية بهدف كشف غموض الجريمة، وجمع الأدلة الرقمية، والحفاظ عليها من الضياع أو التلف، إضافة إلى المساعدة في فهم الجوانب التقنية المعقدة المرتبطة بالفعل الإجرامي.

وتكمن أهمية الخبرة بشكل خاص في الحالات التي تعجز فيها أجهزة الضبط أو التحقيق عن التعامل مع الطبيعة التقنية للجريمة، سواء بسبب نقص التكوين أو بسبب حساسية الأدلة الرقمية وسهولة إتلافها أو تعديلها دون ترك أثر واضح، لذلك فإن تدخل الخبير يصبح وسيلة ضرورية لضمان سلامة إجراءات البحث والتحقيق[3].

ولا يشترط في الخبير أن يكون مجرد صاحب شهادة علمية في الإعلام الآلي، بل ينبغي أن يمتلك كذلك خبرة عملية طويلة في المجال، تمكّنه من الإلمام بتفاصيل الأنظمة والبرمجيات وأساليب عملها.

---

[1] خالد حسن أحمد لطفي، **جرائم الإنترنت**، مرجع سابق، ص 152.

[2] أمير فرج يوسف، **البلطجة الإلكترونية**، مرجع سابق، ص 143.

[3] خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة والنشر والتوزيع، عمان، 2011.

فالتخصص في هذا المجال يشمل، على سبيل المثال، تحليل البرمجيات وأنظمة التشغيل، فهم لغات البرمجة، متابعة التطورات التقنية الحديثة، والقدرة على كشف محاولات الاختراق أو التلاعب بالبيانات. كما أن الجرائم المعلوماتية قد تتخذ صوراً متعددة، مثل التزوير الإلكتروني للمستندات، التلاعب بالبيانات أثناء النقل أو التخزين، جرائم الاعتداء على الأموال عبر الوسائط الإلكترونية، أو انتهاك الحياة الخاصة من خلال نشر صور أو فيديوهات غير قانونية. وهنا يبرز دور الخبير في تفسير هذه الوقائع التقنية وربطها بالجانب القانوني للجريمة.

ويطلق على هذا النوع من الخبراء اسم الخبير الرقمي أو الخبير المعلوماتي الجنائي، ويمكن تعريفه بأنه الشخص الذي تعمّق في دراسة الأنظمة الإلكترونية وتخصص في العمل عليها مدة زمنية طويلة، مما أكسبه خبرة عملية دقيقة، جعلته قادراً على تقديم رأي فني متخصص في القضايا ذات الطابع الرقمي، يتجاوز ما يمكن للشخص العادي إدراكه[1].

ومن أجل أداء مهامه بكفاءة، ينبغي أن تتوفر لدى الخبير مجموعة من المعارف، من أهمها: الإلمام بأنظمة التشغيل، معرفة لغات البرمجة، فهم آليات تصميم وتشغيل البرامج، والقدرة على تحليل الأنظمة وكشف الثغرات الأمنية. كما يفترض أن يكون مدركاً لاحتمال وجود أطراف قادرة على اختراق الأنظمة، مما يساعده في تفسير طبيعة بعض الأفعال الإجرامية.

كما يستحسن تعزيز التنسيق بين الخبير المعلوماتي والمحقق الجنائي قبل وأثناء سير التحقيق، بحيث يشمل هذا التعاون مختلف مراحل القضية، من تلقي البلاغ إلى إجراءات التفتيش الرقمي وجمع الأدلة[2]. ويهدف هذا التنسيق إلى ضمان جمع الأدلة بطريقة علمية منظمة، وترتيبها حسب أهميتها، مع الحفاظ على سلامتها وسلسلة حيازتها القانونية.

وفي المقابل، يقع على عاتق المحقق الجنائي توضيح الإطار القانوني لعمل الخبير، وربط ما يتم التوصل إليه من نتائج تقنية بعناصر وأركان الجريمة محل المتابعة، بما يسمح للقضاء بتكوين قناعة سليمة قائمة على تداخل الجانب الفني مع الجانب القانوني.

الفرع الرابع: الوسائل التقنية المستحدثة لجمع الدليل الرقمي

لا يقتصر إثبات الجرائم المعلوماتية على وجود الدليل الرقمي في حد ذاته، بل يتطلب كذلك وسائل تقنية فعالة تمكن من جمع هذا الدليل واستخراجه من بيئته الرقمية. وفي هذا الإطار، تلعب إجراءات مثل

[1] أمير فرج يوسف، **البلطجة الإلكترونية**، مرجع سابق، ص144.

[2] خالد ممدوح البحر، **حماية الحياة الخاصة في القانون الجنائي (دراسة مقارنة)**، دار النهضة العربية، القاهرة، 1983.

اعتراض المراسلات وتسجيل الأصوات والصور والتسرب الإلكتروني دوراً محورياً، باعتبارها آليات حديثة تتيح الوصول إلى الأدلة الرقمية. غير أن هذه الوسائل لا تُعدّ أدلة قائمة بذاتها، وإنما تشكل طرقاً إجرائية للحصول على الدليل، الذي يبقى خاضعاً في النهاية لتقدير القاضي من حيث حجيته وقيمته الإثباتية.[1]

وقد جاء في نص المادة 349 أنه "**يجوز إثبات الجرائم بأي طريق من طرق الإثبات، بما فيها الإلكترونية، ما عدا الأحوال التي ينص فيها القانون على غير ذلك....**"

كما نص المشرع بموجب القانون 25-14 من خلال المواد من **114 إلى 127** على انه متى استلزمت ضرورات البحث والتحقيق في الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال يجوز لقاضي التحقيق اللجوء إلى بعض أساليب التحري الخاصة فتشمل اعتراض المراسلات الإلكترونية، وتسجيل الأصوات، واعتماد تقنية التسرب الإلكتروني، ذلك بهدف جمع الأدلة وتعقب النشاط الإجرامي المرتبط بالأنظمة والشبكات المعلوماتية[2]، هذه إجراءات أخرى تضمنها القانون رقم 09-04المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والمتمثلة في مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية[3].

أولا: التسرب

يعد التسرب من أساليب التحري الخاصة التي أقرّها المشرّع الجزائري بموجب المواد من 120 إلى **127 من قانون الإجراءات الجزائية**[4]، وعرفت المادة **121 فقرة 1** منه التسرب على انه قيام ضابط أو عون الشرطة القضائية، تحت إشراف ومسؤولية ضابط الشرطة القضائية المكلّف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة، من خلال الاندماج في نشاطهم الإجرامي بإيهامهم بأنه فاعل معهم أو شريك لهم[5].

---

[1] المادة 349 من **قانون الإجراءات الجزائية الجزائري الجديد رقم 14/25**

[2] محمد حزيط، **مرجع سابق**، ص 350.

[3] حليم رامي، **استخلاص الدليل في الجرائم المعلوماتية، دفاتر البحوث العلمية**، المجلد 09، العدد 01، 2021، ص 233. أخذ المشرع الجزائري عند استحداث إجراءات تحري خاصة بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية 06-22 قبل التعديل الأخير، ولأول مرة في قانون الإجراءات الجزائية سنة 2006، حيث أجاز لضباط الشرطة القضائية اللجوء إلى أساليب جديدة للتحري والتحقيق تتمثل أساسا في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب بإذن من وكيل الجمهورية في مرحلة التحقيق الأولى وبإذن من قاضي التحقيق في مرحلة التحقيق القضائي لمواجهة أنواع معينة من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وغيرها من الجرائم .

[4] **المواد 120 إلى 127 من قانون الإجراءات الجزائية الجزائري.**

[5] المادة 121 فقرة 1 من نفس القانون "**التسرب** هو قيام ضابط أو عون الشرطة القضائية ، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف" فيسمح هذا الاجراء لضباط أو عون الشرطة بمقتضى الفقرة 2 من المادة 121 أن يستعمل لهذا الغرض، هوية

ولغرض إنجاح عملية التسرب، أجاز المشرع، بموجب المادة **121 فقرة 2**، لضابط أو عون الشرطة القضائية استعمال هوية مستعارة، والقيام، عند الضرورة[1]، ببعض الأفعال المرتبطة بالنشاط الإجرامي، كاقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصّل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها، وكذا وضع الوسائل ذات الطابع القانوني أو المالي، ووسائل النقل أو التخزين أو الإيداع أو الحفظ أو الاتصال، تحت تصرف مرتكبي الجرائم.غير أنه، وطبقًا لأحكام المادة **125 فقرة 3 من ق.إ.ج.ج** ، يُحظر تحت طائلة البطلان أن تنطوي هذه الأفعال على أي شكل من أشكال التحريض على ارتكاب الجرائم، بحيث يجب أن يقتصر دور ضابط أو عون الشرطة القضائية على الملاحظة والمساهمة السلبية دون دفع أو خلق السلوك الإجرامي[2].

أ- التسرب الإلكتروني:

في مجال الجرائم المعلوماتية، فيتخذ التسرب صورة حديثة تُعرف بالتسرب الرقمي، والذي يتمثل في دخول ضابط أو عون الشرطة القضائية إلى الأنظمة المعلوماتية أو الفضاءات الرقمية بصفة متخفية، باستعمال هويات أو صفات وهمية، بهدف الاندماج داخل المجموعات الإجرامية الإلكترونية، ورصد نشاط المشتبه فيهم، وجمع الأدلة الرقمية المتعلقة بارتكابهم أو شروعهم في ارتكاب الجرائم.

التسرب الإلكتروني في اللغة مشتق من فعل تسرب، أي دخل وانتقل خفية وتوغل،[3] أما في المفهوم الاصطلاحي فيقصد به ذلك التصرف الذي يقوم به ضابط الشرطة القضائية بالتسلل إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر قصد مراقبة الأشخاص المشتبه في ارتكابهم لبعض الجرائم المحددة قانونا، والتواصل معهم عن طريق القيام ببعض الأعمال قصد الحصول على أدلة ضدهم.

ونشير هنا أنه ذات المعنى الذي أشار إليه المشرع الجزائري في المادة 26 من قانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية، حيث تنص على ما يلي: "**مع مراعاة أحكام قانون الإجراءات الجزائية يمكن لوكيل الجمهورية أو قاضي التحقيق، أن يأذن، تحت رقابته، لضابط الشرطة القضائية**

مستعارة وأن يرتكب عند الضرورة دون أن يكون مسؤولا جزئيا أو تشكل تحرضا على ارتكاب جرائم الأفعال المنصوص عليها في المادة 123 من نفس القانون كما يجوز طبقا لنص المادة 127 سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية

[1] حسين طاهري، الجرائم الإلكترونية، **مرجع سابق**، ص 420.

[2] حليم رامي، **نفس المرجع**، ص 234.

[3] المنجد الأبجدي، **المطبعة الكاثوليكية**، دارا لمشرق، بيروت لبنان، 1967.

بالتسرب الإلكتروني إلى منظومة معلوماتية أو أكثر قصد مراقبة الأشخاص المشتبه في ارتكابهم لأية جريمة من الجرائم المنصوص عليها في هذا القانون، وذلك بإيهامهم أنه فاعل معهم أو شريك لهم..."، وهو ما ورد حرفيا في المادة 16 من قانون رقم 20-15 المتعلق بالوقاية من اختطاف الأشخاص ومكافحتها[1].

من الجانب الفقهي فقد أُطلقت العديد من التسميات على هذه العملية منها التسرب الالكتروني أو التسرب الرقمي، الدوريات السيبيرانية أو الافتراضية، التحقيق والتحري تحت اسم مستعار عبر الانترنت وغيرها ، ويتضح من خلال مختلف التعريفات أن التسرب هو أسلوب من أساليب التحري الخاصة التي تهدف إلى مراقبة الأشخاص المشتبه فيهم وكشف أنشطتهم الإجرامية، فهو إجراء يتطلب قدرا كبيرا من الحذر والدقة والكفاءة أثناء تنفيذه، فتدخل التشريع الجزائري وأقر تنظيما قانونيا له من خلال التعديلات التي شملت التسريب الإلكتروني باعتباره وسيلة مستحدثة تتلاءم مع طبيعة الجرائم الرقمية[2].

ب: شروط اللجوء إلى التسرب

بالرجوع إلى نص المادة **120 من قانون الإجراءات الجزائية** التي تحدد الشروط الواجب توفرها من أجل اللجوء إلى التسرب في مجال القرصنة الإلكترونية هو:

1_أن تكون الجريمة التي يجري فيها التحقيق من بين الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

2_ يشترط أن يأذن قاضي التحقيق بمباشرة عملية التسرب التي تتم تحت رقابته بعد إخطار وكيل الجمهورية[3]

3_يجب أن يكون الإذن المسلم مكتوبا ومسببا وهذا تحت طائلة البطلان بموجب المادة **124 من نفس القانون**، بحيث يتضمن نوع الجريمة التي تستوجب القيام بهذا الإجراء.

4_ تحديد هوية ضابط الشرطة القضائية المكلف بعملية التسرب وتحديد مدة التسرب التي لا يمكن أن تتجاوز 04 أشهر قابلة للتجديد حسب مقتضيات التحقيق ويمكن بموجب طلب موجه الى قاضي التحقيق تمديد المهلة في حال انقضائها دون تمكن العون المكلف من إنهاء مهامه أين يرخص القاضي بالتمديد

---

[1] كريمة تاجر، **التسرب الالكتروني كآلية لمكافحة الجريمة الالكترونية (دراسة مقارنة بين القانون الجزائري والفرنسي)**، المجلة النقدية للقانون والعلوم السياسية، المجلد 19، العدد 02، 2024، ص479.

[2] عبد الرحمان خليفي، **مرجع سابق**، ص 135.

[3] محمد حزيط، **مرجع سابق**، ص 352.

لمدة 04 أشهر على الأكثر كما له أن يأمر في أي وقت بوقف عملية التسرب حتى قبل انتهاء المهلة المحددة وهذا طبقا للمادة 124 من نفس القانون.

5_ إيداع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب [1].

6_ لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب في أي مرحلة من مراحل الإجراءات طبقا لنص المادة **125 ق.إ.ج.ج**[2]

يتضح جليا من خلال تحليل نص المواد السالفة الذكر أن استحداث المشرع الجزائري للتسرب الإلكتروني كآلية من آليات البحث والتحري والمتابعة في الجريمة الإلكترونية تعكس التحول العميق في السياسة الجنائية الحديثة، غير أن هذا التحول يقابله خطر المساس بالخصوصية الرقمية واتساع نطاق المراقبة الإلكترونية، مما قد يؤدي إلى المساس بالحقوق الأساسية والشخصية فلابد من ضرورة إخضاع هذا الإجراء إلى رقابة قضائية خاصة ضمانا لمشروعية الدليل.

ثانيا: اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور

بالرجوع للفصل الرابع من الباب الثاني من قانون الإجراءات الجزائية –تعديل سنة 2025– وبقراءة نص المادة **114** التي تنص على: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم القتل العمدي، والمخدرات والمؤثرات العقلية، والجريمة المنظمة عبر الحدود الوطنية، والجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد، وجرائم التهريب، وجرائم الاتجار بالبشر، وجرائم الاتجار بالأعضاء، وجرائم تهريب المهاجرين، وجرائم اختطاف الأشخاص، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

أ_اعتراض المراسلات تتم عن طريق وسائل الاتصال السلكية واللاسلكية،

---

[1] عبد الرحمان خلفي، مرجع سابق، ص 136–137.

[2] **ق.إ.ج.ج المادة 125 منه**" لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات. يعاقب كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين 2 الى خمس 5 سنوات وبغرامة من 200.000 دج إلى 500.000 دج ، إذا تسبب الكشف عن الهية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبناءهم أو أصولهم المباشرين فتكون العقوبة الحبس من 5 سنوات الى 10 سنوات والغرامة من 500.000 دج الى 1000.000 دج وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من 10 سنوات إلى 20 سنة والغرامة من 1.000.000 دج الى 2.000.000.دج دون الإخلال ، عند الاقتضاء، بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات .

ب_وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرّية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص[1]، يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 78 من قانون الإجراءات الجزائية[2]، وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص.

في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة".[3]

نلاحظ من خلال استقراء النص القانوني التوسع الذي يعكس تطور التشريع الجزائري لمواكبة الجرائم الرقمية، حيث أن الاعتراض لا يقتصر على المكالمات الهاتفية، بل يشمل كل أشكال النقل الرقمي للمعطيات عن طريق اعتراض أو تسجيل أو نسخ المراسلات التي تتم عبر وسائل الاتصال، سواء كانت اتصالات هاتفية أو مراسلات عبر الشبكات الرقمية، وذلك بمقتضى ضرورة التحري أو التحقيق الابتدائي في الجرائم المقررة ، وقد تم تناول هذا الطرح و اعتماده في اتفاقية بودبست وتقريرها التفسيري من طرف لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة في 8 نوفمبر 2001 وفتح باب التوقيع على الاتفاقية في بودابيست بتاريخ 23 نوفمبر 2001 بمناسبة المؤتمر الدولي حول الجريمة الالكترونية.[4]

ثالثا: التسجيل الصوتي والمرئي

---

[1] بدري فيصل، **مرجع سابق**، ص 435.

[2] نصت المادة **78 فقرة 3 من ق.إ.ج.ج.** على انه يجوز إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات الليل والنهار في جميع الجرائم المعاقب عليها في المواد 339 إلى 345 من قانون العقوبات، عندما يتعلق الأمر بالجرائم المتصلة بتكنولوجيا الإعلام الاتصال في كل محل سكني أو غير سكني وفي كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مكتوب مسبق من وكيل الجهورية المختص، كما أجاز الشرع لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي اي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك .

[3] مادة 144 مراقبة المحادثات الخاصة والاتصالات السرية للأشخاص باستعمال أجهزة تقنية دقيقة لتسجيل الأصوات للأشخاص والتقاط الصور كزرع الميكروفونات في المساكن أو المكاتب أو المركبات أو غيرها من الأماكن التي يتردد إليها الشخص محل التحري، إضافة إلى استخدام الهواتف المحمولة أو أدوات متطورة قادرة على اختراق السمع والبصر بدرجة عالية من الدقة.

[4] حليم رامي، **المرجع السابق**، ص 235.

وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الانترنت والهاتف.... **الخ**[1]

غير أن هذه الإجراءات، على أهميتها، لا تزال محدودة الفعالية في مواجهة هذا النوع من الجرائم، خاصة في ظل التطور السريع والمتلاحق للتقنيات الحديثة في مجال المعلوماتية، الأمر الذي يفرض ضرورة إعادة النظر فيها وتحيينها بما يتلاءم مع هذه المستجدات، لضمان فعالية أكبر في الكشف عن الجرائم المعلوماتية ومكافحتها.

رابعا: المراقبة الإلكترونية

تقوم المراقبة على السرية والمتابعة المستمرة بغرض جمع الأدلة المرتبطة بالنشاط الإجرامي فهي من الوسائل الأساسية للبحث والتحري، إلا أنها تطورت من صورتها التقليدية إلى صورتها المستحدثة المعروفة ب "**المراقبة الإلكترونية**" في البيئة الافتراضية[2] بما يسمح بتوسيع نطاق البحث والتحري لتعقب المجرم المعلوماتي، نظرًا لطبيعة الجرائم المرتكبة عبر الوسائط الرقمية. وفي هذا الإطار، جاء القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ليضع مجموعة من الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتسجيل محتواها والقيام بإجراءات الحجز داخل منظومة معلوماتية.

أ: المراقبة الإلكترونية والتقاط البيانات الرقمية بإذن قضائي.

اشترطت الفقرة الثانية من المادة 114 من ق إ.ج.ج في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة.[3]

ب: الحالات التي تسمح باللجوء إلى المراقبة الالكترونية:

أكدت المادة 04 من قانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على إمكانية القيام بعمليات المراقبة المنصوص عليها في المادة 03، للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة[4].

---

[1] خالد حسن أحمد لطفي، **جرائم الإنترنت**، 154.

[2] خلفي عبد الرحمان، **مرجع سابق**، ص 132

[3] المادة 114/ 02 قانون 25-14.

[4] المادة **3، 4 من القانون 09-04**

ففي حالة الاعتداء أو توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني على أن تكون طبقا لما تمليه مقتضيات التحري والتحقيق، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وتكون هذه الإجراء بعد صدور إذن مكتوب من السلطة القضائية المختصة[1].

خامسا: الآثار التقنية الناتجة عن الوسائل المستحدثة

تعتبر ملفات الولوج وسجلات النظام من أهم المصادر التقنية، حيث تسجل جميع العمليات التي تتم داخل النظام المعلوماتي، سواء تعلق الأمر بعمليات الدخول أو محاولات الولوج غير المصرح بها أو التفاعل مع الشبكة، وتحتوي هذه السجلات على بيانات دقيقة مثل توقيت النشاط، نوع العملية، والأجهزة أو الخوادم المستعملة، مما يسمح بإعادة بناء الوقائع الرقمية محل التحقيق[2].

يعد هذا الفرع من أهم وسائل الإثبات في الجرائم المعلوماتية، إذ يعتمد على مجموعة من الآثار تتركها الأنشطة داخل الأنظمة والشبكات، وعلى رأسها ملفات الولوج الرقمية التي تتركها الأنشطة عنوان بروتوكول الإنترنت LOGS (IP) ، والبيانات الوصفية (Metadata)[3]

وفي نفس السياق يمثل IPابروتوكول الإنترنت عنصرا محوريا داخل هذه السجلات، فه عنصر تقني فريد لكل جهاز متصل بالشبكة، ويساعد في تتبع مصدر الاتصال وتحديد مساره عبر الشبكة المعلوماتية، غير أن قيمته الإثباتية تبقى نسبية، لكونه قابلا للإخفاء أو التغيير عبر تقنيات مثل "في بي ان " FBN أو "البروكسي" PROXY مما يستوجب دعمه بعناصر رقمية أخرىVPN .

أما البيانات الوصفية Metadada فهي بيانات خفية مرافقة للملفات الرقمية لا تظهر مباشرة للمستخدم، لكنها تحتوي على معلومات تقنية مهمة مثل تاريخ إنشاء الملف وتعديله، وهوية الجهاز أو البرنامج المستخدم، الموقع التقريبي أو إعدادات النظام، وساعة وتوقيت التعديل أو الإرسال، وتكمن أهميته في كونها تساعد على تتبع أصل الملف الرقمي وتحديد ظروف إنتاجه، مما يجعلها عنصرا مهما في كشف التلاعب أو التزوير أو نسب الأفعال الإلكترونية إلى فاعل معين، ويعتمد المحقق الجنائي والخبير المعلوماتي على تحليل هذه العناصر بشكل تكاملي، من خلال مقارنة التقنية وبيانات IP و Metadata مع السلوك المعلوماتي المعتاد، بهدف كشف أي انحراف قد يشير إلى نشاط إجرامي.

---

[1] المادة 04 من القانون 09-04 **مرجع سابق.**

[2] أمير فرج يوسف، البلطجة الإلكترونية، **مرجع سابق**، ص 163.

[3]Solange Ghernaouti, La cybercriminalité Les Nouvelles Armes De Pouvoir, 2éme édition, PRESS POLYTECHNIQUE ET UNIVERSITAIRES ROMANDES, 2018, P73.

كما أن توثيق هذه البيانات وحفظها يعد شرطا أساسيا لضمان حجيتها أمام القضاء، إذ يشمل ذلك تحديد مكان وزمان جمع الدليل، وتوثيق الوسائل التقنية المستخدمة، وحفظ سلسلة الحيازة القانونية (Chain of Custody)، بما يضمن سلامة الدليل الرقمي من أي تعديل أو عبث[1]

المطلب الثالث: سلطة القاضي الجزائي في تقدير الدليل الرقمي واشكالات اثبات الجريمة

تقوم قواعد الإثبات في المادة الجزائية على مبدأ جوهري يتمثل في حرية القاضي الجنائي في تكوين اقتناعه من مختلف الأدلة المعروضة عليه خلال مراحل التحقيق أو المحاكمة، دون أن يخضع في ذلك إلا لضميره وما يستخلصه من عناصر الدعوى، فلا يلزم القاضي بالأخذ بدليل معين، كاعتراف المتهم أو شهادة الشهود أو آراء الخبراء، إلا إذا اطمأن إلى صحته ووافق اقتناعه القضائي، كما لا يتقيد برفض دليل ما لمجرد تقديمه من جهة معينة، وإنما له سلطة ترجيح الأدلة وفق ما يراه أقرب إلى الحقيقة. تأسيسا على هذا المبدأ، فان وسائل الإثبات في المجال الجزائي ليست واردة على سبيل الحصر، رغم أن التشريع يورد أمثلة تقليدية لها، مثل الاعتراف، شهادة الشهود، محاضر الضبطية القضائية، تقارير الخبرة، وغيرها من الوسائل الشائعة لكن مع صدور قانون 09-04، أصبح بالإمكان التعامل معها بشكل أقرب للأشياء المادية، مع وضع وسائل خاصة لحمايتها وجمعها بسرعة[2].

الفرع الأول: حجية الدليل الرقمي في الإثبات الجنائي

لا يعتد بالدليل الرقمي الإلكتروني كوسيلة إثبات لمجرد وجوده أو لكونه يشير إلى وقوع الجريمة ونسبتها إلى شخص معين، بل لا بد أن تتوفر فيه قيمة قانونية تؤهله للاعتماد عليه قضائيًا.وتتحقق هذه القيمة من خلال خضوع الدليل الرقمي لشروط الإثبات الجنائي، وأهمها:

يرتكز الإثبات في مختلف القضايا على مجموعة من الأدلة التي تبنى عليها الأحكام القضائية، قبل التطرق لمدى حجية الدليل الالكتروني في الإثبات وجب التطرق إلى مفهوم الإثبات الجنائي، ثم بيان مدى حجية الدليل الإلكتروني من خلال الوقوف على أهم خصائصه.

يعرف الإثبات الجنائي بأنه عملية تقديم الأدلة والحجج من قبل السلطة القضائية بوسائل مشروعة، لإثبات وقوع الجريمة المنسوبة إلى المشتبه فيه، والتأكد من مدى انطباق نصوص قانون العقوبات على تلك الوقائع.

[1] أمير فرج يوسف، البلطجة الإلكترونية، **مرجع سابق**، ص 164.
[2] مناصرة يوسف، الدليل الإلكتروني في القانون الجزائي، **مرجع سابق**، ص 286.

وتتمثل أهداف الإثبات الجنائي فيما يلي[1]:

1_تعيين وتحديد الأدلة الجنائية المرتبطة بوقائع الدعوى .

2_تقييم قوة هذه الأدلة في تكوين قناعة القاضي وترجيح الحكم .

3_الكشف عن الحقيقة والوصول إليها .

4_التأكد من مشروعية الأدلة، من خلال مقارنتها بوقائع الدعوى ومراحلها مع أحكام قانون العقوبات وقانون الإجراءات الجزائية.

أولا: مبدأ مشروعية الدليل الرقمي

يشترط أن يكون الحصول على الدليل قد تم بطرق مشروعة، وفقًا للقواعد القانونية الشكلية والموضوعية المعمول بها في الاجراءات الجنائية ويقصد بذلك أن يتم استخراج الدليل الرقمي بطريقة إدارية من شخص مختص قانونًا، وبناءً على سبب مشروع ومحدد، إضافة إلى كون محل الإجراء الذي نتج عنه الدليل محددا بوضوح أو قابلاً للتحديد وألا يتضمن الإجراء أي مخالفة قانونية، سواء من حيث طريقة الحصول على البيانات أو الوسائل المستخدمة في جمعها. [2]

أ_ الشكلية

لا يقتصر شرط المشروعية في الدليل الرقمي الإلكتروني على الجانب الموضوعي فقط، بل يجب أيضًا الالتزام بالقواعد الشكلية عند مباشرة إجراءات الحصول عليه، وخاصة من حيث كيفية تنفيذ الإجراء. [3]

ب_ احترام الإجراءات

تعد القواعد الشكلية جزءا أساسيا من الضمانات القانونية، وهي محددة بموجب القانون وتهدف إلى احترام قواعد العدالة والأخلاقيات المهنية. فمشروعية الدليل لا تعني فقط مطابقته للنص القانوني، بل يجب أن يراعى أيضا:

1-حقوق الإنسان وخصوصيته.

---

[1] إبراهيم بالعليات، أركان **الجريمة وطرق إثباتها في قانون العقوبات الجزائري**، دار الخلدونية، الجزائر، الطبعة الأولى، 2007، ص137.

[2] أمير فرج يوسف، البلطجة الإلكترونية، **مرجع سابق**، ص 177.

[3] عفيفي كامل عفيفي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت، 2007، ص 382.

2-الاتفاقيات الدولية ذات الصلة.

3_القيم الأخلاقية والنظام العام

ج: بطلان الدليل غير المشروع

لا يجوز للقاضي الجزائي أن يبني حكمه على دليل تم الحصول عليه بطريقة غير مشروعة، كأن يكون[1]:

1-تم الحصول عليه تحت الإكراه

2-عبر انتهاك السر المهني دون سند قانوني.

3-نتيجة خيانة أمانة أو أي وسيلة مخالفة للقانون.

فأي دليل يثبت أنه مشوب بالبطلان أو التزوير أو تم تحصيله بإجراءات غير قانونية يُعد باطلًا وغير صالح للاستناد إليه.

ثانيا: مبدأ يقينية الدليل الجنائي الرقمي

مشروعية الدليل تمثل حدًا لا يجوز للقاضي تجاوزه، لما لهذا الشرط من أهمية في حماية حقوق الدفاع وضمان محاكمة عادلة[2]. فحرية القاضي في تكوين اقتناعه لا تعني إطلاق يده في الاستناد إلى أي دليل، بل يجب أن يكون هذا الدليل قد تم جمعه بشكل قانوني وسليم، بما يعزز قرينة البراءة ويحترم حقوق المتهم ضمن إطار الخصومة الجنائية العادلة[3].

يقصد بمبدأ يقينية الدليل الجنائي الرقمي أن يكون الدليل الإلكتروني المعروض على القاضي واضحا، دقيقا، وخاليا من الشك، بحيث يؤدي إلى تكوين قناعة جازمة بثبوت الواقعة ونسبتها إلى المتهم، فلا يكفي أن يوجد دليل رقمي، بل يجب أن يكون موثوقا الى درجة اليقين، وليس مجرد احتمال أو قرينة ضعيفة.

فيميز الفقه الجنائي المعاصر بين نوعين من اليقين في مجال الإثبات: اليقين القانوني واليقين المعنوي، فاليقين القانوني هو ذلك الذي يحدده المشرع مسبقا من خلال وضع قواعد وأدلة ملزمة يتعين على القاضي الأخذ بها، فيكون مصدره النص القانوني أكثر من اقتناع القاضي الشخصي. أما اليقين المعنوي، فيقوم

---

[1] غنية بالطي، **مرجع سابق**، ص 218.

[2] أمير فرج يوسف، **البلطجة الإلكترونية**، مرجع سابق، ص 192

[3] رابحي عزيزة، **مرجع سابق**، ص269.

على اقتناع القاضي الحر المستند إلى تقديره للأدلة المطروحة عليه دون تقيد بنوع معين منها، وهو الاتجاه الغالب في الأنظمة الحديثة، ومنها النظام الانجلوسكسوني الذي يشترط للإدانة بلوغ درجة "الإقناع دون شك معقول"[1]

وفيما يتعلق بالدليل الرقمي، فان تحقيق هذا اليقين يقتضي توافر شروط تقنية دقيقة، من أبرها سلامة النظام المعلوماتي الذي أنتجت من خلاله البيانات، ودقة المعطيات المستخرجة منه، وقد اشترطت بعض التشريعات المقارنة، خاصة في البيئة الإنجلوسكسونية أن تكون مخرجات الحاسوب ناتجة عن نظام يعمل بطريقة سليمة حتى تقبل كدليل[2].

ورغم ما يتمتع به الدليل الرقمي من قوة إثباتيه قد ترقى إلى درجة اليقين، باعتباره من الأدلة العلمية، إلا أنه ظل عرضة لبعض الشكوك التي لا تتعلق بمضمونه في حد ذاته، بل بالظروف المحيطة به، فهذه الشكوك قد ترجع إلى احتمال التلاعب بالبيانات أو تعديلها، أو إلى أخطاء تقنية في عملية استخراج الدليل، سواء بسبب استخدام أدوات غير ملائمة أو سوء تفسير النتائج المستخلصة.

غير أن هذه الإشكالات لا تنفي حجية الدليل الرقمي، بل تستدعي إخضاعه لرقابة فنية دقيقة، من خلال اللجوء إلى الخبرة التقنية المتخصصة التي تسمح بالتحقق من سلامته، ومن صحة الإجراءات المتبعة في جمعه وتحليله، وبذلك يتحقق التوازن بين الأخذ بالدليل الرقمي كوسيلة إثبات حديثة، وبين ضمان مصداقيته وتحقيق اليقين القضائي.

ثالثا: مبدأ وجوب مناقشة الدليل الإلكتروني

تعد قاعدة وجوب مناقشة الدليل الجنائي من أهم الضمانات التي تكفل تحقيق العدالة[3] ، سواء تعلق الأمر بدليل تقليدي أو بدليل رقمي ناتج عن الأنظمة المعلوماتية، فالأصل أن القاضي الجزائي لا يجوز له أن يبني حكمه إلا على الأدلة التي طرحت علنا في الجلسة وخضعت للمناقشة بين الخصوم احترام لمبدأي الشفوية والمواجهة.[4]

---

[1] أمير فرج يوسف، **البلطة الالكترونية**، نفس المرجع، ص 192.

[2] يوسف مناصرة، **الدليل الإلكتروني في القانون الجزائي**، مرجع سابق، ص 190.

[3] أمير فرج يوسف، **مرجع سابق**، ص 192.

[4] المادة 349 من **قانون الإجراءات الجزائية" يحكم القاضي في الدعوى حسب لاقتناعه الشخصي**، ولا يجوز له أن يبني حكمه إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت مناقشتها حضوريا أمامه"

من خلال نص المادة 212 من قانون الإجراءات الجزائية (الملغى)، وكذا **349 من القانون لسنة 2025 التي** تعد في نظام الإثبات الجنائي، إذ تكرس مبدأ حرية القاضي في تكوين اقتناعه، بحيث يفصل في الدعوى استنادًا إلى ما يتكون لديه من قناعة شخصية مبنية على الأدلة المعروضة أمامه، غير أن هذه الحرية ليست مطلقة، بل يقيّدها المشرّع بضوابط جوهرية تضمن تحقيق العدالة وصيانة حقوق الدفاع، ومن أهم هذه الضوابط أن لا يبني القاضي حكمه إلا على الأدلة التي قدمت في إطار المرافعات، والتي تم طرحها ومناقشتها حضوريًا أمامه، بما ينسجم مع مبدأي الشفوية والمواجهة.

يتضح من هذا النص أن المشرع الجزائري تبنى نظام الإثبات الحر في المادة الجزائية، حيث لم يحصر وسائل الإثبات في أدلة محددة، بل أتاح للقاضي إمكانية الاستناد إلى مختلف الأدلة، سواء كانت تقليدية كالشهادة والاعتراف، أو حديثة كالدليل الرقمي، ومع ذلك، فإن هذه السلطة التقديرية تخضع لرقابة قانونية تفرض على القاضي الالتزام بعدم الاعتماد على معلوماته الشخصية أو على وقائع لم تُعرض في جلسة المحاكمة، لأن ذلك من شأنه الإخلال بحقوق الدفاع ومبدأ المحاكمة العادلة[1].

كما تبرز أهمية هذه المادة في كونها تفرض على القاضي تسبيب حكمه بشكل ضمني من خلال بيان الأدلة التي اعتمد عليها، مع إظهار سبب اقتناعه بها دون غيرها، وهو ما يسمح برقابة قضائية فعالة على سلامة الأحكام. وتمتد أحكام هذه المادة لتشمل الأدلة الرقمية، حيث لا يجوز الاعتماد عليها إلا إذا تم تقديمها ومناقشتها في الجلسة، وثبتت سلامتها ومشروعيتها، بما يضمن تكوين قناعة قضائية مبنية على أسس موضوعية وقانونية سليمة[2]وعليه، لا يمكن للقاضي أن يستند في حكمه إلى معلوماته الشخصية، أو إلى ما شاهده أو علم به خارج إطار الدعوى، لأن هذه المعطيات لم تُعرض على الأطراف ولم تتح لهم فرصة مناقشتها أو الطعن فيها، ويُعدّ الاعتماد على مثل هذه المعلومات إخلالًا بضمانات المحاكمة العادلة، ومساسا بحقوق الدفاع.

كما أن الجمع بين صفة القاضي وصفة الشاهد يعد أمرا غير مقبول، لأن الشهادة تقتضي نقل الواقعة إلى القضاء ليتم تقييمها وتمحيصها، وهو ما يتطلب تدخل القاضي بصفته محايدا لتقدير مدى صدقها.

أما إذا كان القاضي نفسه مصدر هذه المعلومات، فإنه يفقد حياده ويصبح في وضع يصعب معه ممارسة الرقابة الموضوعية على الدليل، مما قد يؤثر على سلامة الحكم[3]،

---

[1] إلهام شهرزاد روابح، **الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية**، مجلة البحوث والدراسات القانونية والسياسية، العدد10، 2017، ص195.

[2] حسين طاهري، الجرائم الإلكترونية، **مرجع سابق**، ص 268.

[3] أمير فرج يوسف، البلطجة الإلكترونية، **مرجع سابق**، ص 192.

وبذلك، فإن وجوب مناقشة الدليل، خاصة في الجرائم المعلوماتية، يضمن أن تكون جميع الأدلة، بما فيها الأدلة الرقمية، محل فحص وتمحيص علني، بما يؤدي إلى تكوين قناعة قضائية سليمة قائمة على أسس قانونية صحيحة[1].

وعليه، فإن المادة 212 من قانون الإجراءات الجزائية من القانون السابق والمادة 349 من القانون الحالي لسنة 2025 تحقق توازنا دقيقا بين حرية القاضي في تقدير الأدلة من جهة، وضرورة التقيد بضمانات المحاكمة العادلة من جهة أخرى، مما يجعلها أساسا قانونيا لتأطير التعامل مع مختلف وسائل الإثبات، خاصة في ظل تطور الجرائم المعلوماتية وظهور الأدلة الرقمية.

الفرع الثاني: سلطة القاضي الجزائي في تقدير الدليل الرقمي

إن النصوص القانونية تفتح المجال للاعتماد على العديد من الأدلة، بما فيها القرائن وسائر الوسائل المستحدثة، وهو ما يسمح بإدماج الدليل الرقمي ضمن منظومة الإثبات الجنائي دون تعارض مع القواعد العامة[2]

وقد خول المشرع الجزائري في إطار تحقيق المحاكمة العادلة للقاضي الجنائي صلاحية الملائمة بين جميع الظروف والملابسات التي وقعت في ظلها الجريمة، ومما لا شك فيه أن طبيعة ومضمون الدليل التقني تعتبر مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص، على عكس الأدلة التقليدية المتعارف عليها في ساحة القضاء الذي يسهل على الكثير فهم مضمونه وإدراك حقيقته.[3]

أولا: مبدأ الإقتناع الشخصي للقاضي في تقدير الدليل الالكتروني

يتساوى الدليل الرقمي مع الأدلة التقليدية من حيث خضوعه لسلطة التقدير القضائي، إذ يحق للقاضي الأخذ به متى طمأن إلى سلامته ومصداقيته، والتنازل عنه إذا أثار الشك أو شابه خلل يؤثر في حجته. غير أن هذه الحرية ليست مطلقة، بل تقيدها جملة من الضوابط الأساسية، أهمها ضرورة أن يكون الدليل قد تم الحصول عليه ومناقشته وفق الإجراءات القانونية، وأن يعرض ضمن جلسات المحاكمة بما يضمن

[1] المادة 212 من **قانون الإجراءات الجزائية الجزائري المعدل والمتمم للأمر 156/66 الملغى**

[2] بدري فيصل، **مرجع سابق**، ص 247.

[3] محمد أحمد المنشاوي، **سلطة القاضي الجنائي في تقدير الدليل الالكتروني**، مجلة الحقوق، العدد 02، البحرين، 2012، ص 528.

احترام مبدأ المواجهة، فلا يجوز للقاضي أن يبني حكمه على معلومات شخصية أو وقائع لم تطرح للمناقشة القضائية[1]

كرّس القانون رقم 25-14 لسنة 2025 المتضمن قانون الإجراءات الجزائية جملة من المبادئ التي تأطر سلطة القاضي في تقدير الأدلة، بما فيها الأدلة التقنية. فقد نصت المادة 2 منه على أن الدعوى العمومية تُحرك وتُباشر من قبل الجهات القضائية المختصة، مما يضفي الطابع القانوني على استعمال الأدلة. كما أوجب القانون تسبيب الأحكام القضائية، الأمر الذي يلزم القاضي بتبرير موقفه من الأدلة الرقمية، سواء بالأخذ بها أو استبعادها.

كما أن قانون الإجراءات الجزائية المعدل والمتمم قد عزز، ضمانات المحاكمة العادلة من خلال تكريس حق الطعن أمام الجهات القضائية العليا، وهو ما يسمح بمراقبة مدى سلامة تقدير الأدلة التقنية. فقد جاء هذا القانون بمجموعة من الإصلاحات الرامية إلى حماية الحقوق والحريات، خاصة من خلال ضبط إجراءات التحقيق، مما يفرض ضرورة احترام المشروعية في جمع الأدلة الرقمية. وعليه، فإن سلطة القاضي في تقدير الأدلة التقنية في ظل هذا القانون تظل مرتبطة بمدى احترام القواعد الإجرائية وضمانات المحاكمة العادلة[2].

وتبرز أهمية هذه الحرية خاصة في مجال الجرائم المعلوماتية، حيث تلعب الأدلة التقنية دورًا أساسيًا في إثبات الجريمة، نظرًا لطبيعتها غير المادية. ففي هذه الحالات، يكون للقاضي دور حاسم في تقييم مدى مصداقية الأدلة الرقمية، مثل سجلات الدخول إلى الأنظمة، والمراسلات الإلكترونية، وعناوين بروتوكول الإنترنت، وغيرها.

قد يواجه القاضي الجنائي صعوبات عملية عند التعامل مع الدليل الرقمي، خاصة في ظل حداثة هذا النوع من الأدلة وتعقيد طبيعته التقنية، رغم أن التعديلات التشريعية قد أقرت الحجية القانونية للمحررات الإلكترونية دون أن تفصل بشكل دقيق في مسألة المفاضلة بينها وبين الأدلة الكتابية التقليدية. وفي هذا الإطار، يذهب بعض الفقه إلى الاستئناس بالتشريع المقارن، لاسيما القانون الفرنسي، الذي عالج هذه

[1] أمير فرج يوسف، **نفس المرجع**، مرجع سابق، ص 185.

[2] محمد حزيط، **الإثبات في المواد الجزائية في القانون الجزائري**، دار الجامعة الجديدة، 2019، ص 98.

المسألة من خلال إقراره بسلطة القاضي في ترجيح الدليل الأكثر إقناعًا ومنطقية[1]، دون تمييز مسبق بين المحرر الورقي والإلكتروني، وذلك في حال غياب نص وطني صريح ينظم هذه المفاضلة[2].

وفي إطار تكريس الحجية القانونية للمحررات الإلكترونية، يبرز تطبيق القضاء الجزائري من خلال القرار الصادر عن القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بمجلس قضاء الجزائر، حيث عالجت المحكمة قضية المدعو "س.م.م" والتي تتعلق بإنشاء شبكة اتصالات إلكترونية دون رخصة، والدخول والبقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات، إلى جانب جرائم أخرى مرتبطة باستغلال غير مشروع لشبكات الاتصالات. وتعود وقائع القضية إلى شكوى تقدمت بها مؤسسة "اتصالات الجزائر" إثر تسجيل مكالمات دولية غير مبررة، صادرة من خطوط هاتفية من نوع (FTTP) ترتب عنها فواتير مرتفعة دون علم أصحابها. وقد كشفت التحريات التقنية المنجزة من طرف المصالح المختصة، مدعومة بتقارير فنية صادرة عن مختلف المديريات التقنية (الأمن السيبراني، استغلال الشبكات، الدعم التجاري)، عن وجود عملية تحويل احتيالية للمكالمات نحو الخارج، باستعمال تجهيزات إلكترونية متخصصة واستغلال ثغرات في النظام المعلوماتي للمؤسسة[3]. وقد أسست المحكمة قناعتها على جملة من الأدلة الرقمية والتقنية، تمثلت أساسا في نتائج التفتيش الإلكتروني الذي أضفى إلى ضبط معدات تقنية (أجهزة اتصال، منصات ج س م GSM، تجهيزات تحويل المكالمات) تستخدم في إنشاء شبكة اتصالات غير مرخصة، بالإضافة إلى تقارير الخبرة الفنية التي أثبتت قيام المتهم بإنشاء تطبيق إلكتروني يُستعمل كمنصة لإدارة الاتصالات وتحويلها، وربط عدة شرائح هاتفية في آن واحد، البيانات والسجلات الإلكترونية التي أظهرت وجود نشاط مكثف وغير عادي للمكالمات الدولية انطلاقا من الخطوط محل الشكوى، المراسلات والاتصالات الإلكترونية التي كشفت عن وجود تنسيق بين المتهم وشركاءه بالخارج لاستغلال الشبكة وتحقيق أرباح غير مشروعة، ومن خلال ذلك خلصت المحكمة إلى أن الأركان المادية للجريمة قائمة، سواء من خلال إنشاء شبكة اتصالات إلكترونية دون ترخيص أو الولوج إلى نظام المعالجة الآلية للمعطيات واستغلاله، كما اعتمدت في إثبات القصد الجنائي إلى تعمد المتهم لاستخدام وسائل تقنية متطورة واستمراره في السلوك الإجرامي رغم علمه بعدم مشروعيته، فالمحكمة استنتجت أدلتها بعد قيامها

[1] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، مرجع سابق، ص 259.
[2] حسين طاهري، **نفس المرجع، نفس الصفحة.**
[3] حكم صادر **عن القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال**، مجلس قضاء الجزائر، محكمة الدار البيضاء بتاريخ 2025/01/22 (غير منشور).

بإجراءات التفتيش والتحقيق أين تأكدت من قيام الأسس القانونية للجريمة نتيجة قيام الأدلة المشروعة وترابطها والتي كونت لدى القاضي قناعة منطقية بنى على أساسها حكمه بإدانة المتهم وشركائه.

ثانيا: القيود الواردة على سلطة القاضي الجزائي في تقدير الدليل الإلكتروني

لا يتم الاعتماد على مخرجات الأنظمة المعلوماتية (بمعنى البيانات المستخرجة من النظام المعلوماتي) إذا مسها خلل تقني أو إجراء غير مشروع يؤثر على سلامتها وحجيتها، كما أن الدليل الرقمي يخضع لمبادئ أساسية تتحكم في مدى قبوله، يمكن إجمالها في ثلاث مبادئ رئيسية: تتمثل في مبدأ اليقين، أي أن يكون الدليل واضحا خاليا من أي شك، مبدأ وجوب مناقشة الدليل، الذي يكرس حق الدفاع، مبدأ مشروعية الدليل بمعنى الحصول على الدليل بطرق قانونية مشروعة وهو ما تم التطرق إليه سابقا.

أ_ نظام الإثبات الحر

حذا المشرع الجزائري حذو باقي التشريعات في الأخذ بمبدأ حرية الإثبات في المواد الجزائية[1]، ويستند هذا المبدأ إلى قانون الإجراءات الجزائية الجزائري، الذي يكرس حرية القاضي في تكوين اقتناعه الشخصي، بنصه" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها قانون على غير ذلك[2]، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"[3] وهو ما تأكد أيضًا في ظل القانون رقم **25-14 لسنة 2025**، الذي حافظ على هذا التوجه من خلال عدم تقييد القاضي بوسائل إثبات محددة، مع التأكيد على ضرورة تسبيب الأحكام القضائية، الأمر الذي يفرض على القاضي تبيان الأسس التي اعتمد عليها في تكوين قناعته.

ب_ نظام الإثبات المقيد

بالرغم من اعتراف مختلف الشريعات منها التشريع الوطني بمبدأ حرية القاضي في قبول الدليل الرقمي الجنائي الا أن هذه الحرية غير مطلقة إلا اعتمادًا على أدلة معيّنة حددها النص القانوني، دون أن يستند إلى علمه الشخصي أو يضفي على دليل ما قيمة تتجاوز ما قرره له المشرّع. ومفاد ذلك أن القاضي يكون ملزمًا بقبول الدليل أو رفضه وفقًا لما ينص عليه القانون، دون أن يكون له مجال واسع للاجتهاد في هذا الشأن[4]، فهو يخضع لجملة من القيود التي تهدف إلى ضمان سلامة التقدير القضائي. فمن جهة، يلتزم

---

[1] بدري فيصل، **مرجع سابق**، ص 244.

[2] الهام شهرزاد روابح، مرجع سابق، ص196.

[3] ايت حمودة كاهنة، **البحث والتحري الجنائي في مسرح الجريمة الإلكترونية، مجلة الفكر القانوني والسياسي**، المجلد السابع، العدد الأول، 2023، ص 15

[4] حجازي البلومي، **حجية الدليل الإلكتروني في الإثبات الجنائي**، دار الجامعة الجديدة، الإسكندرية، 2010، ص

القاضي بالتحقق من استيفاء الدليل للشروط القانونية اللازمة، وتقييم مدى مصداقيته في ضوء وقائع الدعوى. ومن جهة أخرى، قد تعترض القاضي عوائق ذاتية وموضوعية تحد من فعالية تعامله مع هذا النوع من الأدلة. فمن الناحية النفسية، قد يميل القاضي إلى تفضيل الأدلة التقليدية التي اعتاد التعامل معها، بالنظر إلى رسوخها في الممارسة القضائية، مقارنة بالمحررات الإلكترونية التي تظل حديثة نسبيًا. أما من الناحية التقنية، فإن التحقق من صحة المحررات الإلكترونية، خاصة ما يتعلق بالتوقيع الإلكتروني وسلامة البيانات، يتطلب معرفة تقنية متخصصة، وهو ما قد يتجاوز التكوين التقليدي للقاضي. ورغم إمكانية تجاوز هذا العائق من خلال الاستعانة بالخبرة الفنية، إلا أن ذلك يفرض بدوره ضرورة إلمام القاضي بالحد الأدنى من المعارف التقنية، حتى يتمكن من تقييم تقارير الخبرة تقديرا سليما[1].

ج_ نظام الإثبات المختلط

يذهب جانب من الفقه إلى نظام اعتبار أن نظام حرية الإثبات ونظام الإثبات المقيد لا يشكلان نظاما مستقلا بذاته، وإنما يمثلان مزيجا وتوفيقا بين النظامين، ذل من خلال قيام المشرع بتحديد وسائل الإثبات التي يجوز للقاضي الاعتماد عليها عند الفصل في الدعوى وإصدار الحكم فيها[2].

وإلى جانب ذلك، يقوم المشرع بتحديد الحجية القانونية لكل دليل متى استوفى شروطًا معينة، مما يفرض على القاضي الأخذ به متى توفرت تلك الشروط، وليس له استبعاده بناءا على تقديره الشخصي. وعلى العكس من ذلك، إذا لم تتوافر الشروط المطلوبة، يتعين على القاضي عدم الاخذ به، حتى وإن كان مقتنعًا به من الناحية الشخصية، مما يعني أن دوره يقتصر على تطبيق النصوص القانونية المنظمة لقواعد الإثبات.

أما في الدول التي تعتمد هذا النظام، مثل إنجلترا، فقد أصدرت تشريعات خاصة، من بينها قانون إساءة استخدام الحاسوب لسنة 1990، غير أنه لم يتطرق بشكل صريح إلى مسألة الأدلة المستمدة من الحاسوب. وذلك إلى وجود قواعد الإثبات العامة في قانون الشرطة والإثبات الجنائي لسنة 1984، الذي نظم كيفية قبول الأدلة، بما في ذلك مخرجات الحاسوب والإنترنت، ضمن منظومة الإثبات الجنائي[3].

---

[1] مناصرة يوسف، **الدليل الإلكتروني في القانون الجزائي، دار الخلدونية**، 2018، ص 288

[2] حسين طاهري، **جرائم القرصنة الإلكترونية**، مرجع سابق، ص 199.

[3] محمد أحمد المنشاوي، **المرجع السابق**، ص 533.

ثالثا: الضمانات القانونية المقيدة لسلطة القاضي الجزائي

رغم اتساع السلطة التقديرية للقاضي الجزائي، إلا أنها ليست مطلقة، بل تخضع لقيود قانونية تهدف إلى ضمان مشروعية الإثبات وتحقيق التوازن بين مصلحة المجتمع في مكافحة الجريمة وحماية حقوق الأفراد، ومن أهم هذه القيود

1_ قيد المشروعية:

الذي يقتضي أن يتم الحصول على الأدلة، خاصة التقنية منها، وفقًا للإجراءات القانونية المنصوص عليها. وفي هذا السياق، جاء القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ليحدد الإطار القانوني لجمع الأدلة الرقمية، حيث اشترط احترام إجراءات معينة، مثل الحصول على إذن قضائي عند القيام بعمليات التفتيش الإلكتروني أو اعتراض المراسلات

2_ قيد تسبيب الأحكام القضائية:

يعتبر تسبيب الأحكام القضائية من القيود الجوهرية على سلطة القاضي، حيث أوجب القانون رقم 25-14 لسنة 2025 على القاضي تعليل قراراته، مما يفرض عليه توضيح الأسباب التي دفعته إلى الأخذ بدليل معين أو استبعاده، وهو ما يتيح إمكانية الرقابة على أحكامه من قبل الجهات القضائية الأعلى[1].

إضافة إلى ذلك، تخضع سلطة القاضي لرقابة القضاء الأعلى من خلال طرق الطعن، سواء بالاستئناف أو النقض، حيث يمكن إعادة النظر في مدى سلامة تقدير الأدلة، خاصة إذا شابها خطأ في التقدير أو خرق للقانون.

ولا يمكن إغفال حماية الحقوق والحريات الفردية كقيد أساسي، حيث لا يجوز الاعتماد على دليل تم الحصول عليه بطرق غير مشروعة، كالتصنت غير القانوني أو الاختراق غير المرخص للأنظمة المعلوماتية، لما في ذلك من مساس بحرمة الحياة الخاصة[2].

الفرع الثالث: صعوبات الإثبات في جريمة القرصنة الإلكترونية

إن الإثبات الرقمي الجنائي عملية متكاملة تستهدف البحث عن الأدلة الجنائية التي تثبت حدوث الواقعة الجنائية المرتكبة وظروف ارتكابه وأسبابها وتنسيقها إلى مقترفيها وذلك لتقديمهم للعدالة، بحيث تواجه

---

[1] قانون الإجراءات الجزائية الجزائري، **بموجب القانون رقم 25-14 لسنة 2025، الجريدة الرسمية للجمهورية الجزائرية**، العدد 54، سنة 2025، مرجع سابق.

[2] بدري فيصل، **مرجع سابق**، ص 262.

الجرائم الالكترونية في هذا المجال عدة صعوبات عند إثباتها والتي انعكست بدورها على الأدلة المتحصل عليها من هذه الجرائم.[1]

وتقف وسائل الإثبات الجنائي التقليدية عاجزة عن مواجهة الجرائم الالكترونية التي تنصب على المعلومات والبيانات المخزنة في نظم المعلومات والبرامج مما أدى الى بروز ظاهرة جديدة وهي الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والانترنت نتج عنها ما يسمى بالدليل الالكتروني او الدليل الرقمي لإثبات وقوع الجرائم الالكترونية ونسبتها لمرتكبيها.

غير أن الدليل الالكتروني تعترضه عدة عقبات في استخلاصه من طرف سلطات التحقيق والتحري تتمثل في [2]

_عدم ظهور الدليل الالكتروني وسهولة محوه وتدميره، وأيضا صعوبة الوصول إليه.

_عدم ظهور الدليل الالكتروني يتميز الدليل الالكتروني بأنه يُستخلص من بيئة رقمية من ذات العمليات الالكترونية ولا يمكن أن يتم اكتشافه بالطرق التقليدية وإنما قد يحتاج لاستخدام تقنيات علمية ذات تكنولوجيات متطورة يجب إتباعها للوصول إليه، لكونه دليلاً غير مادي غير مرئي وغير مقروء، فتشمل هذه الخصائص ما يلي:

أولا: الدليل الرقمي دليل غير مرئي

إن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقع عليها أو بواسطتها ما هي إلا بيانات غير مرئية لا تفضح عن شخصية معينة، وهذه البيانات مسجلة إلكترونيا بكثافة بالغة، وبصورة مشفرة غالبا على دعائم أو وسائل للتخزين ضوئية كانت ممغنطة لا يمكن للأفراد قراءتها، وإن كانت قابلة للقراءة من قبل الأدلة نفسها فلا يترك التعديل أو التلاعب فيها أي أثر مما يقطع أي صلة بين المجرم وجريمته ويحول ذلك دون كشف وتجميع الأدلة اللازمة لإثبات وقوع الجريمة ونسبتها لمرتكبيها ويعد من أبرز العوائق التي يمكن أن تواجه جهات التحري والملاحقة.[3]

---

[1]Mutter Maler (C.J.A).Traite de la prévue en matière criminelle. Trad. Alexander. IMP. Librairie général de jurisprudence .Parise.1884.p3

[2]أمير فرج يوسف، **البلطجة الإلكترونية**، مرجع سابق، ص 162.

[3]أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائي، دار النهضة العربية** القاهرة،1981، ص418.

ثانيا: الآثار الرقمية المترتبة عن الجريمة الالكترونية

إن هذه الآثار هي كما أشرنا أعلاه عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة، فلا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان، أيضا حجم البيانات وكم الملفات الالكترونية التي تمس الجريمة من بين الكم الهائل لفصل البريئة منها والتي تؤدي في الغالب إلى اصطدام مهمة الاكتشاف بحق الأفراد في الخصوصية الشخصية.

ثالثا: استخلاص الأدلة يعد تحديا لرجال الأمن

يرى المختصون في جرائم الحاسب الآلي أن الجهاز وما يقع عليه من جرائم معلوماتية يعد تحديا هائلا لرجال الأمن ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بالصورة التقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريم المعلوماتية التي تقع بطريقة تقنية عالية ولذلك فغالبية الجرائم الالكترونية تُكتشف عن طريق الصدفة وليس عن طريق الإبلاغ[1].

ويرى البعض الآخر من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل مسؤوليتها الكاملة، نحو اكتشاف الجرائم وضبطها للمجرمين، [2]وكذا محاكمتهم، والدليل الالكتروني هو طريقة خاصة لإظهار الحقيقة والذي يتم فيه اللجوء إلى إحدى الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب والرسائل الالكترونية المخزنة آو المنقولة رقميا، وان هذا الدليل ينبغي أن يخضع في قبوله لجملة من الشروط وهي أن يكون مشروعا ويقينيا وان تتم مناقشته في جلسة الحكم، كما أن حجيته في الإثبات الجنائي تختلف بحسب نظام الإثبات.

[1] أمير فرج يسف، **مرجع سابق**،157

[2] محمد مصطفى **يوسف، مشروعية الدليل في المسائل الجنائية، الإسكندرية**، مصر: دار الجامعة الجديدة، 2011، ص 64.

خاتمة الفصل الأول:

يتضح أن فعالية مكافحة جريمة القرصنة الالكترونية لا تتوقف على تجريم الافعال والعقاب عليها فحسب، بل ترتبط أساسا بمدى نجاعة اجراءات البحث والتحري والمتابعة الجزائية، التي تستوجب سائل تقنية متطورة وكفاءة متخصصة خاصة في مجال الاثبات والدليل الرقمي.

فخصوصية الإثبات في الجرائم الإلكترونية تعد عنصرا ضروريا لضمان التوازن بين فاعلية التحقيق القضائي وحماية الحقوق والحريات الفردية، خاصة الحق في الخصوصية والسرية وحماية البيانات الشخصية.

ويظهر الدليل الإلكتروني في صور متعددة قد يكون في شكل بيانات أو إشارات أو نبضات رقمية يمكن تجميعها وتحليلها باستخدام تقنيات وبرامج متخصصة، وقد يظهر هذا الدليل في صور متعددة، كالنصوص المكتوبة، أو الصور، أو التسجيلات، أو الأرقام والرموز ذات الدلالة الخاصة Ip،

مما تظهر أهمية هذا النوع من الأدلة في إثبات جرائم القرصنة الإلكترونية، رغم ما يكتنفه من صعوبات تتعلق بقابليته للتغيير أو الإتلاف، الأمر الذي يستدعي اعتماد آليات فنية وإجرائية دقيقة تضمن سلامته وحجيته في مواجهة هذه الجريمة.

الفصل الثاني

آليات المحاكمة في جرائم القرصنة الإلكترونية

بعد الوقوف على أبرز صور القرصنة الإلكترونية التي أفرزتها البيئة الرقمية، وما تتسم به من خصوصية في ارتكابها واخفاء اثارها وصعوبة الكشف عن ادلتها، يقتضي البحث الانتقال الى بيان مدى استجابة الإجراءات الجزائية لهذه الخصوصية، وقد نظم المشرع الجزائري هذه الجرائم ضمن أحكام قانون العقوبات، حيث جرم الأفعال التي تمس بأنظمة المعالجة الآلية للمعطيات، مثل :الدخول أو البقاء غير المشروع في نظام معلوماتي، عرقلة سير النظام المعلوماتي أو تعطيله، إدخال بيانات أو حذفها أو تغييرها بطريقة غير مشروعة، استعمال البيانات أو استغلالها بطريقة غير قانونية، كما اعتبر المشرع أن هذه الجرائم تمس بأمن المعلومات وسلامة الأنظمة الرقمية التي أصبحت تشكل ركيزة أساسية في مختلف المجالات الإدارية والاقتصادية وحتى الأمنية منها، الأمر الذي دفعه لاستحداث إجراءات للتحقيق والمحاكمة تتلاءم مع الطبيعة الخاصة لهذه الجريمة و استنادا للتعديل الأخير لقانون الإجراءات الجزائية الجديد .

تعتبر الإحالة إلى القضاء مرحلة مهمة من مراحل الدعوى العمومية، فهي تنقل الدعوى من طور إلى آخر فهي تنقلها من الاتهام أو التحقيق إلى المحاكمة ومن جهة فهي تجسد معنى اتهام الفرد بارتكاب الجريمة، ومن جهة أخرى تعد المحاكمة في شقها الموضوعي مرحلة إجرائية ترسم نطاق الاتهام في صورة دعوى جزائية تنطوي على شق موضوعي في الوقائع المنسوبة إلى المتهم دون غيرها، أما في شقها الشخصي فتنصب المحاكمة على الشخص المطلوب محاكمته، فيتم تحديد الواقعة أو الوقائع المجرمة والشخص أو الأشخاص محل الاتهام بشكل نهائي، فتلتزم المحكمة بعد ذلك بالفصل في الوقائع المحالة إليها، كما أنها تتقيد بحسب الأصل بمحاكمة من أقيمت عليهم الدعوى[1].

يؤدي التحقيق القضائي دورا مهما في الكشف عن الأدلة التي تثبت الإدانة مع استبعاد الأدلة الضعيفة التي ليس لها تأثير على سير الدعوى وكشف الحقيقة، مما يساعد على توضيح وقائع الدعوى قبل إحالتها إلى المحكمة للفصل فيها. وتعد هذه المرحلة تمهيدا للمحاكمة، إذ لا يهدف التحقيق القضائي إلى إصدار حكم بالإدانة أو البراءة، وإنما يقتصر على جمع العناصر التي تساعد على إظهار الحقيقة[2].

[1] عبد الرحمان خلفي، مرجع سابق، **الإجراءات الجزائية في القانون الجزائري والمقارن**، ص 457.
[2] نفس المرجع

المبحث الأول: التحقيق القضائي والمحاكمة في الجرائم المعلوماتية

يقصد بالتحقيق القضائي مجموعة الإجراءات القانونية التي تباشرها الجهات القضائية المختصة بقصد جمع الأدلة وتحليلها والتأكد من صحة الوقائع المنسوبة إلى المتهم، مع تحديد الوصف القانوني للفعل الإجرامي والكشف عن الحقيقة من أجل اتخاذ القرار المناسب بشأن الدعوى. ويُعد التحقيق القضائي مرحلة أساسية في الجرائم الإلكترونية، لاسيما جرائم القرصنة الإلكترونية، نظراً لما تتسم به من تعقيد تقني وصعوبة في تتبع الأدلة الرقمية وإثباتها. لذلك يحرص قاضي التحقيق على الاستعانة بالخبرة الفنية لفحص الأنظمة المعلوماتية والأجهزة الإلكترونية وكشف وسائل الاختراق المستعملة وتحديد المسؤولية الجزائية للفاعل. وقد أوجب المشرع إجراء التحقيق القضائي في مواد الجنايات وفقاً لأحكام المادة 139 من قانون الإجراءات الجزائية، بينما جعله جوازياً في الجنح ما لم يقرر القانون خلاف ذلك، كما يمكن مباشرته في المخالفات بناءً على طلب وكيل الجمهورية، متى اقتضت ظروف القضية ذلك، خاصة إذا تعلق الأمر باعتداءات إلكترونية تمس أمن الأنظمة المعلوماتية أو البيانات الرقمية

ويتميز التحقيق القضائي بطابع قضائي يختلف عن التحقيق الأولي الذي تباشره الشرطة القضائية، باعتبار أن هذا الأخير لا يحمل الصفة القضائية الكاملة نفسها. كما يقوم التحقيق القضائي على الحياد، والموضوعية في تقدير الأدلة، بما يسمح بتقييمها تقييماً سليماً قائماً على الوقائع والمعطيات المتوفرة ولهذه الأهمية، منح المشرع الجزائري سلطة إجراء التحقيق للقاضي المختص، لما يتمتع به من ضمانات قانونية تسهم في حماية الحقوق والمساعدة على كشف الحقيقة[1].

وفي ظل قانون الإجراءات الجزائية الجديد فقد استبدل المشرع الجزائري مصطلح التحقيق الابتدائي، بالتحقيق القضائي بسبب الخلط بين أعمال الشرطة القضائية، وقاضي التحقيق، لذا تم تخصيص مصطلح التحقيق الابتدائي لعمل الشرطة القضائية ومصطلح التحقيق القضائي لعمل قاضي التحقيق[2].

المطلب الأول: اختصاصات قاضي التحقيق في جريمة القرصنة الالكترونية

لقد نصت المادة 141 من قانون الإجراءات الجزائية على اختصاصات قاضي التحقيق المتعلقة بالبحث والتحري بناء على طلب من وكيل الجمهورية أو على شكوى مصحوبة بادعاء مدني[3]، يقدمها الطرف المتضرر من الجريمة، وذلك وفقا للأحكام المنظمة لإجراءات تحريك الدعوى العمومية، ويباشر قاضي

[1] عبد الرحمان خليفي، **مرجع سابق**، ص 325.

[2] حزيط محمد، **مرجع سابق**، ص 262.

[3] المادة 141 **من قانون الإجراءات الجزائية الجديد لسنة 2025.**

التحقيق سلطاته القانونية خاصة في حالات الجنايات المتلبس بها[1]، حيث يملك صلاحيات واسعة في البحث والتحري وجمع الأدلة واتخاذ الإجراءات الضرورية للكشف عن الحقيقة، مثل التفتيش والحجز وسماع الأطراف والاستعانة بالخبرة الفنية، وهو ما يكتسي أهمية خاصة في جرائم القرصنة الإلكترونية التي تتطلب فحص الأنظمة المعلوماتية وتتبع الأدلة الرقمية،

يقوم التحقيق على مبدأ التقاضي على درجتين على مستوى المحكمة ممثلا من قاضي التحقيق وعلى مستوى المجلس القضائي ممثلا من طرف غرفة الاتهام[2].

الفرع الأول: إجراءات التحقيق في جريمة القرصنة الالكترونية

يمارس قاضي التحقيق مهامه بطريقتين: فقد يباشر إجراءات التحقيق بنفسه، مثل استجواب المتهم، وسماع الشهود، وإجراء المواجهات، والمعاينات، والتفتيش والحجز، كما يمكنه إصدار الأوامر القضائية ذات الطبع الإجباري كأوامر الإحضار والقبض والإيداع، وفي المقابل، قد يكلف بعض الجهات كالخبراء أو إنابة الضبطية القضائية للقيام ببعض إجراءات البحث والتحري باعتبارهم جهات مساعدة.

ولا يقتصر دور القاضي على الأعمال المكتبية داخل المحكمة، بل يمتد إلى الميدان من خلال الانتقال إلى أماكن وقوع الجريمة أو أي موقع يحتمل وجود أدلة أو أثار تفيد في التحقيق، وذلك قصد إجراء المعاينات والتفتيش أو إعادة تمثيل الوقائع وسماع الأشخاص الذين قد تكون لديهم معلومات مرتبطة بالقضية قبل التأثير عليهم أو تغيير أقوالهم.

ولضمن تنظيم إجراءات التحقيق وحفظ مختلف المحاضر والوثائق، يفتح قاضي التحقيق ملفا خاصا لكل قضية، منذ بداية التحقيق إلى غاية انتهائه[3].

حيث أننا تطرقنا إلى إجراءات التفتيش والمعاينة والحجز واعتراض المراسلات أثناء تطرقنا إلى صلاحيات الشرطة القضائية وبالتالي وتفاديا للتكرار فإننا نعرج على هذه الإجراءات المخولة لقاضي التحقيق بنوع من الإيجاز

أولا: المعاينة من طرف قاضي التحقيق

يمكن لقاضي التحقيق إجراء المعاينات التي لم تقم بإجرائها الشرطة القضائية فيكون مضطرا لإجرائها وهو ما جاءت به المادة **155 من قانون الإجراءات الجزائية** التي تنص على أنه "**يجوز لقاضي التحقيق،**

---

[1] المادة 69 فقرة 4 ق.إ.ج.ج "**في حالة الجناية أو الجنحة المتلبس بها، يباشر قاضي التحقيق السلطات المخولة له بمقتضى المادة 91 ومايليها من هذا القانون** "

[2] بدري فيصل، **مرجع سابق**، ص 218.

[3] محمد حزيط، **مرجع سابق**، ص 300.

الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بأمين ضبط التحقيق ويحرر محضرا بما يقوم به من إجراءات"[1].

حيث أن المشرع الجزائري أضفى من خلال نص المادة السالفة الذكر الطابع الشكلي للإجراءات المتمثل في إخطار وكيل الجمهورية وحضور الأمين العام **حتى يحقق نوعا من الرقابة والتنسيق بين جهات التحقيق**، إلا أن تطبيق هذه المادة في الجرائم الإلكترونية يتلقى العديد من الصعوبات لكونه غير محدد جغرافيا، فالانتقال إلى "**مكان الجريمة** " في البيئة الرقمية يثير بعض الصعوبات العملية.

ثانيا: التفتيش الالكتروني

وبقصد بالتفتيش في مكونات **المنظومة المعلوماتية** سواء كانت مادية ملموسة أو غير مادية افتراضية، وقد نصت المادة 76 في فقرتها الأخيرة من قانون **الاجراءات الجزائية لسنة 2025** بتحديد أوقات التفتيش أو الحجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني بدون حضور المتهم أو صاحب المسكن أو الشهود، عندما يتعلق الأمر ببعض الجرائم منها الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، كما يمكن لقاضي التحقق أن يكلف ضباط الشرطة القضائية بالتفتيش نيابة عنه طبقا لنص المادة 234 من نفس القانون إذا تعذر عليه القيام بذلك بموجب إذن بالتفتيش يحمل اسم المصدر و اسم المأذون بتفتيش مسكنه وعنوانه والمهمة والمهلة المحددة مع وصف الجرم موضوع البحث أين يتقيد المناب بالإذن فلا يجوز مخالفته ، وفي حال اكتشاف المناب لوقائع جديدة يقوم بإخطار قاضي التحقيق الذي بدوره يخطر وكيل الجمهورية لاتخاذ الإجراءات اللازمة[2]

وقد أجاز المشرع الجزائري التفتيش ونظمه من خلال القانون 09-04 لاسيما المادة 05 منه التي تم التطرق إليها سابقا غير أن هذا الإجراء يثير إشكالات قانونية معقدة خاصة عندما يمتد الوصول إلى بيانات مخزنة بدولة أجنبية، ففي هذه الحالة قد يعتبر توسيع نطاق التفتيش ليمس بسيادة الدولة التي توجد بها المعطيات أو الأنظمة[3]، مما يستوجب الاستعانة بالسلطات الأجنبية في إطار التعاون القضائي الدولي ووفق الاتفاقات والمعاهدات المبرمة فيما بينهم ليبقى هذا الإجراء مرتبطا لمبدأ المعاملة بالمثل[4] مما قد يحد في الكثير من الأحيان من فعالية التفتيش وسرعة الوصول إلى الدليل الرقمي العابر للحدود.

---

[1] المادة **155 من قانون الإجراءات الجزائية**

[2] محمد حزيط، **مرجع سابق**، ص 330

[3] مجدوب لامية، مرجع سابق، ص 111.

[4] بدري فيصل، **مرجع سابق**، ص 222.

ثالثا: الإنابة القضائية

الإنابة القضائية وسيلة قانونية تمكن قاضي التحقيق ن تكليف جهة قضائية أو ضباط الشرطة القضائية المختصين إقليميا بالقيام ببعض إجراءات البحث والتحري نيابة عنه، مع التزام الجهة المنابة بإبلاغ قاضي التحقيق بكل المستجدات المتعلقة بالقضية، وتزداد الإنابة القضائية في الجرائم الإلكترونية بسبب طابعها العابر للحدود، إذ قد تستدعي التحقيقات تتبع الجناة وجمع الأدلة خارج الإقليم الوطني، وهو ما يفرض اللجوء إلى الإنابة القضائية الدولية التي تستند إلى الاتفاقيات الثنائية والمتعددة الأطراف، إضافة إلى القوانين الوطنية ومبدأ المعاملة بالمثل، وتتم عادة بالطريق الدبلوماسي أو عن طريق السلطات المركزية المختصة بوزارة العدل، سواء تعلق الأمر بالإنابات الواردة إلى الجزائر أو الصادرة منها إلى الخارج .

لقد دعمت الجزائر هذا النوع من التعاون من خلال عدة اتفاقيات دولية من بينها اتفاقية التعاون القضائي مع المملكة المتحدة لبريطانيا وإيرلندا الموقعة بلندن في 11 يوليو 2006 التي حددت مجال تطبيق التعاون وتضمنت إجراءات تبادل طلبات التحقيق وجمع الأدلة والتفتيش والحجز عبر السلطات المركزية المختصة في كلا البلدين[1].

ما يلاحظ من خلال ما سبق أن النصوص التقليدية المنظمة للإنابة القضائية لم توضع تحديدا لمواجهة الجرائم الإلكترونية، الأمر الذي يوضح القصور التشريعي في مجابهة الجريمة، كما أن خضوع الإنابة لمبدأ المعاملة بالمثل قد يعرقل التحقيق في الحالات التي لا يكون فيها اتفاقات تعاون بين الدول، أو عندما ترفض الدولة الأجنبية تنفيذ الطلب بدعوى المساس بسيادتها أو بأمنها المعلوماتي.

رابعا: الخبرة التقنية

يقوم قاضي التحقيق باختيار الخبير المعتمدين في الجدول التابعين للمجس القضائي طبقا لنص المادة 240 من القانون الذي يقوم بالمهام المكلف بها تحت رقابة قاضي التحقيق وفي المدة المحددة من طرفه مع التزامه بالقيام بالخبرة على أكمل وجه[2].

الفرع الثاني: قواعد الاختصاص الإقليمي لقاضي التحقيق في جرائم القرصنة الالكترونية

ناهيك عن القاعدة العامة التي تجيز لقاضي التحقيق الانتقال في حدود دائرة اختصاصه القضائي، فقد أجازت المادة 156 من القانون لقاضي التحقيق الانتقال رفقة امين الضبط الى دوائر اختصاص المحاكم

[1] محمد حزيط، **مرجع سابق**، ص 340.

[2] بدري فيصل، **مرجع سابق**، ص 223.

المجاورة للدائرة التي يمارس فيها وظيفته وهذا بغرض اجراء التحقيق فيقوم بإخطار وكيل الجمهورية مع التنويه عن سبب انتقاله للمعاينة [1]

أما من حيث الاختصاص المحلي لقاضي التحقيق، فإنه يتحدد بمكان ارتكاب الجريمة، أو بمحل إقامة أحد المتهمين أو المشتبه في مساهمتهم في الفعل الإجرامي، كما يمكن أن ينعقد الاختصاص في المكان الذي يوجد فيه أحد هؤلاء الأشخاص حتى ولو كان وجوده بصفة عرضية أو لسبب أخر وهو ما ينطبق على الجرائم الإلكترونية بالنظر إلى الطابع العابر للحدود الذي تتميز به مثلا كأن يقع الاختراق الإلكتروني في مكان بينما توجد الخوادم أو الجناة أو الضحايا في أماكن أخرى[2].

فنجد أن المشرع قد منح لقاضي التحقيق بناء على طلب من النيابة العامة أو من تلقاء نفسه سلطة اتخاذ تدابير تحفظية وأمنية طوال سير الإجراءات، بهدف حماية الأدلة وضمان تنفيذ العقوبة أو التعويضات المحتملة، فتشمل التدابير حجز الأموال والعائدات المتحصل عليها من الجريمة أو الوسائل المستعملة في ارتكابها[3]، وهو إجراء بالغ الأهمية بالنسبة إلى الجريمة الإلكترونية نتيجة قيام الجناة بإخفاء العائدات المتحصل عليها من الجريمة.

أولا: تمديد الاختصاص الإقليمي لقاضي التحقيق في جريمة القرصنة الالكترونية

اهتم المشرّع الجزائري بمواجهة الجرائم الخطيرة، وعلى رأسها الجريمة المتصلة بتكنولوجيا الإعلام والاتصال، من خلال إدخال تعديلات على قانون الإجراءات الجزائية، قصد تمكين أجهزة الضبط القضائي والجهات القضائية من وسائل إجرائية أكثر فعالية في البحث والتحري والتحقيق. ويظهر ذلك بوضوح من خلال توسيع الاختصاص الإقليمي لبعض الجهات المكلفة بالتحقيق، بما يسمح بملاحقة هذه الجرائم التي تتسم غالبًا بالطابع العابر للحدود أو الامتداد الجغرافي الواسع داخل التراب الوطني[4]، فنص بموجب المواد من **335 الى 342 من ق.إ.ج.ج** على الاختصاص الإقليمي لقضاة التحقيق لدى القطب الجزائي لمكافحة

---

[1] محمد حزيط، **مرجع سابق**، ص 324

[2] المادة 70 من نفس القانون "**يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد المتهمين أو المشتبه فيهم ارتكاب المساهمة في ارتكابها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب اخر، مالم ينص القانون على اختصاص اخر**"

[3] المادة 71 من نفس القانون "**يجوز لقاضي التحقيق، تلقائيا أو بناء على طلب النيابة العامة وطوال مدة الإجراءات، أن يأمر باتخاذ كل إجراء تحفظي أو تدبير أمن زيادة على حجز الأموال المتحصل عليها من الجريمة أو التي استعملت في ارتكابها**".

[4] عبد الرحمان خلفي، **مرجع سابق**، ص 343.

الجرائم المتصلة بتكنولوجيا الإعلام والاتصال يمتد إلى كامل الإقليم الوطني[1]، فيختص هذا القطب بالمتابعة والتحقيق في هذا النوع من الجرائم وكذا في الجرائم المتربطة بها، فيختص بالحكم في هذه الجرائم إذا كانت تشكل جنحة طبقا لنص المادة 335 من القانون[2]

ومن هذا المنطلق، اعتمد المشرع الجزائري آليات إجرائية استثنائية تهدف إلى تعزيز فعالية العدالة الجزائية، وذلك من خلال تمديد الاختصاص الإقليمي لكل من الضبطية القضائية ووكلاء الجمهورية وكذا قضاة التحقيق في بعض الجرائم الخطيرة، بما يتلاءم مع طبيعتها وتعقيدها.

ثانيا: توسيع صلاحيات أجهزة التحقيق

لم يقتصر التوسيع الإجرائي على الضبطية القضائية فحسب، بل امتد أيضًا إلى قضاة التحقيق، حيث أجاز المشرع تمديد اختصاصهم الإقليمي في بعض الجرائم ذات الخطورة الخاصة.

فقد نصت المادة **70من قانون الإجراءات الجزائية** على إمكانية تمديد الاختصاص المحلي لقاضي التحقيق إلى دوائر اختصاص محاكم أخرى، وذلك في الجرائم المتعلقة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ويختص قاضي التحقيق المتواجد بالقطب الجزائي الوطني بالتحقيق في الجرائم المرتبطة بالجرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات المؤسسات العمومية وجرائم تبييض الأموال والإرهاب والجرائم المرتبطة بالتشريع الخاص بالصرف .

يؤول اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في الملف المتواجد على مستوى المحكمة المختصة إقليميا سواء كان على مستوى التحريات الأولية أو المتابعة أو التحقيق القضائي فيتم التخلي عنه وجوبا للقطب الذي يتمسك باختصاصه هذا ما نصت عليه الماد **321 إلى 329**، كما يؤول الاختصاص إلى القطب الجزائي الوطني الاقتصادي والمالي وجوبا في حال تزامنه مع اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال طبقا لنص المادة **341 من نفس القانون**، ويؤول الاختصاص إذا تزامن القطب الجزائي الوطني لمكافحة الجرائم

[1] **المادة 336 فقرة 2** ق.إ.ج.ج.

[2] المادة 2/335 تنص على انه "**يقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو الية ذات صلة بتكنولوجيات الإعلام والاتصال**".

المتصلة بتكنولوجيا الإعلام والاتصال مع اختصاص القطب الجزائي لمكافحة الإرهاب والجريمة المنظمة عبر الوطنية وجوبا لهذا الاخير طبقا للمادة 342 منه[1] .

ومن خلال تحليل نص المادة ومقارنته بالاختصاص التقليدي لقاضي التحقيق فإن التعديل جاء بهدف التوجه التشريعي إلى تحقيق فعالية أكبر في مكافحة الجرائم المعقدة التي تتطلب تحقيقات موسعة قد تتجاوز الحدود الإقليمية للمحكمة المختصة، فضلاً عن تعزيز التنسيق بين مختلف الجهات القضائية المكلفة بمتابعة هذه الجرائم[2].

ثالثا: تمديد الاختصاص الإقليمي لغرفة الاتهام

تم تمديد الاختصاص الإقليمي لجهات الاتهام والتحقيق في الجرائم المعلوماتية بموجب قانون الإجراءات الجزائية الجزائري (لاسيما المادتين 37 مكرر و40 مكرر)، وذلك عبر نظام الاختصاص الإقليمي الموسع؛ حيث يخول لوكلاء الجمهورية وقضاة التحقيق العاملين ضمن الأقطاب القضائية المتخصصة ممارسة صلاحياتهم في المتابعة والتحقيق عبر دوائر قضائية متعددة قد تشمل كامل الإقليم الوطني. ويأتي هذا التمديد استثناءً من قواعد الاختصاص التقليدية لمواجهة الطبيعة العابرة للحدود الجغرافية لهذه الجرائم، مما يمنح هذه الجهات سلطة تنفيذ إجراءات تقنية، مثل التفتيش الإلكتروني واعتراض المراسلات كما أشرت في الفصل الأول لأساليب التحري الخاصة، بغض النظر عن مكان وجود النظام ألمعلوماتي أو خوادم البيانات داخل الدول[3].

الفرع الثالث: طرق اتصال قاضي التحقيق بالدعوى

إن مرحلة إحالة القضية إلى القضاء من أهم المراحل الإجرائية في الدعوى العمومية، إذ تنتقل خلالها القضية من مرحلة البحث والتحري إلى مرحلة مباشرة الخصومة القضائية أمام الجهات المختصة. وتختلف طرق الإحالة بحسب طبيعة الجريمة وخطورتها والإجراءات التي يحددها القانون، فقد تتم الإحالة عن طريق التكليف المباشر بالحضور أو وفق إجراءات المثول الفوري أو بناءً على أمر بالإحالة صادر

[1] عبد الرحمان خلفي، **مرجع سابق**، ص344.

[2] راجع **قانون الإجراءات الجزائية الجزائري**، المعدل والمتمم لاسيما النصوص المنظمة للاختصاص وقانون العقوبات فيما يتعلق بالاختصاص الإقليمي، مع تطبيقها على الجرائم المعلوماتية ذات الطابع العابر للحدود، **المواد 37 من ق.إ.ج**، تحدد الاختصاص المحلي لوكيل الجمهورية المادة 40 من نفس القانون وتؤكد نفس معايير الاختصاص بالنسبة لقاضي التحقيق

[3] **المادة 329 تتعلق باختصاص المحكمة (قسم الجنح).**

عن قاضي التحقيق بعد انتهاء التحقيق القضائي. ويهدف المشرع من خلال تنظيم هذه الطرق إلى ضمان حسن سير العدالة وتحقيق التوازن بين حقوق الدفاع ومتطلبات المتابعة الجزائية[1].

ويخول الاختصاص القضائي أهمية بالغة في مجال الفصل في القضايا، لأنه يحدد الجهة القضائية المخولة قانونا بالنظر في الدعوى، سواء من حيث نوع الجريمة أو مكان وقوعها أو صفة مرتكبها. وقد وضع المشرع قواعد دقيقة للاختصاص القضائي قصد تفادي تنازع الاختصاص وضمان عرض القضية أمام المحكمة المختصة قانونا، خاصة في الجرائم الحديثة كجرائم القرصنة الإلكترونية التي قد تتجاوز الحدود الإقليمية التقليدية، مما استدعى توسيع بعض قواعد الاختصاص لمواجهة خصوصية هذا النوع من الإجرام[2].

أولا: الإحالة عن طريق طلب افتتاحي لإجراء التحقيق

في قضايا الجرائم الإلكترونية، فان إحالة الدعوى إلى القضاء تكون عن طريق قاضي التحقيق أو الاستدعاء المباشر، باعتبارهما الطريقان الأكثر شيوعا ناهيك عن عدة صور إجرائية تتلاءم مع طبيعة الجريمة المعلوماتية وتعقيدها التقني، غير أن الإحالة عن طريق قاضي التحقيق تبقى الأكثر اعتمادا، نظرا لما تتطلبه من خبرات تقنية وإجراءات تحقيق معمقة كحجز الأنظمة المعلوماتية وتتبع المعطيات الرقمية والاستعانة بالخبرة الفنية.

كما يمكن للنيابة العامة إحالة بعض قضايا القرصنة الإلكترونية مباشرة إلى المحكمة عن طريق التكليف المباشر بالحضور أو وفق إجراءات المثول الفوري، إذا كانت الوقائع واضحة والأدلة الرقمية كافية ولا تستدعي تحقيقا قضائيا معمقا. وفي المقابل، قد يلجأ المتضرر إلى الادعاء المدني المباشر في الحدود التي يسمح بها القانون، خاصة إذا ترتب عن الجريمة ضرر شخصي مباشر.

إلا أن خصوصية الجرائم الإلكترونية وما تتميز به من طابع تقني وعابر للحدود تجعل التحقيق القضائي أكثر حضورا مقارنة بالجرائم التقليدية، لذلك منح المشرع سلطات أوسع للنيابة العامة وقاضي التحقيق في مجال البحث والتحري وجمع الأدلة الرقمية، بهدف ضمان فعالية المتابعة الجزائية وحماية الأنظمة المعلوماتية من الاعتداءات الإلكترونية .

[1] محمد حزيط، **مرجع سابق**، ص 472.

[2] عبد الرحمان خلفي، **مرجع سابق**، ص 457.

ثانيا: الإحالة عن طريق الادعاء المدني

الأصل أن التحقيق القضائي وجوبي في مواد الجنايات، أما في مواد الجنح، فيكون اختياريا ما لم ينص القانون على وجو بيته، كما يجوز إجراؤه في مواد المخالفات إذا طلبه وكيل الجمهورية.

لا يجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية أو جنحة متلبس بها.

ولقاضي التحقيق سلطة اتهام كل شخص ساهم، بصفته فاعلا أو شريكا، في الوقائع المحال تحقيقها إليه.

فإذا وصلت لعلم قاضي التحقيق وقائع لم يشر إليها في طلب إجراء التحقيق، تعيّن عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع.

ويتبع في حالة الشكوى المصحوبة بادعاء مدني ما نص عليه في المادة 147 وما يليها من هذا القانون.[1] يقوم قاضي التحقيق، وفقا للقانون، باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، وبالتحري عن أدلة الاتهام وأدلة النفي. وبعدها وتحرر نسخة عن هذه الإجراءات وكذلك عن جميع الأوراق، ويؤشر أمين ضبط التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل، وترقّم وتجرد جميع أوراق الملف بمعرفة أمين ضبط التحقيق أولا بأول حسب تحريرها أو ورودها لقاضي التحقيق.[2]

ثالثا: الاحالة في حالة التلبس أو الاجراءات الخاصة

وفي هذا السياق أوردت المادة 476 قانون الإجراءات الجزائية الحالات التي يكلف فيها المتهم بالحضور أمام المحكمة، والتي ذكرها على سبيل الحصر، غير أنه في الحالات التي لم يذكرها ومنها جريمة الدخول الغير مشروع أنه ينبغي الحصول على ترخيص من النيابة العامة للقيام بالتكليف المباشر بالحضور.

المطلب الثاني: الاختصاص القضائي والمحاكمة في جرائم القرصنة الإلكترونية

استحدث المشرع الجزائري نظاماً خاصاً للاختصاص القضائي يتمثل في إنشاء محاكم ذات اختصاص موسع ومحدد للنظر في بعض الجرائم المستحدثة، وعلى رأسها الجريمة الإلكترونية. وقد أُطلق على هذه

[1] المادة 140، **القانون 25-14**، مرجع سابق.

[2] المادة 141، **ق.إ.ج**، نفس المرجع.

الجهات تسمية الأقطاب الجزائية المتخصصة[1].وجاء هذا التنظيم بموجب المرسوم التنفيذي رقم 06-348، المعدل والمتمم بالمرسوم التنفيذي رقم 16-267، حيث نص على تصنيف بعض محاكم الدرجة الأولى كأقطاب جزائية متخصصة، مكلفة بالنظر في هذا النوع من الجرائم ذات الطبيعة التقنية والمعقدة. ويهدف هذا التخصيص إلى ضمان معالجة فعّالة لهذه القضايا من خلال إسنادها إلى هيئات قضائية ذات كفاءة وخبرة في مجال الجرائم الإلكترونية.

كما استحدث المشرع نظام الاختصاص الموسّع لبعض المحاكم، بحيث يمتد اختصاص كل محكمة منها إلى دوائر اختصاص محاكم أخرى، وذلك على مستوى عدة مجالس قضائية، وفقاً لما نصّت عليه المواد 2، 3، 4 و5 من المرسوم التنفيذي المشار إليه سابقاً.

الفرع الأول: إشكالات الاختصاص القضائي في جرائم القرصنة الالكترونية

بالنظر إلى الطبيعة الخاصة لجرائم القرصنة الإلكترونية، فقد أقر المشرع الجزائري قواعد خاصة لتحديد الاختصاص القضائي بالنظر إلى صعوبة تحديد مكان ارتكاب الجريمة في البيئة الرقمي وهو ما نصت عليه المادة 310 من قانون الإجراءات الجزائية على أن الاختصاص المحلي ينعقد عادة للمحكمة التي ارتكبت الجريمة في دائرة اختصاصها، أو التي يقيم فيها المتهم، أو التي تم فيها توقيف المجرم، الا ان القواعد العامة قد لا تكون كافية في الجرائم المعلوماتية، وذلك لأن هذه الجرائم غالباً ما تتم عبر الشبكات الإلكترونية التي تتجاوز الحدود الإقليمية للدولة، مما يجعل تحديد مكان وقوع الجريمة أمرا معقدا.

ولهذا السبب، منح المشرع اختصاصاً موسعاً لبعض الجهات القضائية، بحيث يمكن مباشرة إجراءات المتابعة والتحقيق في الجرائم المعلوماتية حتى ولو ارتكبت جزئياً خارج نطاق الاختصاص الإقليمي التقليدي، طالما أن آثارها أو نتائجها ظهرت داخل الإقليم الوطني طبقا للمادة 310 من قانون الاجراءات الجزائية[2].

أولا: صعوبات تحديد الاختصاص القضائي في الجرائم الالكترونية

إن تخصيص جهات قضائية متخصصة للنظر في الجرائم المعلوماتية يعكس إدراك المشرع لخطورة هذه الجرائم وتعقيدها. فهذه الجرائم غالباً ما تعتمد على وسائل تقنية متطورة، وتتطلب خبرة فنية عالية لفهم أساليب ارتكابها وجمع الأدلة الرقمية المرتبطة بها .كما أن التحقيق في هذا النوع من الجرائم يستلزم التعاون بين عدة جهات، مثل :الأجهزة الأمنية المختصة بالجرائم الإلكترونية .خبراء تقنيين في مجال المعلوماتية .

[1] عبد الله أوهابية، **شرح قانون الإجراءات الجزائية الجزائري**، الجزء الثاني، الجزائر، دار هومة، 2017-2018، ص61.
[2] المادة **310** من قانون الاجراءات الجزائية.

الهيئات القضائية المتخصصة .ومن ثم فإن إنشاء أقطاب قضائية متخصصة يساهم في تعزيز فعالية العدالة الجنائية في مواجهة التهديدات الرقمية المتزايدة[1].

أ_ اختلاف التشريعات بين الدول:

تختلف التشريعات الجنائية والإجرائية من دولة إلى أخرى نتيجة غياب قواعد قانونية موحدة تُعتمد على المستوى الدولي، الأمر الذي يطرح صعوبات عملية أمام الجهات القضائية عند معالجة الجرائم ذات الطابع العابر للحدود، ويظهر هذا الاختلاف من خلال تجريم بعض الأفعال في أنظمة قانونية معينة مقابل عدم الاعتراف بها كجرائم في دول أخرى، إضافة إلى تباين التكييف القانوني للفعل ذاته بحسب التشريع المطبق. ويترتب عن ذلك في العديد من المرات إفلات بعض الجناة من المتابعة والعقاب بسبب تعارض القوانين واختلاف نطاق التجريم بين الدول

ب_ الطبيعة العابرة للحدود للجرائم الالكترونية

تثير الجرائم المعلوماتية صعوبات قانونية بسبب إمكانية ارتباطها بأكثر من دولة في الوقت نفسه، وهو ما يؤدي إلى تنازع القوانين الجزائية، ويظهر ذلك عندما تكون الجريمة صالحة لتطبيق قوانين عدة دول، بسبب اختلاف مكان ارتكاب الجريمة أو جنسية الجاني أو المجني عليه كما أن بعض الأفعال قد تعتبر جريمة في دولة، بينما لا تعاقب عليها دولة أخرى، وقد يختلف التكييف القانوني للفعل نفسه من نظام قانوني إلى آخر. وهذا الوضع يؤدي أحيانا إلى صعوبة ملاحقة الجناة أو تسليمهم، رغم وجود اتفاقيات دولية للتعاون القضائي وتبادل المعلومات وتسليم المجرمين[2].

غير أن بعض الدول ترفض تسليم رعاياها بحجة حماية سيادتها الوطنية[3]

كما تخضع هذه الجرائم، شأنها شأن باقي الجرائم، لقواعد الاختصاص القضائي التي تهدف إلى تحديد الجهة القضائية المختصة والقانون الواجب التطبيق. ولقيام الركن الشرعي للجريمة المرتكبة عبر الوسائل التكنولوجية الحديثة، يشترط أن يكون النص القانوني المجرّم للفعل سابقا لارتكابه، تطبيقا لمبدأ الشرعية الجنائية، غير أن هذا الشرط لا يكفي لوحده، إذ يتعين أيضا تحديد مكان وقوع الفعل الإجرامي، لما لذلك من أهمية في تحديد الاختصاص القضائي والقانون الواجب التطبيق.

---

[1] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، مرجع سابق 242.

[2] سيد علي السيد محمد، **مرجع سابق**، ص 117.

[3] حسين طاهري، **الجرائم الإلكترونية**، ص 271.

وتبرز هذه الإشكالية بشكل خاص في الجرائم المعلوماتية، نظرا لطبيعتها العابرة للحدود وصعوبة تحديد مكان ارتكابها بدقة.

ج_ صعوبة تحديد مكان ارتكاب الجريمة

يطرح تطبيق تحديد مكان ارتكاب الجريمة في الجرائم الإلكترونية صعوبات، لأن الجريمة المعلوماتية ترتكب عبر شبكة افتراضية ولا ترتبط دائما بمكان مادي واضح، فقد يكون الجاني في دولة والخادم الإلكتروني في دولة أخرى والنتيجة الإجرامية في دولة ثالثة[1]

ثانيا: قواعد الاختصاص القضائي في الجرائم الالكترونية

يتحدد الاختصاص الإقليمي أو الصلاحية المكانية بتطبيق قانون الدولة على الجرائم التي تقع داخل إقليمها، سواء كان الجاني أو الضحية أجنبيا أو وطنيا. وهذا المبدأ يعد من أهم قواعد الاختصاص الجزائي لأنه مرتبط بسيادة الدولة على إقليمها.

أ_إقليمية القوانين الجزائية

يقوم الاختصاص الإقليمي للقانون الجنائي على مبدأ خضوع كل جريمة تقع داخل حدود الدولة لأحكام قانونها الوطني، دون الاعتداد بجنسية مرتكب الجريمة أو الضحية. غير أن التطور المتسارع للجريمة، خاصة الجرائم العابرة للحدود، أدى إلى تجاوز آثارها للنطاق الإقليمي التقليدي، مما فرض على الدول تعزيز آليات التعاون القضائي فيما بينها. وقد تجسد ذلك من خلال إبرام اتفاقيات دولية تنظم إجراءات التعاون في المسائل الجزائية، لاسيما ما يتعلق بتسليم المطلوبين وتبادل المساعدة القضائية، بما يحقق مكافحة فعالة للجريمة مع احترام سيادة كل دولة واختصاصها القضائي[2]

ومن ثم، فإن مسألة سريان القانون الجنائي من حيث المكان تكتسي أهمية بالغة، حيث تخضع لمجموعة من المبادئ الأساسية التي يعتمدها المشرع لتحديد نطاق تطبيق النص الجنائي. وتتمثل هذه المبادئ في أربعة: مبدأ الإقليمية، ومبدأ الشخصية، ومبدأ العينية، ومبدأ العالمية.

[1] محمد حزيط، **مرجع سابق**، ص 479

2 عبيد صالح حسن، **سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية**، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، المجلد 24، العدد 95، 2015 ص 38.

ب-مبدأ الصلاحية الإقليمية

يقوم هذا الاتجاه القانوني على منح الدولة حق متابعة رعاياها إذا ارتكبوا أفعالاً مجرّمة خارج حدودها، وذلك لمنع إفلاتهم من العقاب بمجرد مغادرتهم لإقليم الدولة التي وقع فيها الفعل. كما توسع بعض التشريعات في نطاق هذا الاختصاص ليشمل أيضاً الجرائم التي يكون ضحيتها أحد مواطني الدولة، حتى ولو ارتكبت بالكامل في الخارج.

ولا يشترط دائماً أن تقع جميع عناصر الجريمة داخل إقليم الدولة حتى ينعقد اختصاصها القضائي[1]، بل يكفي أحياناً أن يتحقق جزء من السلوك الإجرامي أو تظهر بعض نتائجه داخل إقليمها حتى تتمكن من تحريك الدعوى ومباشرة المتابعة الجزائية.

غير أن تطبيق هذه القواعد يثير صعوبات كبيرة في مجال الجرائم المعلوماتية، خاصة جرائم القرصنة الإلكترونية، لأن هذا النوع من الجرائم يتم عبر فضاء رقمي غير ملموس ولا يرتبط بمكان مادي محدد. فالمخترق قد يوجد في دولة، والخادم الإلكتروني في دولة ثانية، بينما يظهر الضرر في دولة أخرى، وهو ما يجعل تحديد مكان ارتكاب الجريمة والجهة القضائية المختصة أمراً معقداً. كما أن الطابع التقني لهذه الجرائم وصعوبة اكتشاف آثارها الرقمية يزيدان من تعقيد إجراءات البحث والتحقيق والمتابعة القضائية[2].

ج_مبدأ الصلاحية الشخصية

ويطلق عليها مصطلح الصلاحية الشخصية أو مبدأ شخصية النص الجنائي في جريمة القرصنة الإلكترونية بمعنى تطبيق قانون الدولة على الجرائم التي يرتكبها مواطنوها خارج إقليمها. وتأخذ عدة دول بهذا المبدأ من أجل متابعة رعاياها حتى ولو ارتكبوا الجريمة في الخارج.

كما أن بعض الدول، مثل فرنسا، توسع هذا الاختصاص ليشمل الجرائم المرتكبة ضد مواطنيها خارج إقليمها. يقوم الاختصاص الشخصي على فكرة منح الدولة حق متابعة بعض الجرائم التي تقع خارج حدودها الإقليمية متى ارتبطت هذه الجرائم بشخص تجمعه بالدولة رابطة قانونية معينة، كالجنسية أو الإقامة. فالعبرة هنا لا تكون بمكان وقوع الجريمة، وإنما بصفة الجاني أو الضحية وعلاقتهما بالدول[3].

ويختلف هذا النوع من الاختصاص عن الاختصاص الإقليمي الذي يقوم أساسًا على مكان ارتكاب الجريمة، إذ تباشر الدولة اختصاصها الإقليمي على كل فعل إجرامي يقع داخل حدودها البرية أو البحرية

---

[1] حسين بن سعيد الغافري، **السياسة الجنائية في مواجهة الانترنت**، الطبعة الأولى، دار النهضة العربية، القاهرة، 2009، ص 577-578

[2] حسين طاهري، إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية، المحاكمة الإلكترونية، **مرجع سابق**، ص 273.

[3] أمير فرج يوسف، البلطجة الإلكترونية، مرجع سابق، ص 226.

أو الجوية، بغض النظر عن جنسية مرتكبه. أما الاختصاص الشخصي فيرتكز على الصلة القانونية التي تجمع الشخص بالدولة، لذلك قد يمتد تطبيق القانون الجنائي الوطني إلى أفعال ارتكبت خارج الإقليم[1] ويهدف هذا النظام إلى سد الفراغ الذي قد يظهر عند تعذر معاقبة بعض الجرائم وفق مبدأ الإقليمية وحده، خاصة عندما يفلت الجاني من العقاب بسبب وقوع الجريمة خارج الدولة.

وللاختصاص الشخصي صورتان أساسيتان، تتمثل الصورة الأولى في الاختصاص الشخصي الإيجابي، ويقصد به حق الدولة في معاقبة مواطنيها عن الجرائم التي يرتكبونها في الخارج، حتى وإن وقعت هذه الأفعال خارج حدودها[2]. أما الصورة الثانية فهي الاختصاص الشخصي السلبي، ويقصد به حق الدولة في متابعة الجرائم التي يكون ضحيتها أحد رعاياها، ولو كان الفاعل أجنبيًا وارتكبت الجريمة خارج الإقليم الوطني[3].

ورغم أهمية هذا المبدأ في حماية مصالح الدولة ورعاياها، إلا أن الاختصاص الشخصي السلبي تعرض لانتقادات من بعض الأنظمة القانونية، خاصة الدول الأنكلوسكسونية، التي رأت أن معاقبة أجنبي عن أفعال ارتكبها خارج إقليم الدولة يعد توسعًا في الاختصاص الجنائي ويمس بمبدأ سيادة الدول الأخرى[4].

اتخذ المشرع الجزائري نفس نهج المشرع الفرنسي فاعتمد على مبدأ شخصية النص الجنائي من خلال المادة 3 من قانون العقوبات الجزائري التي تنص على انه "يطبق قانون العقوبات الجزائري على كافة الجرائم التي ترتكب في أراضي الجمهورية كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائرية طبقا لأحكام قانون الإجراءات الجزائية "[5].

غير أن تطبيق الصلاحية الشخصية في الجرائم الإلكترونية يواجه صعوبة عملية، تتمثل في تحديد الهوية الحقيقية للجاني، لأن أغلب مرتكبي الجرائم المعلوماتية يستعملون أسماء وهمية أو حسابات مستعارة، مما يجعل معرفة جنسيتهم الحقيقية أمرا معقدا في كثير من الحالات [6].

---

[1] **نفس المرجع**، ص 224.

[2] تنص المادة 113 فقرة 6 من قانون العقوبات الفرنسي "**يطبق القانون الفرنسي على كل جناية يرتكبها فرنسي خارج إقليم الجمهورية ويطبق هذا القانون أيضا على الجنح التي يرتكبها فرنسي خارج فرنسا إذا كانت الوقائع المكونة لها معاقب عليها في قانون الدولة التي ارتكب فيها وتطبق أحكام هذه المادة حتى ولو كان المتهم قد اكتسب الجنسية الفرنسية بعد ارتكاب الواقعة المنسوبة إليه**.

[3] المادة **113فقرة-7** من نفس القانون

[4] أمير فرج يوسف، **نفس المرجع**، ص 225.

[5] المادة **03 من قانون العقوبات الجزائري**.

[6] حسين طاهري، **الجرائم الإلكترونية**، مرجع سابق، ص 449

د_ مبدأ الصلاحية الذاتية

ويسميها البعض بالاختصاص الوقائي أو مبدأ العينية ويقصد به مباشرة الدولة لاختصاصها القضائي بالنسبة للجريمة التي ارتكبت خارج إقليمها والتي مست بمصالحها الحيوية بغض النظر عن جنسية مرتكبيها، ويمكن أن يرتكب هذا النوع من الجرائم في العالم الافتراضي بوسائل معلوماتية، وقد نص المشرع الفرنسي من خلال نص المادة 10/113 من قانون العقوبات الفرنسي على تطبيق قانون العقوبات الفرنسي على جميع الجنايات والجنح التي تقع في الخارج وتشكل اعتداء على المصالح الأساسية للأمة والمنصوص عليها في الباب الأول من الكتاب الرابع[1].

كما أن المشرع الجزائري أقر بمبدأ عينية النص الجنائي، والذي يسمح للدولة بممارسة اختصاصها القضائي بشأن بعض الجرائم الخطيرة حتى وإن ارتكبت خارج الإقليم الوطني ومن طرف أجانب، ويهدف هذا المبدأ إلى حماية المصالح الجوهرية للدولة ومكافحة الجرائم التي تتجاوز أثارها الحدود الوطنية.

نصت المادة **588 من قانون الإجراءات الجزائية** على إمكانية متابعة ومحاكمة الأجنبي الذي يرتكب خارج الجزائر جناية أو جنحة تمس أمن الدولة الجزائرية متى تم توقيفه داخل الإقليم الجزائري ولم يتم تسليمه إلى دولة أخرى، ويفهم من ذلك أن المشرع منح القضاء الجزائري صلاحية النظر في بعض الجرائم ذات الطابع الخطير حماية للمصلحة العامة[2]

كما أكد المشرع أيضا هذا التوجه من خلال بعض نصوص قانون العقوبات، ومن بينها المادة 345 من نفس القانون التي تقرر تطبيق العقوبات المنصوص عليها قانونا على الأفعال التي تستهدف أمن الدولة

---

[1] المادة 113 من القانون الفرنسي" **يطبق قانون العقوبات الفرنسي على جميع الجنايات والجنح التي تقع في الخارج وتشكل اعتداء على المصالح الأساسية للأمة والمنصوص عليها في الباب الأول من الكتاب الرابع وكذا على جرائم تقليد وتزوير أختام الدولة وتزييف العملة المعدنية أو الورقية أو السندات العامة والمعاقب عليها وفقا للمواد (442-1، 443-2، 444-1) وعلى كل جناية أو جنحة ترتكب ضد أعضاء البعثات الدبلوماسية أو القنصلية الفرنسية أو أماكنها خارج الجمهورية**"

[2] تنص المادة 588 من قانون الإجراءات الجزائري" **كل أجنبي ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو بصفة شريك في جناية أو جنحة ضد سلامة الدولة الجزائية أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر تجوز متابعته ومحاكمته وفقا لأحكام القانون الجزائري إذا ألقى القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها** ".

أو تمس بمصالحها الأساسية، بما يعكس رغبة المشرع في توسيع نطاق الحماية الجنائية عدم حصرها داخل الحدود الإقليمية فقط[1]

هـ_ مبدأ عالمية النص الجنائي في جريمة القرصنة الإلكتروني

يسميه البعض بالاختصاص الشامل ويقصد به تطبيق القانون الجنائي للدولة على كل جريمة يقبض على مرتكبها في إقليم الدولة مهما كان الإقليم الذي ارتكبت فيه ومهما كانت جنسية مرتكبها، بمعنى يكفي أن يتم القبض على الجاني في إقليم الدولة حتى يخضع لقانونها، إلا انه قد تثار إشكالية ملاحقة نفس المجرم على ذات الجرم مرتين، فيتعرض للملاحقة والمحاكمة ذاتها أمام أكثر من دولة، وهو ما يؤدي إلى ازدواجية المتابعة الجزائية وتعارض الأحكام القضائية[2].

إلا انه لتفادي هذه الصعوبات، تتجه التشريعات الحديثة إلى تعزيز التعاون والتنسيق بين السلطات القضائية في الدول المعنية، من خلال تبادل المعلومات وإعلام الجهات القضائية المختصة بالإجراءات المتخذة، وذلك لتجنب تكرار المحاكمات وضمان صدور حكم واحد بشأن الجريمة نفسها[3].

مبدأ الاختصاص العالمي هو المبدأ الأكثر تلاءما مع طبيعة الجريمة المعلوماتية، باعتبارها جرائم عابرة للحدود يصعب أحيانا تحديد مكان ارتكابها بدقة، كما أن أثارها قد تمتد إلى أكثر من دولة في الوقت نفسه، لذلك أصبح توسع نطاق تطبيق هذا المبدأ ضروريا لمواجهة التطور المستمر لهذا النوع من الجرائم ومنع إفلات مرتكبيها من العقاب.

الفرع الثاني: اختصاص الجهات القضائية الجزائرية في مكافحة جرائم القرصنة الالكترونية

يخضع الاختصاص الإقليمي للقواعد العامة المنصوص عليها في قانون إ.ج ج، فقد نصّت المادة 467 من قانون الإجراءات الجزائية على أن المحكمة تختص بالنظر في الجنح والمخالفات التي يعاقب عليها القانون بالحبس لمدة تزيد عن شهرين وغرامة تفوق 2.000 دينار، ما لم يرد نص خاص في قوانين أخرى، أما المادة 389 من القانون نفسه، فقد حدّدت الاختصاص الإقليمي الموسّع للمحكمة، حيث أجازت

[1] تنص المادة 345 من القانون العقوبات الجزائري " **تطبق العقوبات المنصوص عليها في المواد 342_ 344 حتى ولو كانت بعض الأفعال المكونة لعناصر الجريمة قد وقعت خارج أراضي الجمهورية.**

[2] **حسين طاهري، مرجع سابق، ص 274.**

[3] أمير فرج يوسف، **البلطجة الإلكترونية**، مرجع سابق، ص 231.

نظر المحكمة في الجنحة التي وقعت في دائرة اختصاصها، أو في مكان إقامة أحد المتهمين أو شركائه، أو في مكان القبض على أحدهم[1].

لا تختص محكمة محل حبس المحكوم عليه بالنظر في الدعوى إلا إذا تم القبض على المعني لسبب آخر، وذلك وفقاً للأوضاع المنصوص عليها في المادتين 716 و717 من قانون الإجراءات الجزائية[2]. كما تختص المحكمة كذلك بالنظر في الجنح والمخالفات غير القابلة للتجزئة أو المرتبطة، وتختص المحكمة التي ارتكبت في نطاق دائرتها المخالفة أو المحكمة الموجودة في مكان إقامة مرتكبها بالنظر في تلك المخالفة، كما يجوز تمديد الاختصاص المحلي للمحكمة المختصة في قضايا المخدرات عن طريق التنظيم، ليشمل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والجريمة المنظمة عبر الحدود الوطنية، وجرائم تبييض الأموال، والجرائم المالية المعقدة، والجرائم المتعلقة بالتشريع الخاص بالصرف[3].

أولا: الأقطاب الجزائية المتخصصة في جريمة القرصنة الالكترونية

وحسب المرسوم التنفيذي رقم 348/06 المؤرخ في 10 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق عبر كامل التراب الوطني، تم تحديد المحاكم المعنية بهذا التوسيع **كما يلي:**

أ_القطب الجزائي لمحكمة سيدي أمحمد بالجزائر، تم توسيع اختصاصه المحلي، بما في ذلك وكيل الجمهورية وقاضي التحقيق، ليشمل دوائر اختصاص المجالس القضائية في كل من البليدة، بومرداس، تيبازة، المدية، البويرة، المسيلة، الجلفة، تيزي وزو، الشلف، والأغواط.

ب_القطب الجزائي لمحكمة قسنطينة، مُدد اختصاصه المحلي كذلك بالنسبة لوكيل الجمهورية وقاضي التحقيق، ليشمل جميع المحاكم التابعة للمجالس القضائية في أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، قالمة، عنابة، سكيكدة، الطارف، خنشلة، سوق أهراس، ميلة، وبرج بوعريريج.

---

[1] المادة 467، 389، **مرجع نفسه.**

[2] المادتين 716، 717 من **قانون الإجراءات الجزائية.**

[3] المادة 2 من المرسوم التنفيذي رقم 348/06 المعدل والمتمم بموجب المرسوم التنفيذي رقم 267/16.

مكان القبض على أحدهم[1].

ج_القطب الجزائي لمحكمة ورقلة: تم تمديد الاختصاص المحلي لمحكمة ورقلة ووكيل الجمهورية وقاضي التحقيق بها إلى دوائر اختصاص أخرى تشمل جميع المحاكم التابعة للمجالس القضائية التالية: ورقلة، أدرار، تمنراست، النعامة، بشار، البيض، بسكرة، الوادي، غرداية.

د_القطب الجزائي لمحكمة وهران: تم توسيع الاختصاص المحلي لمحكمة وهران ولوكيل الجمهورية وقاضي التحقيق التابع لها إلى دوائر اختصاص جميع المحاكم التابعة للمجالس القضائية التالية: وهران، تلمسان، عين تموشنت، سيدي بلعباس، مستغانم، معسكر، غليزان، سعيدة، الشلف، عين الدفلى، تيارت.

مع الإشارة إلى أنه وبموجب الأمر 20/04 المعدل والمتمم للأمر رقم 66/155 المتضمن قانون الإجراءات الجزائية، تم استحداث القطب الجزائي المالي والاقتصادي، حيث جاء ضمن الباب الرابع من هذا القانون موسوم ب: القطب الجزائي الاقتصادي والمالي، المادة 16 مكرر منه تنص على إنشاء هذا القطب الجزائي على مستوى محكمة ذات اختصاص محلي ونوعي في مكافحة الجريمة الاقتصادية والمالية. وتم تمديد اختصاص وكيل الجمهورية وقاضي التحقيق لدى القطب الجزائي الاقتصادي والمالي وتوسيع هذا الاختصاص ليشمل التراب الوطني.

ثانيا: تعريف القطب الجزائي المتخصص

لم يعرف المشرع الجزائري القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وإنما اكتفى بالنص على إنشائه فقط، اين استحدثه المشرع الجزائري في إطار تحديث المنظومة القضائية وتعزيز فعالية السياسة الجنائية في مواجهة الجرائم الإلكترونية .وقد تم إنشاء هذا القطب بموجب الأمر رقم 21-11 المؤرخ في 25 أوت 2021 المعدل والمتمم لقانون الإجراءات الجزائية، حيث نص المشرع على إنشاء أقطاب جزائية متخصصة على مستوى مجلس قضاء الجزائر، تتولى مهمة المتابعة والتحقيق والفصل في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال [2].

وينظر القطب الجزائي في الجرائم التي يختص بالنظر والفصل فيها بموجب المادة 211مكرر 22 من القانون155 /66 المتضمن قانون الإجراءات الجزائية (الملغى) والذي نص على إنشاء قطب جزائي وطني متخصص في المتابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى مستوى

[1] المواد 389،467 **نفس المرجع.**

[2] الامر رقم 21-11 المؤرخ في 25 أوت 2021

محكمة مقر مجلس قضاء الجزائر، كما نص على الأحكام المتعلقة إجراءات المتابعة و كيفية إحالة الملفات إلى جهات المتابعة و التحقيق القطب.[1]

غير أنه ومع تعديل قانون الإجراءات الجزائية تم تعديل نص المادة واستحداث المادة 367 والتي تنص على: " مع مراعاة أحكام الفقرة 2 من المادة 335 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب، حصريا، بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه، وكذا الجرائم المرتبطة بها:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني،
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع،
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية،
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية،
- جرائم الاتجار بالبشر أو بالأعضاء البشرية أو بتهريب المهاجرين،
- جرائم التمييز وخطاب الكراهية".[2]

ويهدف هذا التوجه التشريعي إلى تحقيق عدة غايات أساسية، من بينها:

- تعزيز التخصص القضائي في مجال الجرائم الإلكترونية،
- تحسين فعالية التحقيقات في الجرائم التي تتطلب خبرة تقنية عالية.
- توحيد الاجتهاد القضائي في القضايا ذات الطبيعة المعلوماتية؛ ضمان سرعة وفعالية الإجراءات القضائية المرتبطة بهذا النوع من الجرائم .

---

[1] بنياحي إبراهيم، **القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية لمكافحة الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية**، المجلد 18، العدد 03، سنة 2025، ص 479.

[2] المادة 337 من القانون 25-14، **مرجع سابق**.

ويختص هذا القطب بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، سواء تعلق الأمر بجرائم الاعتداء على الأنظمة المعلوماتية، أو الجرائم التي يتم ارتكابها باستعمال الوسائل الإلكترونية والشبكات الرقمية .

وفقا لتعريف المشرع الجزائري لهذا النوع من الجرائم وبالإضافة للوسائل المعتمدة والتي حددها وفق ما ورد في المادة 335 فقرة 3 من قانون الإجراءات الجزائية، ويشمل اختصاص القطب الجزائي الوطني مجموعة من الجرائم التي تمس بمصالح الدولة والمجتمع، ومن بينها على وجه الخصوص :الجرائم التي تمس بأمن الدولة أو الدفاع الوطني،

الجرائم المرتبطة بالإرهاب وتمويله عبر الوسائل الإلكترونية، الجرائم المنظمة التي تستعمل الوسائل الرقمية في ارتكابها، الجرائم المرتكبة عبر الشبكات الاجتماعية أو المواقع الإلكترونية والتي قد تمس بالأمن العام، كما يمتد اختصاص هذا القطب إلى النظر في الجرائم التي تتم عبر الفضاء الرقمي والتي قد يكون لها أثر واسع الانتشار بين أفراد المجتمع، مثل نشر أو ترويج الأخبار الكاذبة بين الجمهور إذا كان من شأنها المساس بالأمن أو السكينة العامة. وتكمن خطورة هذا النوع من الجرائم في قدرته على التأثير السريع والواسع في الرأي العام، نظراً للانتشار الكبير لوسائل التواصل الاجتماعي والمنصات الرقمية، الأمر الذي قد يؤدي إلى زعزعة الاستقرار الاجتماعي أو المساس بالنظام العام .كما يشمل اختصاص القطب أيضاً الجرائم المتعلقة بنشر أو ترويج أنباء مغرضة من شأنها المساس بالنظام العام أو بالأمن العمومي، لاسيما إذا تم ارتكابها عبر الوسائط الإلكترونية أو المنصات الرقمية التي تتيح انتشار المعلومات بسرعة فائقة[1].

إن استحداث هذا القطب الجزائي المتخصص يعكس إدراك المشرع الجزائري للطبيعة المعقدة للجرائم الإلكترونية كما أشرنا سابقا في الخصائص المميزة لهذه الأخيرة عن غيرها من الجرائم.

أ_ الاختصاص النوعي للجهات القضائية المختصة بنظر الجرائم الالكترونية

تم تحديد الاختصاص النوعي للأقطاب الجزائية المتخصصة، حيث تم حصر هذا الاختصاص وذلك في نوع معين من الجرائم التي حددها المشرع على سبيل الحصر، من الجرائم المتعلقة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال

[1] المواد 582، 584 من القانون 14/25

والإرهاب والرشوة، وكذا جرائم الفساد بمقتضى التعديل الذي أجري في سنة على القانون الخاص بالوقاية من الفساد ومكافحته.[1]

كما أشار إليه المشرع الجزائري في القسم السابع مكرر من قانون العقوبات، المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى المادة 394 مكرر 7، حيث أدرج المشرع الأفعال المجرمية التي تمس بأنظمة المعالجة الالية للمعطيات[2].

ب_ الاختصاص الإقليمي (المحلي) للقطب الجزائي المتخصص

يمتد الاختصاص الإقليمي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى كامل الإقليم الوطني، حيث نصت المادة 336 من قانون الإجراءات الجزائية رقم 25-14 على أن وكيل الجمهورية لدى هذا القطب وقاضي التحقيق ورئيسه يمارسون صلاحياتهم على كامل الإقليم الوطني، والتي تشمل[3]:

*جرائم المخدرات.

*الجريمة المنظمة عبر الحدود الوطنية.

*الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات،

*جرائم تبييض الأموال.

*جرائم الإرهاب.

*والجرائم المرتبطة بتشريع الصرف.

فإن ضابط الشرطة القضائية يُبلغ فورًا وكيل الجمهورية لدى المحكمة المختصة إقليميًا، ويرسل الملف مرفقًا بإجراءات التحقيق. بعد ذلك، يقوم وكيل الجمهورية مباشرة بإرسال نسخة ثانية من الملف إلى وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع.

---

[1] ميرفت، **مرجع سابق**، 165.

[2] ميرفت، **نفس المرجع**، ص 164.

[3] المادة 37، **الأمر 20/ 04**.

أما المادة 43، فقد نصّت على أنه يحق لوكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الموسع، وبعد أخذ رأي النائب العام، الشروع في الإجراءات فورًا، متى تبين له أن الجريمة تدخل ضمن اختصاص المحكمة المختصة وفقًا للمادة 58 من القانون[1].

وفي هذه الحالة، يتولى ضباط الشرطة القضائية العاملون ضمن دائرة اختصاص المحكمة تنفيذ التعليمات مباشرة من وكيل الجمهورية لدى الجهة القضائية المختصة.

الفرع الثالث: إجراءات المحاكمة في جرائم القرصنة الإلكترونية

تعتبر مرحلة المحاكمة مرحلة جوهرية في الدعوى العمومية، إذ يتم فيها عرض ملف القضية أمام جهة الحكم للفصل فيه وفقًا لما يقرره القانون، بعد استكمال مراحل البحث والتحري والتحقيق، وفي مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تكتسي هذه المرحلة طابعا خاصا نتيجة الطبيعة التقنية للأدلة الرقمية وتعقيدها، مما يستوجب تكييف إجراءات المحاكمة مع خصوصية هذا النوع من الإجرام.[1]

إن محاكمة الجرائم المعلوماتية مثلها مثل محاكمة الجرائم التقليدية من حيث احترام المبادئ الأساسية للمحاكمة العادلة، مثل مبدأ العلنية والشفوية وحق الدفاع والمواجهة بين الخصوم، وتقوم المحكمة خلال الجلسة بسماع أقوال المتهم والشهود، ومناقشة الأدلة المعروضة، كما يمكنها الاستعانة بالخبراء المختصين في المجال التقني لتوضيح المسائل الفنية المرتبطة بالجريمة المعلوماتية[2].

وتشمل إجراءات المحاكمة كذلك مناقشة محاضر الضبط القضائي، والاستماع إلى رجال الضبط القضائي باعتبارهم شهودا في الدعوى[2]، ثم تمنح المحكمة للأطراف فرصة تقديم ملاحظاتهم والرد على ما أثير أثناء الجلسة، مع إعطاء الكلمة الأخيرة للمتهم قبل اختتام المرافعات وبعد ذلك تنسحب هيئة المحكمة للمداولة ثم تصدر حكمها في جلسة علنية.

إن المشرع الجزائري، من خلال التعديلات الأخيرة لقانون الإجراءات الجزائية، سعى إلى تعزيز فعالية المحاكمة في الجرائم المعلوماتية، عبر تنظيم وسائل الإثبات الرقمية وتدعيم دور الخبرة التقنية وضمان حقوق الدفاع في مواجهة الدليل الإلكتروني .

---

[1] الأمر رقم 20-04 المؤرخ في 30 أوت 2020، المعدّل والمتمّم للأمر رقم 66-155 المؤرخ في 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 51، الصادر بتاريخ 31 أوت 2020، ص 9 وما يليها.

[2] طاهري حسين، **الجرائم الإلكترونية**، مرجع سابق، ص 448.

تقوم المحاكمة في الجرائم المعلوماتية على مبدأ أساسي يتمثل في عرض الدليل الإلكتروني أمام القاضي بطريقة تمكنه من الإحاطة بمضمونه وفهمه، وهو ما يختلف عن الأدلة التقليدية التي تكون مادية ومباشرة.

فالدليل الرقمي غالبًا ما يكون في شكل بيانات أو سجلات أو رسائل إلكترونية أو معطيات مخزنة داخل أنظمة معلوماتية، مما يستوجب إعادة تقديمه في شكل قابل للعرض والمناقشة أمام المحكمة.[4] وفي الجرائم الإلكترونية تظهر أهمية الدليل الرقمي بشكل أكبر، لذلك يجب عرض الأدلة بطريقة واضحة ومبسطة حتى يسهل على القاضي فهمها، خاصة أن القاضي ليس بالضرورة خبيرا في مجال الإعلام الآلي، ولهذا يلتزم أطراف الدعوى وخاصة الدفاع والنيابة، بتقديم الحجج والوثائق التقنية بصورة دقيقة ومنظمة، مع تحضير الأسئلة التي توجه للخبراء أو الشهود أو المتهمين أثناء المحاكمة

أولا: خصوصية إجراءات المحاكمة في جرائم القرصنة الإلكترونية

إن مسألة تحديد المحكمة المختصة بالنظر في الجرائم المعلوماتية، خاصة جرائم القرصنة الإلكترونية، قد أحدثت نقاشًا فقهيًا واسعًا بسبب الطبيعة العابرة للحدود التي تتميز بها هذه الجرائم وصعوبة تحديد مكان ارتكابها بدقة. لذلك اهتم الفقه بوضع معايير تساعد على تحديد الجهة القضائية المختصة والقانون الواجب التطبيق على هذا النوع من الجرائم.

وفيما يتعلق بتحديد المحكمة المختصة، اعتمدت أغلب التشريعات على معيار الاختصاص المكاني، الذي يمنح الاختصاص لمحاكم الدولة التي وقعت الجريمة داخل إقليمها كليًا أو جزئيًا. ويعد هذا المعيار الأكثر شيوعًا لارتباطه بمبدأ إقليمية القانون الجنائي.

كما ظهر اتجاه فقهي يدعو إلى الأخذ بمعيار القانون الأكثر ملائمة، ويقصد به تطبيق القانون الذي يكون أكثر قدرة على تحقيق العدالة ومواجهة الجريمة بالنظر إلى ظروفها ونتائجها. في حين يرى اتجاه آخر ضرورة الاعتماد على معيار مكان ارتكاب الفعل الإجرامي أو المكان الذي ظهرت فيه النتيجة الإجرامية، خاصة في الجرائم الإلكترونية التي قد تتعدد فيها أماكن التنفيذ والضرر في وقت واحد.

أما بالنسبة للقانون الواجب التطبيق، فإن الأصل يتمثل في تطبيق مبدأ الإقليمية، حيث تختص محاكم الدولة بالنظر في الجرائم التي تقع كلها أو جزء منها داخل إقليمها، ولو كان مرتكب الجريمة أجنبيًا. ووفقًا لذلك، فإن القضاء الجزائري يختص بالفصل في الجرائم المعلوماتية متى تحقق جزء من النشاط الإجرامي أو نتج أثره داخل الإقليم الجزائري[1]، وذلك حماية للنظام العام ولمصالح الدولة والأفراد، وهو ما سوف نتطرق إليه من خلال الفروع التالية:

[1] أمير فرج يوسف، البلطجة الإلكترونية، **مرجع سابق**، ص 205

ثانيا: تنازع الاختصاص القضائي في الجرائم الالكترونية

حاول الفقه حل مشكلة تنازع الاختصاص، وانقسم إلى ثلاثة اتجاهات تتمثل في معيار الاختصاص المكاني معيار القانون أكثر ملائمة، ومعيار الضرر المرتقب.

أ_ معيار الاختصاص المكاني

تتوزع الجرائم الإلكترونية غالبًا بين أكثر من دولة أو منطقة، إذ قد يقع السلوك الإجرامي في مكان معين بينما تظهر نتائجه في مكان آخر. ولهذا يمكن أن تتعدد الجهات القضائية المختصة في القضية الواحدة فتستند معظم التشريعات عند تحديد المحكمة المختصة بالنظر في الجريمة إلى عدة معايير أساسية، أهمها مكان ارتكاب الجريمة، أو محل إقامة المتهم، أو المكان الذي تم فيه توقيفه. وعند توافر أكثر من معيار في القضية نفسها، ينعقد الاختصاص عادة للمحكمة التي ترفع أمامها الدعوى أولا[1]. ويقوم هذا الاتجاه على منح الاختصاص للمحكمة التي وقع داخل نطاقها الفعل الإجرامي، أي المكان الذي بدأ فيه النشاط غير المشروع، دون التركيز فقط على المكان الذي ظهرت فيه النتيجة أو الأضرار الناتجة عن الجريمة. ويرجع ذلك إلى أن الاعتماد على النتيجة وحدها قد يثير صعوبات عملية، خاصة في الجرائم المعلوماتية التي تتميز بتعدد أماكن التنفيذ والآثار.

فمثلًا، إذا قام شخص بإرسال فيروس إلكتروني من دولة معينة، ثم تسبب هذا الفيروس في إتلاف بيانات موجودة في دولة أخرى، وألقي القبض على الفاعل في مكان مختلف، فإن الاختصاص قد ينعقد لمحاكم أي من هذه الأماكن، سواء مكان تنفيذ الفعل أو مكان تحقق الضرر أو مكان توقيف المتهم[2] .

ب_ معيار القانون الأكثر ملائمة

يرى أنصار معيار القانون الأكثر ملائمة أن الطبيعة الخاصة للجرائم المعلوماتية، وما يترتب عنها من أضرار قد تمتد إلى عدة دول في الوقت نفسه، تفرض ضرورة البحث عن القانون الأكثر ارتباطًا بالجريمة والأكثر قدرة على تحقيق العدالة. فهذه الجرائم لا تقف آثارها عند حدود دولة واحدة، بل قد تتفاوت درجة الضرر من دولة إلى أخرى، الأمر الذي يدفع إلى منح الاختصاص للدولة التي أصابها الضرر الأكبر بصورة فعلية ومباشرة[3].

ويستند هذا الاتجاه إلى فكرة توسيع قواعد الاختصاص القضائي بما يسمح بإسناد الدعوى إلى المحكمة

---

[1] نفس المرجع.

[2] أمير فرج يسف، البلطجة الإلكترونية، نفس المرجع، ص 198

[3] نفس المرجع.

الأقدر على معالجة النزاع[1]، مع إمكانية تنازل بعض الدول عن اختصاصها لفائدة الدولة الأكثر تضررًا، تحقيقًا لحسن سير العدالة وتفاديًا لتعدد المحاكم المختصة.

كما يؤكد هذا الرأي أن مجرد إمكانية الوصول إلى المعلومات أو المواقع الإلكترونية من داخل دولة معينة لا يكفي وحده لمنح محاكم تلك الدولة الاختصاص القضائي، لأن هذا الأمر أصبح متاحًا تقريبًا في أغلب دول العالم بفعل طبيعة شبكة الإنترنت، وبالتالي لا يمكن الاعتماد عليه وحده كأساس قانوني كافٍ لتقرير الاختصاص .

ج_ معيار الضرر المرتقب وتحقق النتيجة الاجرامية

يقصد بمعيار الضرر المتوقع أو الافتراضي، الذي يقوم على إمكانية تحقق الضرر داخل دولة معينة نتيجة النشاط الإجرامي الإلكتروني، حتى وإن لم يكن الفعل قد ارتكب فعليًا داخل حدودها. ويهدف هذا المعيار إلى توسيع نطاق الحماية القانونية لمواجهة الطبيعة العابرة للحدود التي تتميز بها الجرائم المعلوماتية[2].

يقوم هذا المعيار على الاعتداد بإمكانية تحقق الضرر أو وقوع آثاره الإجرامية داخل إقليم دولة معينة، متى كان النشاط الإجرامي الإلكتروني من شأنه أن يرتب نتائج تمس مصالح أو حقوقًا يحميها قانون تلك الدولة، حتى ولو تم ارتكاب الفعل المكوّن للجريمة، كليًا أو جزئيًا، خارج إقليمها. ويكتسب هذا المعيار أهمية خاصة في مجال الجرائم المعلوماتية، بالنظر إلى سهولة ارتكابها عن بُعد وإمكانية امتداد آثارها إلى أقاليم متعددة، بما يقتضي عدم حصر الاختصاص الجزائي في مكان ارتكاب السلوك الإجرامي وحده

غير أن مجرد احتمال وقوع الضرر لا يكفي بذاته، وإنما ينبغي أن تكون هناك صلة حقيقية ومباشرة بين النشاط الإجرامي والنتيجة أو الآثار المترتبة عليه داخل إقليم الدولة، بما يسمح بإسناد الاختصاص إليها وفقًا للقواعد القانونية المقررة. ويُستحسن، في هذا السياق، التمييز بين الضرر الفعلي والضرر المرتقب؛ إذ لا يُعتد بالأخير إلا متى كان وقوعه متوقعًا على نحو جدي، ومستندًا إلى معطيات موضوعية، وليس مجرد احتمال نظري أو افتراض مجرد. كما ينبغي أن يظل تطبيق هذا المعيار مقيدًا بمتطلبات التناسب وعدم التوسع غير المبرر في الاختصاص، تفاديًا لتنازع الاختصاصات بين الدول.

[1] خلفي عبد الرحمان، مرجع سابق.
[2] أمير فرج يوسف، **البلطجة الالكترونية**، مرجع سابق، **ص 199**

ثالثا: تحديد القانون الواجب التطبيق

يتحدد القانون الواجب التطبيق في الجرائم المعلوماتية وفق مجموعة من المبادئ القانونية التي تعتمد عليها الدول لتقرير اختصاصها الجنائي، ويأتي في مقدمتها مبدأ الإقليمية، الذي يعد الأساس العام في تطبيق القانون الجنائي. فبموجب هذا المبدأ تختص محاكم الدولة بالنظر في كل جريمة تقع كليًا أو جزئيًا داخل حدودها، سواء تعلق الأمر بالفعل الإجرامي نفسه أو بالنتيجة المترتبة عنه، دون النظر إلى جنسية الجاني أو الضحية. وبالتالي، إذا ارتكبت جريمة معلوماتية داخل إقليم الدولة وظهرت آثارها داخله، فإن قانون تلك الدولة يكون هو الواجب التطبيق بصورة طبيعية.[1]

كما يمتد الاختصاص أحيانا استنادا إلى مبدأ العينية، الذي يهدف إلى حماية المصالح الأساسية للدولة. ووفق هذا المبدأ يجوز للدولة أن تباشر اختصاصها القضائي بشأن بعض الجرائم الإلكترونية التي تمس أمنها أو مصالحها الجوهرية، حتى ولو ارتكبت خارج حدودها ومن طرف شخص أجنبي.

ومن جهة أخرى، يعتمد الاختصاص كذلك على مبدأ الشخصية، الذي يقوم على رابطة الجنسية، وينقسم إلى صورتين. تتمثل الصورة الأولى في الشخصية الإيجابية، ومقتضاها خضوع مواطني الدولة لقانونها الجنائي ولو ارتكبوا الجريمة خارج الإقليم الوطني. أما الصورة الثانية فهي الشخصية السلبية، وتعني إمكانية تطبيق القانون الجنائي الوطني متى كان المجني عليه يحمل جنسية الدولة، حتى وإن وقع الفعل خارج الإقليم وكان مرتكبه أجنبيا.

وتبرز أهمية هذه المبادئ في الجرائم المعلوماتية بسبب طبيعتها العابرة للحدود، إذ قد تتداخل عدة دول في الجريمة الواحدة من حيث مكان التنفيذ أو ظهور النتيجة أو جنسية أطرافها، الأمر الذي يفرض توسيع قواعد الاختصاص لضمان عدم إفلات الجناة من المتابعة والعقاب.

المطلب الثالث: ضمانات المحاكمة العادلة في مواجهة الدليل الرقمي

تخضع المحاكمة في الجرائم المعلوماتية بصفة عامة وفي جريمة القرصنة الالكترونية بصفة خاصة إلى مجموعة من الضمانات الأساسية التي تهدف إلى حماية حقوق الدفاع وتحقيق التوازن بين مصلحة المجتمع وحقوق المتهم.

ومن أهم هذه الضمانات مبدأ المواجهة، الذي يسمح للأطراف بمناقشة الدليل الإلكتروني والخبرة التقنية بشكل علني أمام المحكمة، إضافة إلى مبدأ حق الدفاع الذي يتيح للمتهم الطعن في سلامة الدليل الرقمي أو طريقة استخراجه.

[1] فيصل بدري، **مرجع سابق**، ص 197.

كما يشترط احترام مشروعية الإجراءات التي تم من خلالها الحصول على الدليل، وإلا تعرض هذا الأخير للاستبعاد أو عدم الأخذ به، تقوم المحاكمة في الجرائم المعلوماتية على مبدأ أساسي يتمثل في عرض الدليل الإلكتروني أمام القاضي بطريقة تمكنه من الإحاطة بمضمونه وفهمه، وهو ما يختلف عن الأدلة التقليدية التي تكون مادية ومباشرة[1].

فالدليل الرقمي غالبا ما يكون في شكل بيانات أو سجلات أو رسائل إلكترونية أو معطيات مخزنة داخل أنظمة معلوماتية، مما يستوجب إعادة تقديمه في شكل قابل للعرض والمناقشة أمام المحكمة. ويتم ذلك عادة من خلال تقارير الخبرة القضائية التي تُحوّل المعطيات التقنية إلى محتوى مفهوم للقاضي والأطراف، بما يضمن شفافية المناقشة القضائية[2] .

الفرع الاول: الإشكاليات التقنية في المحاكمة

تطرح المحاكمة في الجرائم المعلوماتية عدة إشكالات تقنية، أهمها صعوبة فهم الدليل الرقمي من قبل القاضي غير المتخصص، مما يجعل الاعتماد على الخبرة أمرًا ضروريًا.

كما أن مسألة التلاعب بالبيانات أو تعديلها أو تشفيرها تثير إشكاليات تتعلق بسلامة الدليل، ومدى إمكانية الاعتماد عليه في تكوين القناعة القضائية.

إضافة إلى ذلك، فإن الطبيعة العابرة للحدود للجرائم المعلوماتية قد تطرح إشكالات تتعلق بالاختصاص القضائي وصعوبة الحصول على الأدلة المخزنة في خوادم خارج الدولة.

أولا: دور القاضي في إدارة المحاكمة الرقمية

لا يقتصر دور القاضي الجزائي في هذه المرحلة على تقدير الدليل كما هو الحال في الفصل السابق، بل يتمثل أساسًا في إدارة عملية المحاكمة وضمان احترام الإجراءات القانونية أثناء عرض ومناقشة الأدلة الرقمية.

فالقاضي يشرف على سير الجلسة، ويضمن احترام حقوق الدفاع، ويأمر بالخبرة عند الحاجة، ويقرر استبعاد الأدلة غير المشروعة دون الدخول في تقييم تقني مباشر للمعطيات الرقمية.

وبذلك، فإن دوره يكون إجرائيًا تنظيميًا أكثر منه تقنيًا، وهو ما يميز مرحلة المحاكمة عن مرحلة تقدير الدليل الإلكتروني[3].

---

[1] نفس المرجع

[2] مجدوب لامية، مرجع سابق، ص 116

[3] حسين طاهري، **الجرائم الإلكترونية**، مرجع سابق، ص 455

يتبين مما سبق أن المحاكمة في جرائم أنظمة المعالجة الآلية للمعطيات تختلف عن المحاكمة التقليدية من حيث طبيعة الأدلة وآليات التعامل معها، إذ تعتمد بشكل كبير على الخبرة التقنية وضمانات المحاكمة العادلة، بدل الاعتماد المباشر على اقتناع القاضي بالدليل الرقمي. كما أن المشرع الجزائري حاول التوفيق بين التطور التكنولوجي ومتطلبات العدالة الجنائية من خلال تنظيم كيفية عرض ومناقشة الأدلة الرقمية دون المساس بحقوق الدفاع

ثانيا: آليات تكريس المحاكمة العادلة في ظل الأدلة الرقمية

تستند المحاكمة العادلة إلى مجموعة من الضمانات الجوهرية التي تكفل حماية حقوق الأطراف، ومن أبرزها مبدأ الوجاهية، والحضورية، والعلانية، والشفافية. وفي هذا الإطار، تقوم المحاكمة الجزائية على الطابع الشفوي، حيث تُعرض خلالها مختلف الطلبات والدفوع والمرافعات بحضور الخصوم، ولا يجوز للقاضي أن يؤسس حكمه على عناصر لم تُعرض للنقاش العلني داخل الجلسة، كما يشمل ذلك مناقشة وسائل الإثبات عبر سماع الشهود والاستعانة بالخبراء وتمكين الأطراف من مناقشة الأدلة المعروضة[1]وفيما يتعلق بالأدلة الرقمية، يقتضي تحقيق هذه الضمانات تمكين الخصوم من الاطلاع عليها وفحص محتواها ومناقشتها بفعالية، من خلال وسائل تقنية تسمح بعرضها بشكل واضح ومفهوم، بما يضمن تكافؤ الفرص بين الأطراف. ويثير هذا التطور تساؤلات حول مدى إمكانية الحفاظ على المبادئ الأساسية للمحاكمة العادلة في ظل الاعتماد المتزايد على وسائل تقنية حديثة، وسبل تفادي أي مساس بهذه الضمانات، خاصة ما تعلق منها بمبدأ الوجاهية والحضورية، والعلانية، والشفافية وهو ما سوف نعرضه وفقا للاتي:

ثالثا: مبدأ الوجاهية والحضورية

يقوم مبدأ الوجاهية والحضورية على ضرورة مشاركة جميع الخصوم في جلسات المحاكمة، بما يتيح لكل طرف الإحاطة بما يقدمه الطرف الآخر من أقوال ودفوع، وما يعرض من وثائق ووسائل إثبات، إلى جانب الاستماع إلى الشهادات ومناقشتها، ويكفل هذا المبدأ تحقيق التوازن بين أطراف الدعوى، من خلال تمكينهم من عرض حججهم بحرية، والرد على ما يُثار ضدهم، بما يعزز مبدأ تكافؤ الفرص في الدفاع.

رابعا: مبدأ العلانية

أما مبدأ العلانية، فيتمثل في إتاحة جلسات المحاكمة للجمهور دون تمييز، بما يسمح بالاطلاع على سير الإجراءات والتأكد من احترام القواعد القانونية والضمانات المقررة لحماية حقوق المتهم، كما يؤدي هذا الانفتاح إلى تعزيز الرقابة المجتمعية على عمل القضاء، الأمر الذي يدفع القاضي إلى مزيد من الالتزام بالحياد والنزاهة، ويسهم في ترسيخ الثقة في العدالة، دون أن يكون للحضور أي دور في التأثير على

[1] خلفي عبد الرحمان، **مرجع سابق**، ص 475.

مجريات المحاكمة، وقد نصت على علانية الجلسات طبقا للمواد **421** من قانون الإجراءات الجزائية لسنة **2025**، فيما نصت المادتان **492** و **421** على مبدأ علانية الجلسات بالنسبة لمحكمة الجنح ، والمادتان **600** و **492** بالنسبة للغرفة الجزائية بالمجلس القضائي إلا ما أستثني منها والمتعلق بالقضايا التي تمس بالنظام العام أو الآداب العامة\[1].

خامسا: مبدأ الشفاهية

اعتماد المحاكمة على العرض الشفوي لما يُقدم من مرافعات ودفوع، بحيث يتمكن الخصوم من متابعة كل ما يُطرح أثناء الجلسة، وإبداء ملاحظاتهم بشأنه، مع تمكين القاضي من الإلمام بكافة عناصر القضية من خلال ما يُعرض أمامه مباشرة. ويساعد ذلك على تكوين قناعته بناءً على مناقشة حية ومباشرة لمختلف الأدلة والمعطيات[2].

غير أن اعتماد الوسائل الرقمية في سير المحاكمة يثير إشكالات متعددة تتعلق بمدى احترام هذه المبادئ، خاصة في ظل إجراء الجلسات عن بُعد. فقد تظهر مخاوف مرتبطة بالأعمال التقنية أو التدخلات غير المشروعة، إضافة إلى مخاطر المساس بسرية المعطيات القضائية أو اختراق الأنظمة المعلوماتية. ومن ثم، تبرز أهمية توفير ضمانات تقنية وقانونية كفيلة بحماية نظم العدالة الإلكترونية وتأمين تداول المعلومات القضائية، بما يضمن سلامة الإجراءات واستمرار الثقة في القضاء الرقمي، وهو ما سوف نعرضه في الفرع الرابع[3].

سادسا: تدوين التحقيق

يقصد بتدوين إجراءات التحقيق أو جلسات المحاكمة تحرير محضر رسمي يتضمن جميع الوقائع والإجراءات التي تمت أثناء انعقاد الجلسة تحت إشراف رئيس الجهة القضائية، يشمل التدوين اذا ما كانت الجلسة علنية أو سرية، مع ذكر أسماء القضاة و أمين الضبط والمحامين و الخصوم والشهود، كما يثبت فيه مضمون ما جرى أثناء المحاكمة كتصريحات المتهم سواء بالاقرار أو الانكار، وأقوال الشهود، وطلبات الطرف المدني، ودفوع الدفاع ومرافعاته، إضافة إلى مختلف الإجراءات المتخذة خلال الجلسة[4]. وقد أوجب قانون الإجراءات الجزائية من خلال نص المادة 373 فقرة 2 لمحكمة الجنح بعبارة "مذكرات الجلسة

---

[1] محمد جزيط، **مرجع سابق**، ص 473

[2] حسين طاهري، مرجع سابق.

[3] خلفي عبد الرحمان، **مرجع سابق**، ص 476

[4] محمد حزيط، **مرجع سابق**، ص 475

Les notes d'audience وهو إثبات هذه البيانات بما يعرف بمحضر أو مذكرة الجلسة، والتي يوقع عليها رئيس الجلسة وأمين الضبط خلال أجل محدد بعد انعقادها. غير أن الإخلال بهذا الإجراء لا يعد من النظام العام الذي يترتب على مخالفته البطلان أو النقض، وإنما يهدف أساسا إلـى تمكين جهة الاستئناف من الاطلاع على مجريات المحاكمة وما دار أمام محكمة الدرجة الأولى [1].

سابعا: مبدأ عدم مشاركة القاضي في النظر في الدعوى على مستوى الدرجتين [2]

كرس المشرع هذا المبدأ في المادة **397** من قانون الإجراءات الجزائية بهدف ضمان حياد القاضي وتحقيق المحاكمة العادلة. ويقصد به منع القاضي الذي سبق له مباشرة إجراءات التحقيق في قضية معينة من المشاركة لاحقا في الحكم فيها ضمن تشكيلة محكمة الجنح أو المحكمة الجنائية، حتى لا يتأثر تكوين قناعته بما سبق أن اطلع عليه أثناء مرحلة التحقيق.

كما يمنع على القاضي الذي شارك سابقًا في نظر القضية على مستوى غرفة الاتهام أن يكون عضوًا ضمن هيئة المحكمة الجنائية التي تفصل فيها، تفاديًا لأي تأثير قد يمس بمبدأ الحياد القضائي. وينطبق الأمر ذاته على القاضي الذي سبق له الفصل في القضية أمام جهة قضائية معينة، إذ لا يجوز له المشاركة مرة أخرى في تشكيلة جهة أعلى أو في إعادة النظر في القضية نفسها. ويهدف هذا التنظيم إلى تكريس استقلال القضاء وضمان صدور الأحكام عن هيئة قضائية محايدة لم يسبق لها إبداء رأي في النزاع المعروض أمامها[3].

الفرع الثاني: الضمانات الأمنية لتحقيق العدالة الجنائية الرقمية

تعتمد المحاكم الحديثة على أنظمة رقمية متطورة قائمة على تقنيات المعلومات والاتصال، حيث تُجهَّز بحواسيب وشبكات مترابطة تسمح بتبادل البيانات والمعطيات المتعلقة بالقضايا المعروضة أمامها، وتشمل هذه المعطيات مختلف الوثائق والمستندات والقرارات القضائية، إضافة إلى المراسلات والإجراءات التي تصدر عن أطراف الخصومة أو ترتبط بسير الدعوى.

---

[1] المادة 373 من ق.إ.ج.ج.ج " **يقوم أمين الضبط، تحت إشراف الرئيس، بإثبات سير المناقشات**، ولاسيما أقوال الشهود وأجوبة المتهم.

ويوقع أمين الضبط على مذكرات الجلسة ويؤشر عليها من الرئيس في ظرف الثلاثة أيم التالية لكل جلسة على الأكثر".

[2] محمد حزيط، نفس المرجع، **نفس الصفحة**

[3] المادة 397 من قانون الإجراءات الجزائية" **لا يجوز للقاضي الذي سبق له النظر في قضية، بوصفه قاضيا للتحقيق أو الحكم أو عضوا بغرفة الاتهام أو ممثلا للنيابة العامة، أن يجلس للفصل فيها بمحكمة الجنايات، كما يجوز للمحلف سبق له أن شارك في الفصل في القضية أن يجلس للفصل فيها من جديد**".

ونظرًا لحساسية هذه المعلومات وطبيعتها السرية، فإن ملف الدعوى يُعد من الملفات التي تتطلب درجة عالية من الحماية، بما يضمن عدم وصوله إلى أشخاص غير مخولين أو إلى جهات غير معنية. ويستدعي ذلك توفير حماية مزدوجة، مادية وتقنية وقانونية، للأنظمة المعلوماتية المعتمدة داخل المرفق القضائي، بما يضمن سلامة المعطيات وحسن سير العدالة.

وفي هذا الإطار، تبرز أهمية تأمين هذه الأنظمة من مخاطر الاختراق أو العبث الإلكتروني، حيث أن أي تسلل غير مشروع إلى قواعد البيانات القضائية أو التلاعب بمحتواها من شأنه أن يهدد موثوقية العمل القضائي، كما أن ضعف الحماية قد يشجع بعض مرتكبي الجرائم على محاولة إخفاء آثار أفعالهم أو التأثير على سرية التحقيقات الجارية.

أولا: الحماية المادية، التأمين المادي للأجهزة(Physical Security)

تتميز إجراءات المحاكمة في جريمة القرصنة الإلكترونية بخصوصية ناتجة عن الطبيعة الرقمية للأدلة محل الإثبات، الأمر الذي يفرض على القضاء اعتماد مجموعة من الضمانات الكفيلة بحماية هذه الأدلة وضمان سلامة سير الدعوى، وتتمثل أولى هذه الضمانات في الحماية المادية التي تشمل تأمين المرافق القضائية والأجهزة المعلوماتية وقواعد البيانات، إضافة إلى حماية أماكن حفظ الملفات الرقمية من أي تدخل أو تخريب مادي قد يؤثر على سير العدالة.

ثانيا: الحماية التقنية

يقصد بالحماية التقنية اعتماد أنظمة معلوماتية مؤمنة تضمن التحكم في صلاحيات الولوج إلى المعطيات القضائية، وتسجيل جميع عمليات الدخول والتعديل والنسخ، بما يسمح بتتبع أي نشاط غير مشروع داخل النظام، وتندرج ضمن هذه الحماية مختلف التدابير الوقائية ضد الاختراقات والفيروسات والهجمات السيبرانية التي قد تستهدف الملفات القضائية أو تعطل عمل المنظومة العدلية.

أ_ أهم أساليب الحماية التقنية:

في سياق العدالة الجنائية الرقمية (مثل جرائم القرصنة الإلكترونية)، تعتمد الأنظمة القضائية على مجموعة من أساليب الحماية التقنية لضمان أمن المعلومات وتحقيق محاكمة عادلة. فيما يلي شرح مبسّط لأهم هذه الأساليب.

1- التشفير(Encryption) :

إن التشفير هو وسيلة تقنية من أهم الوسائل التقنية لحماية البيانات المتداولة داخل بيئة المحاكمة، إذ يضمن سرية المعلومات أثناء نقلها أو تخزينها، ويحول دون اطلاع غير المصرح لهم على محتوى الأدلة الرقمية، مما يعزز موثوقيتها ويحافظ على حجيتها أمام القضاء[1]، فالتشفير يعتبر من أهم الصعوبات التي

[1] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، مرجع سابق، ص 315.

تواجه أجهزة إنفاذ القانون، لا سيما فيما يتعلق بالوصول إلى محتوى البيانات المتبادلة بين المستخدمين. فاعتماد تقنيات متقدمة وبرمجيات متخصصة يمنح مستوى عالياً من الحماية والسرية، مما يحدّ من إمكانية الاطلاع على هذه المعطيات من قبل الغير.

ورغم ما يتيحه التشفير من أمان، فإنه لا يشكل عائقاً مطلقاً أمام أعمال التحقيق، إذ يمكن تجاوز هذه الصعوبات متى توفرت لدى الجهات المختصة الخبرات التقنية والوسائل اللازمة لفك الأنظمة المعتمدة، غير أنّ ذلك يظلّ مرتبطاً بإجراءات قانونية تضمن مشروعية التدخل، من خلال الحصول على إذن قضائي يخول استخدام أدوات أو برامج تمكّن من فكّ التشفير والوصول إلى مضمون البيانات. كما قد تفرض بعض التشريعات التزامات على الشركات المقدّمة للخدمات الرقمية، كإمكانية الاحتفاظ بمفاتيح التشفير أو تقديم المساعدة التقنية للسلطات المختصة عند الطلب، تحت طائلة المسؤولية القانونية في حال الامتناع. ويمكن أيضاً إقرار آليات تُلزم المستخدمين بالكشف عن هويتهم عند الولوج إلى الشبكات، بما يسهّل تتبّع الأنشطة غير المشروعة[1].

وتُسهم هذه التدابير، القائمة على التنسيق بين الجهات القضائية والتقنية، في تحقيق توازن بين متطلبات حماية الخصوصية وضمان فعالية التحقيقات الجنائية .

3_ حماية سرية المعلومات وتنظيم الولوج إليها:

تُعد سرية المعلومات القضائية من الركائز الأساسية لضمان نزاهة المحاكمة، حيث يتعين قصر استعمال البيانات على الغرض الذي جُمعت من أجله، ومنع أي استعمال خارج هذا الإطار. ولتحقيق ذلك، تعتمد المحكمة نظاماً معلوماتياً مؤمّناً يقوم على بروتوكول تنظيمي ملزم لكافة المتدخلين، يحدد بدقة شروط الولوج إلى المنصة الرقمية .**(Access Control)**

ويتم منح حق الدخول إلى النظام وفق آلية قائمة على تحديد الصلاحيات، بحيث يُمكَن كل من القاضي، والنيابة العامة، وأطراف الدعوى، ومحاميهم، من الوصول فقط إلى البيانات التي تدخل ضمن نطاق مهامهم، كما يتم تزويدهم بوسائل تحقق شخصية، كأسماء المستخدمين وكلمات المرور، بما يضمن عدم تسرب المعلومات أو إساءة استعمالها[2].

4_ ضمان سلامة البيانات الإلكترونية مكافحة البرمجيات الخبيثة(Antivirus & Anti-malware)

تستوجب المحاكمة في جرائم القرصنة الإلكترونية تأمين البيانات من أي تحريف أو إتلاف أو تعديل

[1] حسين طاهري، **الجرائم الإلكترونية**، مرجع سابق، ص 446.

[2] جاءت المادة **19 من قانون الإجراءات الجزائية الجزائري** لتقر سرية التحقيق، وكذا المادة **76 من نفس القانون** التي تقر بسرية التفتيش من طرف ضباط الشرطة القضائية أو أعوان المكلفون بذلك، وعدم جواز إفشاء المعلومات المتصلة به كما تدعمه المادة **114** المتعلقة بالوسائل التقنية وعدم جواز إفشاء المعلومات المتصلة به كما تدعمه المادة 114 المتعلقة بالوسائل التقنية والتي تجيز اعتراض المراسلات وتسجيلها بإذن قضائي، الدخول إلى الأنظمة المعلوماتية، تفتيش المعطيات الرقمية، نسخ وحجز البيانات

غير مشروع، خاصة في ظل الطبيعة الرقمية للأدلة. لذلك، يجب اعتماد وسائل تقنية متطورة لحماية المعطيات، سواء أثناء تخزينها أو عند تداولها بين مختلف الجهات القضائية، كما ينبغي ضمان التحقق من هوية كل من مرسل ومستقبل البيانات، من خلال تقنيات التوثيق الإلكتروني، بما يعزز حجية الأدلة الرقمية ويحول دون الطعن في صحتها.

5_ تقييد حق الاطلاع على ملفات الدعوى

يخضع الاطلاع على ملفات الدعوى لقيود قانونية صارمة، حيث يُسمح فقط للأشخاص المخول لهم قانوناً بالوصول إلى المعلومات، كلٌّ في حدود اختصاصه. ويهدف ذلك إلى حماية المعطيات الحساسة ومنع أي إفشاء غير مشروع قد يؤثر على سير العدالة أو يمس بحقوق الأطراف[1].

6_ الحماية الجزائية للأنظمة المعلوماتية القضائية(المادة 394 فقرة 01)

تعزيزاً لهذه الضمانات، يتدخل المشرّع الجزائي لتجريم مختلف صور الاعتداء على الأنظمة المعلوماتية القضائية، باعتبارها تمثل البنية الأساسية لسير المحاكمة الإلكترونية. وتشمل هذه الجرائم الولوج غير المشروع، وقرصنة البيانات، وتغيير محتواها أو إتلافها، إضافة إلى تزوير الوثائق الإلكترونية المرتبطة بالدعوى[2].

كما تمتد الحماية لتشمل كل الأفعال التي من شأنها عرقلة سير العدالة الجنائية أو التأثير على سلامة إجراءاتها، مما يكرّس الثقة في القضاء الإلكتروني ويضمن تحقيق محاكمة عادلة .

وبذلك، فإن هذه الضمانات مجتمعة تشكل إطارًا أساسيًا لتأمين المحاكمة في جرائم القرصنة الإلكترونية، من خلال تحقيق التوازن بين فعالية الإثبات الرقمي وحماية حقوق الدفاع وضمان نزاهة الإجراءات القضائية، كما أظهر المشرع الجزائري من خلال قانون الإجراءات الجزائية لسنة 2025 توجها واضحا نحو رقمنة العدالة الجنائية، خاصة في مجال مكافحة جرائم القرصنة الإلكترونية، من خلال تكريس الدليل الرقمي وتوسيع وسائل التحري الفنية، مع الحفاظ على ضمانات المحاكمة العادلة.

---

[1] تخول المادة 408 من ق.إ .ج.ج للمتهم حرية الاتصال بمحاميه، ويعد هذا الحق من أهم الضمانات التي يقرها الدستور، كما أنها واردة في المادة 70 من قانون تنظيم السجون وإعادة الإدماج الاجتماعي، يسهم المحامي في إظهار جوانب الجريمة محل الدعوى، من خلال عرض الوقائع وشرح ملابساتها بصورة واضحة تساعد المحكمة على فهمها وتحليلها، بما يمكنها من تكوين قناعتها القانونية للفصل في القضية سواء بالحكم بالإدانة أو القضاء بالبراءة .

[2] المادة 394 مكرر تنص على تجريم الدخول غير المشروع إلى نظام معلوماتي، أما المادة 394 مكرر 1 فتنص على عرقلة سير نظام معلوماتي، في حين جاءت المادة 394 مكرر 2 بالنص على إدخال أو حذف أو تعديل معطيات، والمادة 394 مكرر 3 تزوير المعطيات ذات الطابع المعلوماتي كما تشمل الحماية الوثائق الإلكترونية القضائية باعتبارها محررات رسمية.

المبحث الثاني: آليات مكافحة جريمة القرصنة الإلكترونية

تكتسي دراسة الجريمة الإلكترونية أهمية خاصة بالنظر إلى خطورتها واتصالها المباشر بحياة الإنسان الخاصة، فضلاً عن مساسها بالمؤسسات وبالاقتصاد الوطني، بل وبالأمن القومي والسياسي للبلاد. فمخاطر هذه الجريمة لا تقف عند حدود انتهاك سرية المعلومات والحق في الخصوصية، وإنما تمتد لتشكل عائقاً أمام التنمية بمختلف أبعادها: العلمية والثقافية والاقتصادية والاجتماعية. كما أنها تؤثر سلباً على الأفراد وحياتهم الخاصة، وهو ما دفع أغلب التشريعات الوطنية والاتفاقيات الدولية إلى الاهتمام بتنظيمها ومكافحتها.وقد حظيت هذه الجريمة منذ بداياتها باهتمام إقليمي ودولي ملحوظ، خاصة بعدما اتسع نطاقها وتنوعت أساليب ارتكابها وتزايدت خطورة عواقبها، نتيجة للانتشار الكبير للإنترنت والكمبيوتر والتطور السريع في تقنيات البرمجة. وانطلاقاً من هذا، يتناول هذا الفصل صور التعاون الدولي في ميدان مكافحة الجرائم المعلوماتية، من خلال مبحثين أساسيين: الاتفاقيات الدولية (المطلب الأول)، والتعاون القضائي لمواجهة هذه الجرائم على المستوى الوطني (المطلب الثاني).

من المُسلم به أن التعاون الدولي يعتبر وسيلة ضرورية لنجاح السياسة الجنائية في مكافحة الجرائم المعلوماتية، خاصة في الجرائم العابرة للحدود الجغرافية للدول، ونظيرا للتطور التكنولوجي الذي يشهده العالم اليوم ونظرًا لكون هذه الجرائم عابرة للحدود ويصعب حصرها داخل نطاق دولة معينة، أصبح من الضروري تفعيل دور المجتمع الدولي لكافحتها، نتطرق في هذا المبحث إلى أبرز الأدوار التي يلعبها المجتمع الدولي، من منظمات واتفاقيات وتعاون قضائي وأمني، في مكافحة الجريمة المعلوماتية[1].

المطلب الأول: الجهود الدولية والاتفاقيات

يعد التعاون الدولي من الركائز الأساسية في مكافحة الجريمة المعلوماتية، نظرا لكون هذه الجرائم ذات طبيعة عابرة للحدود يصعب التصدي لها بالإجراءات الداخلية وحدها. فالتشريعات الوطنية، مهما بلغت دقتها، تبقى قاصرة عن مواجهة التحديات التي تفرضها الجرائم الإلكترونية والتي غالباً ما تتجاوز السيادة الإقليمية للدول. ومن ثم، كان من الضروري إرساء آليات للتنسيق الدولي تقوم على تبادل المعلومات والخبرات وتوحيد الجهود، بما يضمن حماية المجتمع الدولي من مخاطر هذه الظاهرة المستحدثة[2].

[1] محمد منير الجنيبهي، ممدوح محمد الجنيبهي، **مرجع سابق**، ص 169.
[2] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، **نفس المرجع**، نفس الصفحة.

الفرع الأول: اتفاقية تربس

تعد الاتفاقية من أهم الاتفاقيات الدولية المطروحة على الساحة في ظل النظام الدولي المعاصر وقد استغرقت مفاوضات الاتفاقية ما يزيد على سبع سنوات، لتنتهي بالتوصل إلى الصيغة الختامية للجولة، تضمنت كافة الاتفاقية والوثائق، ووافق مندوبو الدول عليها بتوافق الآراء في 15 ديسمبر 1993.[1]

اتفاقية تربس هي اتفاقية تتعلق بأوجه التجارة المتصلة بحقوق الملكية الفكرية، تم التوقيع على المعاهدة سنة 1994، وتناولت هذه الأخيرة تحرير التجارة العالمية، فجاء في نص المادة 10 في فقرتها الأولى:" تتمتع برامج الحاسب الآلي أو الكومبيوتر، بالحماية باعتبارها أعمال أدبية بموجب معاهدة برن".[2]

جاءت الاتفاقية كنتاج لمفاوضات استمرت عدّة سنوات لتكون واحدة من أهم الأدوات الخاصة بتحرير التجارة العالمية التي أحدثت جدلا ونقاشا طويلا أثناء المفاوضات بين الدول النامية والدول الصناعية المتقدمة.

وقد اشتملت الاتفاقية على مواد اتفاقية تريبس بأوجه التجارة المتصلة بحقوق الملكية الفكرية على مكافحة الجريمة المعلوماتية بالنص في المواد 10 في فقرتها الأولى على أن تتمتع برامج الحاسب الآلي أو الكومبيوتر سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة بن 1971 كم نصت في فقرتها الثانية على حماية البيانات المجمعة أو البيانات أو المواد الأخرى بشروط معينة.[3]

أولا: مبدأ المعاملة الوطنية

في إطار حماية الملكية الفكرية أخذت الاتفاقية بقاعدة عامة مفادها المساواة في الدولة العضو بين الأجانب المنتمين إلى إحدى الدول الأعضاء والوطنيين المنتمين إليه، فقد ألزمت المادة الثالثة من الاتفاقية كل دول عضو منح الأجانب الذين ينتمون إلى دولة أخرى من الدول الأعضاء معاملة لا تقل عن تلك التي تمنحها لمواطنيها، في هذا الشأن حماية للملكية الفكرية وتشمل المساواة في الحماية تحديد المستفيدين من الحماية، سبل الحماية، سبل اكتسابها، نطاقها، استمرارها، إنفاذ مدتها، وغيرها، من الأمور التي تؤثر في استخدام حقوق الملكية الفكرية المنصوص عليها في هذه الاتفاقية[4].

---

[1] ربحي امحمد، لعروسي أحمد، **قراءة في اتفاقية تريبس**، مجلة المعيار، المجلد: 13 العدد (01) جوان 2022، ص 553-554.

[2] المادة العاشرة من اتفاقية برن

[3] طرشي نورة، **مرجع سابق**، ص 74.

[4] بدري فيصل، **مرجع سابق**، ص 24.

ثانيا: مبدأ الدولة الأولى بالرعاية

قراءةً لما جاء في المادة الرابعة من اتفاقية تريبيس على الدول الأعضاء وذلك بمنح المنتمين لكافة الدول فورا، وبدون أي شروط، أي مزايا، أو أي حصانة أو معاملة تفضيلية تمنحها للمنتمين إلى أي دولة أخرى تتعلق بحماية الملكية الفكرية، بما معناه أن كل دولة عضو في منظمة التجارة العالمية قامت بمنح دولة أخرى عضو ميزة تفضيلية معينة يتعين عليها منح جميع الدول الأعضاء الأخرى نفس الميزة، غير أن هذا لمبدأ يلاحظ عليه أنه لا يمنع الدول الأعضاء من القيام بفرض قيود لتنظيم التجارة الدولية، ويشترط أن تكون هذه القيود لتنظيم التجارة الدولية، ويشترط أن تكون هذه القيود عامة وموضوعية ومجردة دون أن تحمل مزايا للبعض دون الآخر.[1]

ثالثا: وضع حد أدنى من الحماية القانونية

فرضت الاتفاقية حدًا أدنى من الحماية بحيث يجب على كل دولة عضو الالتزام به، وهذا يشمل:

مدة الحماية.

نطاق الحقوق الممنوحة.

سبل إنفاذ هذه الحقوق.

رابعا: إنفاذ اتفاقية تريبس

تعتبر الدول الصناعية المتقدمة هي الأكثر ضررا من قرصنة الملكية الفكرية، كرست مجهوداتها لإجبار الكثير من الدول النامية للانقياد وراء الاتفاقيات والحد من القرصنة الالكترونية، ولكن هذه الدول الصناعية لم تستطع التوصل إلى عقد اتفاقية تريبس مالم يكن لها القدر الكافي من المرونة التي من مظاهرها الرضا بالفترات الانتقالية التي تم إقرارها وهي فترات سماح لا تلزم خلالها الدول بالالتزامات التي فرضتها الاتفاقية.

إذن فمصلحة الدول الصناعية المتقدمة وعلى رأسها الولايات المتحدة الأمريكية، كانت الأولى في تطبيق قواعد اتفاقية تريبس من لحظة إبرامها.

[1] مليكة عطوي، **الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت**، رسالة دكتوراه، جامعة الجزائر 03، 2010، ص 270.

خامسا: المعاملة التفضيلية للدول النامية

من أهم مقاصد اتفاقية تريبس مراعاة الاحتياجات الخاصة لأقل البلدان الأعضاء نموًا، فهي تراعي المرونة في تنفيذ أحكامها خاصة على الصعيد الداخلي لهذه الدول الأعضاء، فاتفاقية تريبس أرادت من المعاملة التفضيلية للدول النامية تمكين هذه الدول من إنشاء قاعدة تكنولوجية متطورة تخدم مصالحها الاقتصادية وتساعدها على الاندماج بعجلة التجارة الدولية.

لا يمكن إنكار فعالية الاتفاقيات الدولية التي لعبت دورًا بارزًا في مكافحة الجريمة المعلوماتية على المستوى الدولي، بالإضافة إلى ذلك يجب التنويه أيضًا لدور المنظمات العالمية في مكافحة الجريمة المعلوماتية كمنظمة الأمم المتحدة في جهودها المبذولة للإحاطة بالإجرام المعلوماتي، حيث أنها في تقرير لها تحت عنوان "اقتراحات المعالجة الدولية تجاه ظاهرة تطور الجريمة" عام 1987، وفي اجتماع آخر لها عام 1990، تمت مناقشة مشروع لمكافحة مشكلة الجريمة المرتبطة بالحاسب الآلي، فركزت على أهمية جهد الدول الأعضاء لضبط جرائم المعلوماتية نظرًا لآثارها السلبية والخطيرة على الأفراد والمجتمع[1].

الفرع الثاني: معاهدة بودبست 2001

في أواخر سنة 2001، وفي قلب العاصمة المجرية بودبست انعقدت أولى المعاهدات الدولية التي تكافح جرائم الإنترنت وتبلور معالم التعاون والتضامن الدوليين في محاربة هاته الجرائم ومحاولة الحد منها خاصة مع التفشي الذي تشهده مع تزايد درجات الخطورة التي تشكل تهديدا للأشخاص والممتلكات.[2]

خضعت المعاهدة إلى صياغة من جانب عدد كبير من الخبراء القانونيين في مجلس أوروبا هذا بمساعدة دول أخرى على رأسها الولايات المتحدة الأمريكية بعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطاع الإعلام الآلي على مستوى العالم، الأمر الذي أدى في النهاية للتوقيع عليها من قبل ثلاثين دولة 23 نوفمبر 2001 في عاصمة المجر وهذا لمواجهة الاستخدام غير المشروع للحسابات وشبكات المعلومات أو ما يسمى بالإجرام الكوني أو الإجرام المعلوماتي أو الجرائم المعلوماتية،[3] وقد وقعت عدَّة دول غير أعضاء مجلس أوروبا منها كندا، واليابان وجنوب إفريقيا، والولايات المتحدة الأمريكية، فهي في الأصل أوروبية الميلاد، غير أنها ذات طابع دولي لأنها مفتوحة أي تسمح بانضمام الدول الأخرى غير المجموعة

[1] طرشي نورة، **مرجع سابق**، ص 74.

[2] منير محمد الجنبيهي–ممدوح محمد الجنبيهي، **مرجع سابق**، ص180.

[3] بدري فيصل، **مرجع سابق**، ص 29.

الأوروبية (المادة 48) غير أن هذه الدعوة للانضمام لا تقارن من أي اتفاقية تم إعدادها في إطار المجموعة الأوروبية.[1]

أولا: أهم ما جاءت به المعاهدة

إدراكاً من المجتمع الدولي لخطورة الجريمة المعلوماتية باعتبارها جريمة عابرة للحدود، تم التوقيع على اتفاقية دولية بهذا الخصوص في العاصمة المجرية "بودابست" من قبل ثلاثين دولة، من بينها دول أعضاء في الاتحاد الأوروبي، إضافة إلى كل من كندا، اليابان، جنوب إفريقيا، والولايات المتحدة الأمريكية. وقد جاءت هذه الاتفاقية لمعالجة إشكالية الطابع الدولي للجريمة الإلكترونية وتجاوزها للحدود الوطنية، بما يسهم في تعزيز جهود الدول في مكافحة هذا النوع من الجرائم، وتعقب مرتكبيها، والمساعدة على الاستدلال عليهم وضبطهم. كما حددت الاتفاقية أفضل الآليات والإجراءات التي ينبغي إتباعها في مجال التحقيق في جرائم الإنترنت، والتي تلتزم الدول الموقعة بالتعاون الوثيق بشأنه

العنصر الأول: يتمثل في أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية.

العنصر الثاني: يتمثل في أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الالكترونية أي النصوص الإجرائية.

العنصر الثالث: يتمثل في أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم، والانطلاق مما أنجز من جهود دولية وإقليمية هذا المجال.

تضمنت المادة(27) من الاتفاقية على الإجراءات المتعلقة بالمساعدة القضائية في حالة وجود اتفاقية دولية واجبة التطبيق بشأن الطلبات المتعلقة بالمساعدة المتبادلة، بحيث تضمنت أن يرفض طلب المساعدة إذا كان الطلب متعلق بجريمة سياسية، أو أن الطلب يمس سيادة الدول أو الأمن أو النظام العام.[2]

وفقا للقواعد التي جاءت بها الاتفاقية، والنصوص التي سنَّها المشرع الجزائري حول الحماية ضد جريمة المعالجة الآلية للمعطيات من بابها الموضوعي والإجرائي كما قد قدَّم تبيان مدى توافقية الموضوعية

---

[1] بدري فيصل، **مرجع سابق، ص 88**

[2] خالد ظاهر عبد الله جابر السهيل المطيري، **مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية**، دكتوراه في القانون الجنائي، أكاديمية سعد العبد الله للعلوم الأمنية، الكويت، ص 05.

للنصوص القانونية المتاحة وكفاءتها في مواجهة هذا النوع من الجرائم بين نصوص اتفاقية بودبست ونصوص المشرع الجزائري.

تتكون الاتفاقية من ديباجة وثمان وأربعين (48) مادة وهي تعالج ثلاث محاور، الجرائم التي تتعرض لها شبكة الانترنت والحاسب الآلي، والثاني الجوانب الإجرائية للجرائم المعلوماتية، والثالث التعاون الدولي بين الدول الأعضاء لمكافحتها، ومن بين البنود التي تناولتها الاتفاقية هو الإرهاب الدولي، وعمليات تزوير بطاقات الائتمان ودعارة الأطفال، لأنها تعتبر من أكثر الجرائم انتشارا على المستوى العالمي، وورد في التقرير السنوي لاتفاقية الجريمة الالكترونية الصادر عن مجلس أوروبا (سلسلة المعاهدات الأوروبية رقم 185)[1]، أنه بالإضافة إلى تدابير التعاون الدولي من خلال تسليم المجرمين والمساعدة القضائية، ينبغي معالجة المسائل المتعلقة بالقانون الإجرائي بكل ما يتصل باستخدام تكنولوجيا المعلومات، وحددت المواضيع القانونية التي يجب إعادة النظر فيها:[2]

جرائم الفضاء الالكتروني، كالمعاملات المالية غير المشروعة، انتهاك حقوق المؤلف، تقديم خدمات غير قانونية والجرائم التي تنتهك كرامة الإنسان وحماية القُصَّر.

وجوب تبني مقاربة مشتركة لأغراض التعاون الدولي.

استخدام طرق قسرية كالرقابة الالكترونية واعتراض الاتصالات على شبكات المعلومات ويصل الأمر إلى مصادرة مواقع الانترنت وقد يمتد في البيئة الالكترونية إلى تجاوز الحدود، وحماية المعلومات بالتشفير مثلا.

تناول مسألة الاختصاص القضائي فيما يتعلق بجرائم تكنولوجيا المعلومات لتحديد ارتكاب الجريمة، والقانون الواجب التطبيق، تنازع الاختصاص الإقليمي.

بالإضافة إلى أن الاتفاقية تحدد أفضل الأساليب والطرق الواجب الطرق إتبَّاعها في جرائم الانترنت، كما تحاول إقامة توازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، وأيضا تهدف بصفة خاصة إلى السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية من غير الدول

---

[1] ميرفت محمد حبايبه، **مكافحة الجريمة الالكترونية "دراسة مقارنة" في التشريع الجزائري والفلسطيني**، أطروحة لنيل شهادة دكتوراه في الحقوق: تخصص القانون العام، جامعة عمَّار ثليجي-الأغواط، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2021، ص 193-194.

[2] منير محمد الجبيهي، ممدوح محمد الجبيهي، **مرجع سابق**، ص 180.

الأوروبية، وتحقيق المعاهدة للتوازن بين حقوق الإنسان والإجراءات المتخذة لمواجهة هذه الجرائم، وقد عمل الأعضاء المشاركين على بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم الالكترونية في جميع أنحاء العالم.

ثانيا: الاتفاقية الدولية

نظام الكومبيوتر: أي جهاز يتألف من أجهزة وبرمجيات تم تطويرها من أجل المعالجة التلقائية للبيانات الرقمية، ويمكن أن يشمل المداخلات والمخرجات، ويُرافق التخزين، ويمكن أن يشتغل لوحده أو لوحده وأن يكون مثلا بشبكة مع غيره من الأجهزة المماثلة.

الشبكة: تُعرف شبكة الحاسوب على أنها: " نظام لربط جهازين باستخدام إحدى تقنيات نظم الاتصالات من أجل تبادل المعلومات الموارد، والبيانات، كما تسمح بالتواصل المباشر بين المستخدمين"،[1] واعتبرتها أيضا أهم الشبكات، وتسمى أيضا بشبكة الشبكات، وهي عبارة عن" مجموعة من الحواسيب المتصلة فيما بينها عن طريق أسلاك أو دون أسلاك، أي إمكانية وصول أي منها لمحتوى الآخر واستخدامه للموارد الخاصة به من تطبيقات وقواعد معطيات وغيرها من المعلومات"، إذن فهي تتضمن الملفات وقواعد البيانات والبرامج...إلخ[2]، وتعود الأهمية الدائمة للشبكة في تشارك المصادر.

مقدمو الخدمة: يشكلون فئة واسعة من الأشخاص والهيئات الذين يتفردون بدور خاص فيما يتعلق بالاتصال أو المعالجة الآلية للبيانات ذات الصلة بأنظمة الكومبيوتر، (تخزين، معالجة، استضافة...).

بيانات الحركة: تتمثل في جزء من بيانات الكومبيوتر التي تخضع لنظام قانوني خاص، ويتم توليدها من أجهزة الكومبيوتر لسلسلة من الاتصالات من أجل توجيه اتصال من المصدر الأصلي إلى الوجهة، تعبر البيانات عن حركة فرعية ومساعدة على الاتصال في حد ذاته.

كما جاء في نص المواد من المادة الثانية إلى المادة السادسة، الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية، وهي جرائم الدخول غير المشروع للنظم المعلوماتية والاعتراض غير القانوني لهذه النظم والاعتداء على سلامة البيانات وإساءة استخدام أجهزة الحاسوب، كما تناولت المادتان السابعة والثامنة التزوير والغش المعلوماتي، كما جاء في المادة العاشرة الاعتداء على حقوق الملكية الفكرية والحقوق

[1] دليل الأدلة الالكترونية، **دليل أساسي لموظفي الشرطة، والمدعين العامين والقضاة**، دليل مجلس أوروبا حول الأدلة الالكترونية، النسخة2، قسم الجريمة الالكترونية، المديرية العامة لحقوق الانسان وسيادة القانون، ستراسبورغ، فرنسا، 15 ديسمبر 2014، ص 18.

[2] عبد الله عبد الكريم عبد الله، **مرجع سابق**، ص20.

المجاورة، والمادة 11 فقد تطرقت للشروع والاشتراك في هذا النوع من الجرائم، أما عن مسؤولية الأشخاص المعنوية المترتبة عن الجرائم المعلوماتية والتي تُعتبر مسؤولية مستحدثة في التشريعات الجنائية المقارنة المعاصرة سعت هذه الاتفاقية إلى تحسين وإصلاح وسائل منع وقمع الإجرام المعلوماتي، وهذا من خلال تحديد الحد الأدنى المشترك الذي يسمح باعتبار بعض التصرفات من فئة الجرائم الجنائية، وهذا النوع من التجانس يتيح أكثر المكافحة هذه الجرائم سواءً على المستوى الوطني أو الدولي. وخصصت الاتفاقية المحور الثاني للجوانب الإجرائية إذ أوصت الدول الأعضاء باتخاذ الإجراءات اللازمة والضرورية لضبط ونسخ الأدلة المعلوماتية.

من خلال استقراء ما جاءت به الاتفاقية نستخلص الأهداف التي سعت إليه في التالي:

العمل على تحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية على غرار الدول الأوروبية.

التأكيد على إلزامية التعاون الإقليمي والدولي في الميادين المتعلقة بمكافحة الجرائم الالكترونية وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة الإجرام المعلوماتي.

وجوب وضع الخطط الفعالة لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكومبيوتر وشبكاته وأنشطة إساءة استخدامها بما في ذلك تحديد الإطار الموضوعي.

تحقيق التوازن بين حماية حقوق الإنسان الأساسية المعترف بها بموجب اتفاقية مجلس أوروبا لحماية حقوق الإنسان وحرياته الأساسية لعام 1950 والعهد الدولي للحقوق المدنية والسياسية لعام 1960، والاتفاقيات العالمية الأخرى في ميدان حقوق الإنسان، وتحديد الحقوق المتصلة بالرأي وحرية الحصول على المعلومات وحرية البحث والتلقي والنقل للمعلومات والأفكار، وبين الحق والخصوصية في حيازة المعلومات، والإفادة من عناصر الملكية الفكرية لها، ولعل هذا المنطلق يمثل النظرة الحكيمة من الناحية الفلسفية لظاهرة الجرائم الالكترونية ووجوب الحماية منها.[1] الفرع الثالث–الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010م.

[1] بدري فيصل، **مرجع سابق**، ص 33.

الفرع الثالث: الاتفاقية العربية لمكافحة الجريمة

وقَّع مجلس وزراء الداخلية والعدل العرب في (2010/12/23) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ويأتي ذلك ضمن الجهود الحديثة التي تقوم بها جامعة الدول العربية لتعزيز التدابير الأمنية لمكافحة الجرائم المتعلقة بتقنية المعلومات في ضوء الأسس النظامية، والبيئة القانونية[1].

وتتكون الاتفاقية العربية من ثلاث وأربعين مادة، وتشكل في إلزام الدول الأطراف بإدخال بعض التعديلات؛ لتجريم جرائم تقنية المعلومات وضبط الفاعلين، وذلك بهدف حماية الخصوصية، والاعتماد على سلامة البيانات، والاعتداء على حرمة الحياة الخاصة، والاعتداء على الملكية الفكرية، وإساءة استخدام وسائل تقنية المعلومات، والتزوير، والاحتيال، والجرائم المتعلقة بالإرهاب، وغسيل الأموال، والمخدرات، والاتجار في الجنس البشري وأعضاء البشرية والأسلحة، والمساس بالثقة البنكية أو النظام العام، والتهديد، والابتزاز، والاتجار في الآثار والعنف اللفظي، والاستخدام غير المشروع لأدوات الائتمان والوثائق الإلكترونية.

وقد عنيت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بمواجهة عدة جرائم، ومن أهمها[2]:

أ-جريمة الدخول غير المشروع.

ب-الاعتراض غير المشروع لخط سير البيانات.

ج-الاعتداء على سلامة البيانات.

د-جريمة إساءة استخدام وسائل تقنية المعلومات.

هـ-جرائم التزوير والاحتيال.

و-الجرائم الإباحية والجرائم المتعلقة بانتهاك حق المؤلف.

المطلب الثاني: الجهود الوطنية في مكافحة جريمة القرصنة الالكترونية

أصبحت مكافحة الجريمة الإلكترونية هاجساً يؤرق رجال القانون، لذلك لا بد من التعاون بين القضاء والنيابة العامة ورجال الضبطية العدلية والسلطات الرقابية والرجال المتخصصين في التقنيات الرقمية

---

[1] محمد حمد عمر الغياثين، **الجرائم المعلوماتية عابرة للحدود-دراسة مقارنة-**، رسالة قُدمت لنيل درجة الدكتوراه في الحقوق جامعة القاهرة، عام 2013م، ص65.

[2] خالد ظاهر عبد الله جابر السهيل المطيري، **لمواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية**، ص 44.

والمؤسسات المستعملة، لوضع قواعد قانونية لمجابهة هذه الجريمة التي تشكل خطراً. فالجريمة الإلكترونية، فيما يتعلق بأساليب مكافحتها والوقاية منها والجهات المكلفة بذلك، تعد من أبرز الجرائم الحديثة، وهي مرتبطة بالشبكات المفتوحة، الأمر الذي جعلها تتجاوز الحدود الوطنية للدول، وهو ما يفرض مواجهة دولية متكاملة.لقد أثبتت التجارب قصور الجهات الأمنية التقليدية المكلفة بالتصدي للجريمة الإلكترونية، وعدم القدرة على تغطية مختلف جوانبها، الأمر الذي جعلها تمثل خطورة كبيرة ومتزايدة، وترتب على ضرورة العمل على إيجاد آليات حديثة تتناسب مع خصوصية هذه الجريمة[1].

ولقد تبينت مجموعة من الآليات الإجرائية على المستوى الوطني لمواجهة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال الجزائرية، إذ تم إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية التي يرأسها وزير الدفاع الجزائري، ووحدة الجرائم الإلكترونية في فلسطين، كما أكدت الاختصاص القضائي لمحاكم متخصصة تطبق قانون العقوبات وقانون الإجراءات الجزائية وبعض القوانين ذات الصلة.

الفرع الأول: الآليات القانونية والقضائية

مع صعوبة التتبع والإثبات في الجرائم الإلكترونية وقصور القواعد التقليدية في مجابهة الجريمة كان لزاما على المشرع الجزائري التدخل بسن نصوص آمرة لتجريم الظاهرة من جهة وإصدار قوانين خاصة تتلاءم وطبيعة الجريمة ومستلزمات المكافحة التي ترتكز على التعاون بين الجهات القانونية والمختصين في المعلوماتية زيادة على التعاون الدولي.

أولا: الاليات القضائية

ومن بين الأساليب التي كرسها المشرع لمكافحة جريمة القرصنة الإلكترونية

أ_ الاختصاص القضائي أين أنشأ أقطاب متخصصة للنظر في الاعتداءات الواقعة على أنظمة المعلومات أو الجرائم العابرة للحدود باستخدام الوسائل الرقمية. وقد أنشئ هذا القطب بهدف ضمان فعالية المتابعة القضائية للجرائم المعلوماتية[2]، كما تم التطرق إليه بالتفصيل في المبحث الأول من هذا الفصل[3].

ب_ توفير قضاة مختصين يمتلكون المعرفة التقنية والقانونية اللازمة.

---

[1] ميرفت محمد حبايبه، **المرجع السابق**، ص153.

[2] المادة 37 **من قانون الإجراءات الجزائية الجزائري**.

[3] المادة 335 **نفس القانون**، مذكورة سابقا.

ج_ تسهيل التنسيق بين مختلف الجهات الأمنية والقضائية، تحسين وسائل التحقيق في الجرائم المرتكبة عبر الشبكات الرقمية عن طريق سلطة الضبط المتمثلة في

د_ تعزيز صلاحيات حجب المحتوى غير القانوني في التشريع الجزائري[1]

ثانيا: الاليات القانونية

اعتمد المشرع الجزائري في مواجهة الجرائم الإلكترونية والقرصنة الإلكترونية على معيار عام يتمثل في اعتبار كل محتوى يشكل جريمة قانونية قابلاً للحجب أو تقييد الوصول إليه، دون وضع قائمة دقيقة ومفصلة للمحتويات غير المشروعة كما فعلت بعض التشريعات المقارنة. لذلك فإن أي محتوى رقمي يرتبط بأفعال مجرمة، كاختراق الأنظمة المعلوماتية، نشر البرمجيات الخبيثة، المساس بأمن الدولة، أو الاعتداء على المعطيات الإلكترونية، يمكن أن يكون محل للحجب والمنع.

كما دعمت بعض القوانين الخاصة هذا التوجه، خاصة في مجال الاتصالات الإلكترونية والتجارة الإلكترونية، من خلال منع استعمال الوسائط الرقمية في الأنشطة غير المشروعة أو المضرة بالأمن والنظام العام. غير أن المشرع لم يحدد بصورة واضحة إجراءات الحجب والجهات المختصة به، مما ترك مجالاً واسعاً للتفسير وأثار إشكالات تتعلق بحماية الحقوق الرقمية وحدود الرقابة على الفضاء الإلكتروني[2]

الفرع الثاني: الآليات المؤسساتية والهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام والاتصال

أسندت مهام مكافحة الجرائم السيبرانية إلى عدة مؤسسات على غرار أجهزة الأمن الوطني والدرك الوطني، ومصالح وزارة الدفاع، إضافة إلى هيئات تنظيمية وبحثية مثل مركز البحث في الإعلام العلمي والتقني(CERIST)، فضلاً عن دور وزارة العدل والنيابة العامة في المتابعة القضائية. ويهدف هذا التنظيم المؤسساتي إلى ضمان حماية الفضاء السيبراني الوطني، وردع محاولات القرصنة التي تستهدف الأفراد والمؤسسات على حد سواء، بما ينسجم مع التوجهات الدولية في هذا المجال، فنعالج من خلال هذه العناصر مهام ودور المجلس الوطني لأمن الأنظمة، ووكالة أمن الأنظمة المعلوماتية.

أولا: المجلس الوطني لأمن الأنظمة المعلوماتية

يتشكل المجلس الوطني لأمن الأنظمة المعلوماتية رئيسا يتمثل في وزير الدفاع الوطني أو ممثلا عنه، بالإضافة إلى ممثل عن رئاسة الجمهورية، ممثل عن الوزير الأول–الوزير المكلف بالشؤون الخارجية–

[1] مناصرة يوسف، **شرعية حجب المواقع الإلكترونية بين التشريع الجزائري والمقارن وأثره على حرية التعبير**، دار الخلدونية، 2022، ص225.

[2] نفس المرجع.

الوزير المكلف بالداخلية–الوزير المكلف بالمالية–الوزير المكلف بالطاقة–الوزير المكلف بالاتصالات–الوزير المكلف بالتعليم العالي، كما يمكن للمؤسسة أن تستعين بأي شخص طبيعي أو معنوي من شأنه تنويره في أعماله.

أ_مهام المجلس الوطني لأمن الأنظمة المعلوماتية

في إطار الإعداد العملي للاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، يمتهن المجلس في وجه خاص ما يلي:[1]

البت في العناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديها.

دراسة مخطط عمل الوكالة وتقرير نشاطها والموافقة عليه.

دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتصدر قرار الموافقة عليها.

الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في المجالات المتعلقة بأمن الأنظمة المعلوماتية.

الموافقة على سياسة التصديق الالكتروني للسلطة الوطنية للتصديق الالكتروني.

الموافقة على تصنيف الأنظمة المعلوماتية.

اقتراح ما يتلاءم مع الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية.

عند الضرورة يُبدي المجلس رأيا مطابقا في أي مشروع نصوصا تشريعية أو تنظيمية ذات صلة بأمن الأنظمة المعلوماتية.

ب_ كيفية ممارسة مهام المجلس الوطني لأمن الأنظمة المعلوماتية

يجتمع المجلس كلما دعت الحاجة لذلك، حي يقوم أعضاءه بالمصادقة على نظامه الداخلي، ويجتمع في ذلك هيئات عمومية وخاصة من أجل وضع استراتيجية بناءً على استدعاء رئيسه، 22ويقوم رئيس

[1] حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية –قراءة في أحكام المرسوم الرئاسي 05–20، مجلة الحقوق والعلوم الإنسانية، العدد الثالث، المجلد الثالث عشر، 2020، ص182.

المجلس إعداد جداول وأعمال مع ضمان اليقظة التكنولوجية في مجال أمن الأنظمة، كما يعمل على تنظيم اجتماعات المجلس وتحديد تاريخها.[1]

يرسل المجلس الاستدعاءات وجدول سير الأعمال إلى الأعضاء من تاريخ الاجتماع، وفي الحالة الاستعجالية، يمكن تبليغ جدول الأعمال أثناء انعقاد الجلسة، أما بالنسبة للقرارات الصادرة عن المجلس فتتخذ بالأغلبية، وفي حال تساوي الأصوات، يكون الرئيس مُرجحًا، [2]وعلى هذا الأساس تُدَون نتائج أشغال اجتماعات المجلس في محضر كما تتوج أعمال المجلس بحسب الحالة، بقرارات وتوصيات وآراء وكذا تقارير كما تفرد وتسجل الاعتمادات اللازمة لسير المجلس، في ميزانية وزارة الدفاع الوطني.[3]

ثانيا: وكالة أمن الأنظمة المعلوماتية

سبق المشرع التونسي في إنشاء الوكالة الوطنية للسلامة المعلوماتية والتي استحدثها بموجب القانون المتعلق بالسلامة المعلوماتية سنة 2014، وتشهد تحيينًا مستمر ففي سنة 2019 شرعت في تنظيم ورشات تعنى بحماية البنى التحتية المعلوماتية الحيوية وآلية المراكز القطاعية للاستجابة للطوارئ المعلوماتية والسلامة المعلوماتية.

ليلتحق به المشرع الجزائري في تبني وكالة أمن الأنظمة المعلوماتية الذي يُعتبر قد جاء متأخرا، حيث تعتبر الوكالة حسب نص المادة 17 من المرسوم الرئاسي، مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية، والاستقلالية المالية.

بموجب المادة 18 على الخصوص بما يأتي[4] :

1-تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس.

2-تنسيق تنفيذ الاستراتيجية الوطنية في مجال الأمن الأنظمة المعلوماتية المحددة من قبل المجلس.

3-اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.

4-إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية.

---

[11] المادة 13 من الرسوم الرئاسي 20-05.

[2] المادة 14 من المرسوم الرئاسي، 20-05.

[3] المادة 16 من نفس المرسوم.

[4]- المادة17-18 من نفس المرسوم

5-السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية.

6-متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية.

7-تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية.

8-ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية.

9-مرافقة الإدارات والمؤسسات والهيئات بالتشاور مع الهياكل المختصة في هذا المجال في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية، بعد الرأي المطابق للمجلس.

10-إعداد وتحديث المرجعيات والإجراءات والأدلة العملية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية.

11-اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها

12-اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني.

ثالثا: الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال

تعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من أبرز الجهات القانونية المكلفة بمكافحة الجرائم الالكترونية والوقاية منها، الهيئة استحدثت بموجب المادة 13 من القانون 09-04 والتي جاء في نصها ما يلي" تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"، ليأتي بعدها المرسوم 15-261 وتم بموجبه تشكيل الهيئة وتنظيمها وتحديد كيفيات سيرها،[1] وقد تم منح الهيئة صلاحيات واسعة في مجال الأمن المعلوماتي، مع تحديد تشكيلتها وتنظيمها ومختلف المهام الموكلة إليها في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما وضحت كيفيات سيرها مختلف الأحكام المالية والقانونية المتعلقة بها.[2]

[1] المرسوم الرئاسي 15-261 **المحدد لتشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال** المؤرخ في 08-10-2015، الجريدة الرسمية العدد 53.

[2] المادة **13 من المرسوم الرئاسي 15 – 261** المحدد لتشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال المؤرخ في 08-10-2015، الجريدة الرسمية، العدد 53.

الهيئة هي عبارة عن سلطة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى الوزير المكلف بالعدل، مركزه بالجزائر العاصمة تتشكل الهيئة من: [1]

1-لجنة مديرة.

2-مديرية عامة.

3-مديرية التنسيق التقني.

4-ملحقات جهوية.

تم تكليف الهيئة في إطار عملها بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أي أنها هيئة متخصصة اسند إليها جملة مهام تمارسها تحت الرقابة القضائية، بما يتوافق مع القانون والتشريع المعمول بهما وعلى وجه الخصوص قانون الإجراءات الجزائية الجزائري، والقانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الجزائري، تتمثل المهام في:[2]

1-اقتراح عناصر السياسة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

2-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

3-مساعدة السلطات القضائية ومصالح الشرطة في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما فيها جمع المعلومات والتزود بها من خلال الخبرات القضائية.

4-ضمان المراقبة الوقائية للاتصالات الإلكترونية بهدف الكشف عن الجرائم التي تتعلق بالأعمال الإرهابية والتخريبية وكذا المساس بأمن الدولة تحت سلطة القاضي المختص.

5-تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

6-السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال الاختصاص.

---

[1] المادة 06 من ذات المرسوم.

[2] تم تحديد هذه المهام والتفصيل فيها بموجب: **المادة الرابعة عشر (14) من المرسوم الرئاسي** 15-261 السابق ذكره.

7-العمل على تطوير التعاون بين المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

8-المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

وضمانا لقيام الهيئة بالمهام الموكلة إليها على الوجه الصحيح بما هو مقرر ومحدد قانونا، عمل المشرع الجزائري على ضبط كيفيات صيرورتها وهذا لبيان مختلف الإجراءات التي تتبعها في سياق القيام بالمهام المتمثلة بها[1]:

1-تجتمع الهيئة المديرة بناءً على استدعاء من رئيسها أو بطلب من أحد أعضائها.

2-إعداد نظامها الداخلي والمصادقة عليه.

3-إمكانية الاستعانة بأي خبير أو أي شخص يمكن أن يسهل القيام بمهامها المنوطة.

4-طلب أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لإنجاز المهام الموكلة إليها قانونا.

5-مراقبة الاتصالات الالكترونية وتجميع وكذا تسجيل محتواها في حين قيامها بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية وتحت سلطة قاضي مختص وهذا بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو تخريب أو مساس بأمن الدولة، وفقا لما تنص عليه أحكام المادة 13 من القانون 09-04.

قابلية وضع وحدة للمراقبة أو أكثر مع تزويدها بالوسائل والتجهيزات التقنية لتنفيذ عملية المراقبة للاتصالات الإلكترونية، وتتشكل الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط واحد من ضباط الشرطة القضائية أو أكثر ينتمي للهيئة، مع إلزامية امتثال الوحدة في عملها لأحكام التشريع المعمول به وشوط الرخصة المسلمة من الشرطة القضائية.

إمكانية الحصول على المساعدة من الموظفين المختصين من الوزارات المعينة في مجال تكنولوجيات الإعلام والاتصال.

لحساسية المهام الموكلة إليها ومجال الاختصاص، فقد أقر المشرع بإلزامية عدم استخدام الهيئة المعلومات والمعطيات التي تستلمها أو تجمعها لأغراض غير تلك المتعلقة بمجال مكافحة الجرائم المتصلة

[1] حسين طاهري، **جرائم القرصنة الإلكترونية**، مرجع سابق، ص 214.

بتكنولوجيا الإعلام والاتصال ومكافحتها مع إلزام مستخدميها بالسر المهني وواجب التحفظ وإخضاعهم لإجراءات التأهيل وأداء اليمين قبل تنصيبهم[1].

للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك لما تتمتع به من مزايا تبدأ من تكلفتها البشرية والتي تتكون من جهات لها دور هام في مجال مكافحة الجريمة عموما والإلكترونية خصوصا[1].

كما أن المشرع الجزائري جعل من مهامها وظائف ردعية ووقائية عقابية ومنحها في هذا الإطار صلاحية عامة، يعود أساسها لما تمّتلك به الهيئة من تخصص ألا وهي صلاحية اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلا أنه وفي مقابل هذه الصلاحيات والمهام الهامة التي أولاها المشرع في سبيل مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلا أن دور هذه الهيئة غير فعّال في الواقع.

وقد استلهم المشرع الجزائري بجملة من العراقيل، جعلت رئيس الجمهورية يستحدث مرسوما رئاسيا 261/15، وذلك تقييما للظروف السياسية والأمنية التي عرفتها البلاد في تلك الفترة، مما أفضى إلى ظهور مخاطر فعلية للتعرض للأمن العمومي وكذلك المؤسسات الدستورية للخطر، فجاء هذا المرسوم ليغير من الطبيعة القانونية للهيئة، حيث تم نقل الإشراف عليها من وزارة العدل إلى وزارة الدفاع، مما حولها إلى هيئة ذات طابع أمني[2].

أصبحت الهيئة تُقسم ضمن مجلس التوجيه برئاسة وزير الدفاع الوطني القائد الأعلى للقوات المسلحة أي رئيس الجمهورية ومن الناحية التنظيمية، فإن نائب وزير الدفاع هو من ينوب في رئاسة الهيئة، أما ممثلو الوزارات التالية: وزارة الدفاع الوطني، وزارة الداخلية، وزارة العدل، وزارة الموصلات السلكية واللاسلكية، كلٌّ يمثل حسب مرسوم من المجلس الوزاري.

ويرأسها ممثل عام يتم تعيينه طبقًا للنظام المعمول به في وزارة الدفاع الوطني، ويتضح لنا الطابع الأمني للهيئة من خلال التشكيلة التي يغلب عليها عامل الانتساب.

---

[1] المرسوم الرئاسي 172/19 المؤرخ في 06 يونيو 2019، والذي يحدد **تشكيلة الهيئة الوطنية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتنظيمها وكيفية تسييرها**، الجريدة الرسمية، العدد 37، الصادرة في 09 يونيو 2019.

[2] نفس المرجع

إن تغيير طبيعة الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال من طبيعة قضائية، حيث كانت تخضع لإشراف القضاء، وكذلك تنوع تشكيلة الضبطية القضائية التي تقوم بإجراءات التحري وتحول هذه الهيئة إلى إشراف السلطة العسكرية ممثلة في وزارة الدفاع لا يؤثر في الحقيقة على عملها حيث أنها تبقى في مضمونها تعمل تحت رقابة القضاء.[1]

وكما صدر المرسوم الرئاسي الخاص بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية رقم 20-50 مؤرخ في 20 جانفي2020[2] بحيث يتبين من هذه المنظومة الإطار التنظيمي الذي يفرض على إعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، وبشكل من مصالح حساسة، كوكالة أمن الأنظمة المعلوماتية، وتكلف بوضع وتنفيذ السياسة الوطنية لأمن المعلومات ويترأس المجلس الوطني لأمن الأنظمة المعلوماتية وزير الدفاع الوطني أو ممثل عنه كما يُشكل أيضا من ممثل عن رئاسة الجمهورية وممثل عن وزير الداخلية ووزير المالية إضافة إلى الطاقة والاتصالات والتعليم العالي.[3]

أ_ آليات وإجراءات الحجب بإعذار من الهيئة الوطنية

عند اكتشاف محتوى إلكتروني غير مشروع، تقوم الهيئة الوطنية المختصة بإخطار مقدمي خدمات الإنترنت بضرورة منع الوصول إليه أو سحبه خلال أجل محدد، ويتم ذلك بوسائل رسمية تضمن إثبات التبليغ. ورغم أن القانون من خلال نص المادة 394 مكرر 8 لم تحدد شكلًا معينًا لهذا الإعذار، إلا أنه يجب أن يكون مكتوبًا ويتضمن بيان المحتوى المخالف والأساس القانوني للإجراء والمواقع المعنية. وفي حالة وجود نقص في الإعذار، ثار خلاف حول الجهة المختصة بالطعن فيه، بين من يراه من اختصاص القضاء الجزائي مادام الأمر يتعلق بمتابعة جزائية ، في حين يراه الدكتور مناصرة يوسف في كتابه شرعية حجب الموقع الإلكترونية بين التشريع الجزائري والمقارن، عملاً إداريًا يجوز الطعن فيه أمام القضاء الإداري باعتباره صادرا عن الهيئة الوطنية التي تعد هيئة ادراية مستقلة تتمتع بالشخصية المعنوية طبقا لأحكام

[1] المادة 13 **من المرسوم الرئاسي** 172/19 المؤرخ في 06 يونيو 2019، مرجع سابق.

[2] المرسوم الرئاسي رقم 20-50 مؤرخ في 20 جانفي 2020 والذي **يتعلق بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية.**

[3] المادة 03 من القانون رقم 38 لسنة 2021 لسنة 2021، المعدل القرار بقانون رقم 10 لسنة، **وتعديلاته بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات،** المنشور في مجلة الوقائع رقم 186 بتاريخ 2021/11/25.

المادة 3 من المرسوم 15-261 ويكون ذلك قبل مباشرة الدعوى العمومية أو أثنائها حتى تكون من الدفوعات التي يتم إثارتها أمام القاضي الجزائي للطعن في صحتها[1].

كما يمكن الاستغناء عن الإعذار إذا قام مقدم الخدمة تلقائيًا بإزالة المحتوى غير المشروع، طبقا لنص المادة 12 من القانون 04/09 مع بقاء حق المتضرر في اللجوء إلى القضاء المدني للطعن في هذا الإجراء[2]. كما يترتب على الاعذار الصحيح في حالة عدم الالتزام به المتابعة الجزائية لمقدم خدمت الإنترنت طبقا للقواعد العامة في متابعة الشخص الطبيعي والمعنوي، فمن دونه لا تستطيع النيابة مباشرة إجراءاتها باعتباره شرط للمتابعة الجزائية.

ب_ آليات وإجراءات الحجب بحكم قضائي

عند نشر محتوى إلكتروني غير مشروع، يمكن التبليغ عنه لدى الجهات القضائية أو الأمنية المختصة لاتخاذ الإجراءات القانونية المناسبة، وقد تنتهي المتابعة بالمحاكمة أو بحفظ الملف، كما يجوز للشخص المتضرر تقديم شكوى أمام مصالح الضبطية القضائية أو اللجوء مباشرة إلى قاضي التحقيق عن طريق الادعاء المدني، من أجل المطالبة بمتابعة الفاعل والتعويض عن الضرر. وفي هذه الحالة قد تصدر المحكمة حكمًا يفصل في الدعوى العمومية والدعوى المدنية التابعة لها.

ومن جهة أخرى، يمكن للمتضرر المطالبة بإزالة المحتوى غير المشروع أو منع الوصول إليه متى كان ذلك ممكنًا من الناحية التقنية، سواء بطلب من القضاء أو بمبادرة من مقدم خدمة الإنترنت بعد ثبوت مخالفة المحتوى للقانون.

وقد يختار المتضرر كذلك اللجوء إلى القضاء المدني، خاصة القضاء الاستعجالي طبقا لنص المادة 05/20، للمطالبة بحماية حقوقه وإلزام مقدم خدمة الإنترنت بالتدخل السريع لسحب المحتوى المخالف أو تعطيل الوصول إليه.

وفي حالة صدور حكم قضائي نهائي وامتناع مقدم الخدمة عن التنفيذ، يمكن مباشرة المتابعة الجزائية ضده وفق الشروط التي يحددها القانون، خاصة بعد إثبات عدم الامتثال للأوامر القضائية الموجهة إليه[3] .

---

[1] يوسف مناصرة، **شرعية حجب الموقع الإلكترونية بين التشريع الجزائري والمقارن وأثره على حرية التعبير**، دار الخلدونية، الطبعة الأولى ،2022، ص 292.

[2] يوسف مناصرة، شرعية حجب المواقع الإلكترونية بين التشريع الجزائري والمقارن، نفس المرجع، ص 294

[3] نفس المرجع.

الفرع الثالث: الآليات التقنية للحماية لأمن النظم المعلوماتية ضد القرصنة الالكترونية

استخدمت الأنظمة المعلوماتية وشبكات الحاسوب في أغراض متعددة، منها ما هو مشروع ومنها ما هو مخالف للقانون، إذ قد يتم الوصول إلى بيانات ومعلومات تخص الغير بطرق احتيالية أو من خلال إساءة استعمال هذه الأنظمة.وقد تصدى المشرّع الجزائري لهذا النوع من الأفعال من خلال تجريمه في المادة 394 مكرر من قانون العقوبات، التي نصت على أن:يُعد دخولاً أو بقاءً غير مشروع في كل نظام للمعالجة الآلية للمعطيات، ويُعاقب عليه بالحبس من ثلاثة (03) أشهر إلى سنة (01) وبغرامة من 50.000 دج إلى 200.000 دج، أو بإحدى هاتين العقوبتين فقط[1]

كما قد تناولنا ظروف التشديد التي نصت عليها المادة 394 مكرر 1 العقوبة إذا نتج عن هذا الدخول أو البقاء غير المشروع حذف أو تغيير للبيانات أو تسبب في تعطيل النظام المعلوماتي. وكذا الجهود الدولية والمؤسساتية للحماية من خطر الهجمات السيبيرانية.

من جهة أخرى توجد هناك طرق تقنية للحماية ولأمن المعلومات، تتجسد في الحماية المادية فهناك العديد من الطرق البسيطة التي يتبعها المعلوماتيون لتجنب أي اختراق على أجهزتهم نتناولها في هذا المطلب في الفروع التالية:

أولا: الجدران النارية آلية تأمين الأنظمة المعلوماتية Firewalls

نظرا لانتشار الواسع حاليا لقرصنة المعلومات و التجسس المعلوماتي وذلك بسبب انتشار برامج القرصنة ووجودها في الكثير من المواقع أصبح من الممكن اختراق أي جهاز أو نظام معلوماتي و بدون عناء فور إنزال إحدى البرامج و خاصة مع وجود ثغرات في الأجهزة أو الأنظمة ومن أثار تلك التهديدات التعرض للسرقة و الاحتيال عن طريق تغيير المعلومات التي يتم إدخالها في النظام أو تغيير المخرجات التي تخرج منه التجسس الصناعي عن طريق تنزيل الأسرار الصناعية من الكمبيوتر إلى إحدى الشركات و إرسالها عبر البريد الإلكتروني مباشرة إلى منافستها، الأمر الذي يستدعي ضرورة إيجاد آليات مواجهتها من بينها الجدران النارية[2]

الجدار الناري هو عبارة عن جهاز، أو تطبيق، ويتم وضعه عند الخادم، وعند مصافي الشبكة، كل حسبّ إن احتياجاته وقد جاءت فكرة الجدار الناري من الطريقة الأمنية المعروفة قديما وهي عبارة عن حفر

[1] المادة 394 مكرر من قانون العقوبات الجزائري

[2] صورية بورباية، **قواعد الأمن المعلوماتي**، رسالة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس،2016-2015، ص53-51.

خندق حول قلعة لمنع أي شخص من الدخول أو الخروج من القلعة ويمكن تفتيشه من قبل الحراس على القلعة، لذا يقصد بالجدار الناري :" مجموعة أنظمة توفر سياسات أمنية بين الإنترنيت والشبكة الخاصة لتصبح جميع عمليات العبور إلى الشبكة أو الخروج منها تمر من خلال الجدار الناري الذي يصد المستعملين غير المرغوب فيهم"، فالجدار الناري يقوم بالتحقق من صلاحية المستعمل المحلي والمستعمل الخارجي ونظام الدخول والخروج وتشفير المعلومات، وإجراءات الحماية من الفيروسات.[1]

من المزايا التي يوفرها الجدار النّاري هي:

1-توفير الحمأَية اللازمة للشبكة والمعلومات، وكذا توفير خدمات التشفير في تكنولوجيا الجدار الناري.

2-يعمل الجدار الناري على تخزين العمليات والمعلومات التي تمر من خلاله.

3-تتبع كل مستخدمي الشبكة وإصدار إنذار في حالة العبث فيها.

إذن فالجدار الناري يضمن حماية الأفراد الطبيعة والمعنوية ويعمل على تحصين الأجهزة ضد أي اختراق يمس ببياناتها.

ويهدف هذا التجريم إلى حماية الأنظمة المعلوماتية من أي اختراق أو اعتداء غير قانوني، وضمان أمن المعطيات وسلامتها لما تمثله من أهمية في حياة الأفراد والمؤسسات. [2]

فالمساس بها يهدد الأمن المعلوماتي والاقتصادي والاجتماعي للدولة، الأمر الذي استوجب تدخل المشرّع لوضع إطار قانوني رادع يضمن حماية المعطيات والثقة في تكنولوجيا الإعلام والاتصال.

ثانيا: البصمة الإلكترونية

تزامن ظهور البصمة الإلكترونية التوقيع الإلكتروني، وبوجه خاص التوقيع الرقمي.

والبصمة الإلكترونية هي عبارة عن إحدى تقنيات التشفير باتجاه واحد التي تهدف إلى الحصول على ما يسمى بـ مفتاح الشفرة. وتتميز هذه التقنية بكونها لا تسمح بفك التشفير أو استرجاع الرسالة الأصلية من المفتاح الناتج، ولهذا السبب سُمّي هذا الأسلوب بأسلوب التشفير أحادي الاتجاه. ويُستخدم هذا النوع من

[1] الجواد دلال صادق، **أمن المعلومات**، دار اليازوري العلمية للنشر والتوزيع، الأردن 2008، ص41 وما يليها.

[2] حزام فتيحة، **مرجع سابق**، ص 175.

التشفير عادةً في الأنظمة التي تتطلب التحقق من صحة المعلومات دون الحاجة إلى معرفة محتواها الأصلي[1].

ففي هذا النظام، يؤدي تشفير نفس الرسالة بنفس الخوارزمية دائمًا إلى إنتاج نفس مفتاح الشفرة، مما يجعله وسيلة فعالة للتحقق من سلامة البيانات وعدم التلاعب بها. فعلى سبيل المثال، إذا حصلنا على بيانات من مصدر معيّن، يمكننا عبر مقارنة بصمتها الإلكترونية بالبصمة الأصلية التأكد مما إذا كانت هذه البيانات قد تعرضت لتغيير متعمد (كالهجوم أو الفيروسات)، أو تعديل غير مقصود أثناء عملية التحميل من الإنترنت بسبب خطأ تقني في الاتصال[2].

وبالتالي، تُستخدم البصمة الإلكترونية أو ما يعرف بالتشفير باتجاه واحد غالبًا في التوقيع الرقمي من أجل التأكد من سلامة وصحة البيانات المنقولة إلكترونيًا عبر الوسائط المختلفة.

ومن هذا المنطلق، سعى المشرّع الجزائري إلى مواجهة هذه التحديات من خلال حماية المعطيات أثناء معالجتها بالوسائل الإلكترونية، وذلك عبر القانون رقم 04-15 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، لا سيما في القسم السابع المعنون بالاعتداء على أنظمة المعالجة الآلية للمعطيات[3]. كما تضمّن قانون الإجراءات الجزائية أحكامًا تهدف إلى منع إساءة استخدام السلطة أو انتهاك الحق في الحياة الخاصة، خصوصًا في المواد 44 وما يليها، التي كفلت هذه الحماية كأصل قانوني عام[4].

ثالثا: آليات منع إفشاء المعلومات

نظرًا لتزايد المخاطر التي تهدد سرية المعلومات وخصوصيتها، أصبح من الضروري اعتماد وسائل وقائية فعّالة لضمان حماية البيانات من أي اختراق أو إفشاء غير مشروع. فقد أتاح التطور الهائل في تقنيات المعلومات والاتصال إمكانية تخزين كميات ضخمة من البيانات الشخصية وجمعها ومعالجتها من

---

[1] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، المحاكمة الإلكترونية _دراسة تحليلية مقارنة مدعمة بالفقه والقضاء المقارن، دار العلا، الجزائر، ص 182.

[2] خالد حسن أحمد لطفي، **الأمن المعلوماتي، التهديدات والتدابير التشريعية والتقنية لحمايته**، مرجع سابق، ص 134.

[3] أرزقي سي حاج محند، **مرجع سابق**، ص 175.

[4] أسست على المستوى الدولي أول رقابة على معالجة المعطيات ذات الطابع الشخصي في فرنسا سنة 1978 تحت تسمية اللجنة الوطنية للمعلوماتية والحريات، أدخل المشرع الجزائري هذه المؤسسة في نظام حماية المعطيات ذات الطابع الشخصي منظما أحكامها في المواد من **22 إلى 31 ومن 46 إلى 48**. فكرة الهدف من تأسيس السلطة الوطنية في التشريع الجزائري، أوردتها المادة **25** التي نصها،" **تكلف السلطة الوطنية بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي إخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة** ".

قبل المؤسسات الحكومية، والهيئات الإدارية، والشركات الخاصة، مما جعل مسألة الحفاظ على الخصوصية أكثر تعقيدًا من أي وقت مضى.

كما يمكن اليوم تخزين هذه البيانات في قواعد مؤمنة ونقلها بسهولة وسرعة بين مختلف المناطق، وفي غضون ثوانٍ معدودة، وبأقل التكاليف، الأمر الذي يبرز حجم التحدي الذي تواجهه الأنظمة الحديثة في ضمان حماية الخصوصية المعلوماتية.

إن انتشار التقنيات المتطورة مثل أنظمة المراقبة، وبطاقات الهوية الذكية، وقواعد البيانات المركزية، يزيد من احتمالية انتهاك الخصوصية الفردية، مما يستدعي اعتماد إجراءات صارمة لحماية البيانات من أي تهديدات إلكترونية.

ومن هذا المنطلق، أصبحت وسائل أمن المعلومات تمثل مجموعة من الآليات **التقنية والتنظيمية** التي تهدف إلى الوقاية من المخاطر المعلوماتية وتقليل احتمالات الاختراق أو التلاعب بالأنظمة الإلكترونية. وتشمل هذه الوسائل استخدام التشفير، والمراقبة الأمنية، ونظم الكشف عن التسلل، وسياسات التحكم في الوصول إلى المعلومات.

أ_ أنظمة الحماية التقنية في المصارف الإلكترونية

تحرص المصارف الإلكترونية على تبني أنظمة حماية متطورة تضمن سرية المعاملات البنكية وسلامة بيانات العملاء. وتستند هذه الأنظمة إلى مجموعة من التقنيات مثل:

التشفير الإلكتروني لحماية المعلومات أثناء نقلها عبر الشبكات.

1_آليات التحقق من هوية المستخدمين ككلمات المرور والتواقيع الرقمية.

2_أنظمة الجدار الناري والكشف عن التسلل لمراقبة أي نشاط غير مألوف.

3_ سياسات داخلية صارمة تحدد صلاحيات الوصول إلى البيانات الحساسة.

وبذلك تسعى المصارف إلى تحقيق توازن بين سهولة الخدمات الإلكترونية وضمان أمن المعلومات، لأن الثقة في النظام المصرفي الإلكتروني تعدّ الأساس الرئيس لنجاح التعاملات الرقمية

سعيًا من المصارف الإلكترونية إلى توفير الحماية التقنية لعمليات الدفع الإلكتروني ووسائلها، قامت هذه المصارف بوضع أنظمة خاصة تُمكّنها من أداء مهامها بدرجة عالية من السرية والموثوقية، حيث تتيح

لها التحقق من هوية العميل المتعامل معها، وتؤكد — في حال استخدامها بشكل صحيح — أن من يقوم بالعملية هو فعلاً صاحب الحساب. وتُعد هذه الأنظمة من قبيل التواقيع الإلكترونية المؤمّنة، ومن أبرزها ما يلي[1]:

1: نظام هوية المستخدم وكلمة السر

يُعد هذا النظام الأكثر شيوعًا في المعاملات المصرفية الإلكترونية. فعند دخول العميل إلى موقع البنك عبر الإنترنت للاستفادة من الخدمات الإلكترونية، يُطلب منه إدخال هوية المستخدم وكلمة السر. ويُعتبر إدخالهما وسيلة للتحقق من الشخصية، ودليلًا على أن الشخص الذي قام بالعملية هو صاحب الحساب الحقيقي.

وفي حال كان موقع البنك يسمح بإجراء العمليات بمجرد الدخول إليه باستخدام الهوية وكلمة السر، فإن هذين العنصرين يُعدّان دليلًا على اتجاه إرادة العميل والتزامه بمضمون العملية التي أجراها.

ويُعتبر هذا النظام بمثابة توقيع إلكتروني، لأنه لا يمكن تنفيذ أي عملية دون إدخال هوية المستخدم وكلمة السر، وهما بذلك مرتبطان برسالة المعلومات الخاصة بالعملية المنفذة، وباعتبارهما خاصين بالعميل وحده، فهما يُميزان شخصيته ويُعبّران عن إرادته في الالتزام بمضمون العملية.

2: نظام كلمة السر التي لا تتكرر(One-TimePassword)

تُسمّى هذه الطريقة كلمة السر التي لا تتكرر لأنها تُستخرج من جهاز توثيق خاص وتكون صالحة لمرة واحدة فقط وخلال مدة زمنية محددة (عادة دقيقة واحدة). وتُعد هذه الكلمة بمثابة توقيع إلكتروني مؤقت، إذ يتم إنشاؤها وفق خوارزمية رياضية تُعرف باسم القيمة الاختبارية(Checksum) ، وهي مجموعة من العمليات الحسابية التي تُستخدم للتحقق من سلامة البيانات وعدم تزويرها.

يُستخدم هذا النظام كوسيلة إضافية للنظام السابق، حيث تعتمد عليه بعض البنوك عند تنفيذ العمليات التي تتضمن أوامر دفع أو معاملات تؤثر على الذمة المالية للعميل.

ويتم ذلك من خلال تعاون العميل والبنك للوصول إلى كلمة السر التي لا تتكرر، إذ يُزوَّد كلٌّ منهما في البداية بجملة مرور واحدة وعدد محدد من مرات تطبيق الخوارزمية، حيث تُجرى عمليات حسابية لإنتاج سلسلة من الحروف ذات طول معين، مشتقة رياضيًا من رسالة أطول تمثل البيانات المراد تشفيرها.

[1] حزام فتيحة، **مرجع سابق**، ص 178-179.

ويُستخدم هذا النظام أيضًا لاكتشاف أي تغيير في البيانات الأصلية، حيث إن أي تعديل ولو بسيط في الرسالة يؤدي إلى تغيير كبير في القيمة الاختيارية.

وتتم العملية وفق ثلاث مراحل رئيسية

المرحلة التمهيدية: يُدخل العميل جملة المرور، ثم تُضاف إلى الرقم العشوائي الذي يُرسله البنك، وتُرسل النتيجة إلى البنك.

مرحلة التوليد: تُنفّذ خوارزمية القيمة الاختيارية عدة مرات لإنتاج كلمة السر المؤقتة، ويُخزَّن عدد مرات التنفيذ في جهازي العميل والبنك.

مرحلة الإخراج: يتم توليد كلمة السر ذات 64 خانة (Bit) تُستخدم مرة واحدة فقط.

ويعتمد عمل الحاسوب الآلي على تحويل المعلومات بجميع أشكالها (بيانات مكتوبة، صوت، صورة) إلى أرقام ثنائية (Binary)، وسُميت كذلك لأنها تتكوّن من رمزين فقط يمثلان النظام الرقمي الثنائي المستخدم في جميع العمليات الإلكترونية[1].

ب_ التدابير التنظيمية

لا يكفي الاعتماد على الوسائل التقنية وحدها، مثل أنظمة الحماية وبرامج مكافحة البرمجيات الضارة، لضمان أمن المعلومات داخل المؤسسة، وإنما يجب وضع إطار تنظيمي يحدد الضوابط التي تحكم حماية الأسس المعلوماتية، وبالتالي فان سياسة أمن المعلومات هي الوثيقة التي يتم اعتمادها لتبيين التوجهات العامة للمؤسسة في المجال المعلوماتي وتحديد الأهداف التي يسعى إلى تحقيقها دون الخوض في التفاصيل الفنية والاجرائية الخاصة بالتنفيذ[2].

ولكي يتحقق ذلك لابد من اتباع الشروط التالية:

1_ أن تكون السياسة مكتوبة وواضحة لجميع المستخدمين.

2_ ان تتميز بالاختصار والتركيز مع تجنب الغموض والتعقيد

3_ يجب صياغتها بطريقة منظمة ومنسجمة وملائمة تسهل تطبيقها

---

[1] خالد مصطفى فهمي، **النظام القانوني للتوقيع الإلكتروني في ضوء الاتفاقات الدولية والتشريعات العربية**، دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص 101-102.

[2] خالد حسن أحمد لطفي، **الأمن المعلوماتي التهديدات والتدابير التشريعية والتقنية لحمايته**، مرجع سابق، ص 130.

4_أن تحقق توازنا بين متطلبات الحماية واستمرارية الأداء والإنتاج

5_أن تحدد المسؤوليات والصلاحيات الملقاة على كل طرف

6_ أن تبين الأهداف الأساسية للسياسة الأمنية

7_ تعريف المستخدمين بحقوقهم واجباتهم فيما يتعلق باستخدام الأنظمة المعلوماتية[1].

تمثل سياسة أمن المعلومات الركيزة الأساسية في بناء منظومة أمنية فعالة، فهي توفر مرجعا موجدا يوجه جميع التدابير التقنية والإدارية الرامية إلى حماية المعلومات وتقليل المخاطر التي قد تتعرض لها.

[1] خالد حسن أحمد لطفي، نفس المرجع

خاتمة الفصل الثاني:

في ختام هذا الفصل المخصص للإطار الإجرائي ومكافحة جريمة القرصنة الإلكترونية، يتضح أن المواجهة القانونية لهذه الظاهرة لم تقتصر على النصوص الموضوعية التي تجرم الفعل فقط، بل أصبحت ترتكز على فعالية الآليات الإجرائية التي تكفل الكشف عنها إثباتها ملاحقة مرتكبيها، فخصوصية الجريمة المعلوماتية، من حيث طابعها غير المادي وعابرها للحدود الجغرافية وسرعة ارتكابها وإخفاء أثارها، تفرض تطويرا مستمرا في قواعد التحقيق والمحاكمة، وكذا في وسائل الإثبات آليات المحاكمة.

ففيما يتعلق بالمبحث الأول، المتعلق بإجراءات التحقيق والمحاكمة، تبين أن المشرع سعى إلى تكييف القواعد الإجرائية التقليدية مع خصوصيات البيئة الرقمية، من خلال إقرار وسائل حديثة كالتحقيق التقني، والتفتيش الإلكتروني، واعتراض المراسلات، وتتبع البيانات، مع إخضاعها لضمانات قانونية تحافظ على التوازن بين متطلبات الأمن الرقمي وحماية الحقوق والحريات الفردية، خاصة الحق في الخصوصية وسرية المراسلات، كما أن فعالية المحاكمة تبقى رهينة بمدى تكوين القضاة أعوان العدالة في المجال التقني، إلى جانب تعزيز التعاون القضائي الدولي نظرا للطابع العابر للحدود لهذه الجرائم .

كما يظهر من خلال التنظيم الإجرائي الحديث أن المشرع الجزائري قد عمل على تعزيز فعالية العدالة الجزائية من خلال استحداث الأقطاب الجزائية المتخصصة، التي تعد آلية مؤسساتية تهدف إلى تجميع الخبرات القضائية والتقنية في معالجة الجرائم ذات الطابع المعقد، وعلى رأسها الجرائم المعلوماتية والاقتصادية، بما يضمن سرعة الفصل ودقة المعالجة.

وفي هذا الإطار، يتجلى نهج المشرع الجزائري من خلال القانون رقم 25-14 لسنة 2025 كمحطة تشريعية هامة في تطوير المنظومة الإجرائية الجزائية، وكذا تدعيم اليات مكافحة الجريمة كمبحث ثاني ، حت تتكيف هاته الإجراءات مع التطور التكنولوجي.

وعليه، فان مكافحة جريمة القرصنة الإلكترونية تقتضي مقاربة شاملة ومتكاملة، تجمع بين الفعالية الإجرائية، والتطور التقني، والتعاون الدولي، في إطار احترام دولة القانون وضمانات المحاكمة العادلة، فكلما كان النظام الإجرائي مرنا ومتطورا، كلما زادت قدرته على التصدي لهذه الجرائم المستحدثة، وتحقيق الردع وحماية المجتمع الرقمي.

الخاتـــــمـــــة

الخـاتمـة

في ختام هذه الدراسة التي ترتبط بموضوع جريمة القرصنة الإلكترونية التي تعد ظاهرة قانونية متعددة الأبعاد، نظرا لارتباطها المباشر بالتطور التكنولوجي وسهولة انتشارها وصعوبة اكتشافها وإثباتها وقد بينت الدراسة أن هذه الجريمة تستدعي تحديدا دقيقا لمفهومها وتمييزها عن غيرها من الجرائم المعلوماتية، كما تم الوقوف على خصائصها التي تجعلها مختلفة عن الجرائم التقليدية، من حيث طابعها غير المادي، فيظهر أن المشرع بالرغم من محاولاته مواكبة التطور، لا يزال يواجه صعوبات في الإحاطة بكافة صورها المستحدثة مما يفرض ضرورة التحديث المستمر للنصوص القانونية وتوحيد المفاهيم ذات الصلة بها .

كما أصبحت من أبرز التحديات الأمنية والقانونية في العصر الرقمي، لما تسببه من تهديد مباشر للأفراد، والمؤسسات، والدول على حدّ سواء، كونها لا تقتصر على سرقة البيانات أو اختراق الأنظمة، بل تمتد آثارها إلى زعزعة الثقة في الفضاء الرقمي، وتعطيل الخدمات الحيوية، والتأثير في الاستقرار العام. كما أنّ الطابع العابر للحدود لهذه الجرائم يجعل مكافحتها صعبة، ويبرز الحاجة إلى تعاون دولي فعّال، وتبادل للمعلومات والخبرات التقنية بين الدول.

لقد بات من الضروري اليوم تعزيز الوعي الأمني الرقمي لدى المستخدمين، وتطوير التشريعات الوطنية والدولية بما يواكب التطورات التقنية المتلاحقة، إضافة إلى توطيد التعاون الدولي من أجل مكافحة هذه الجرائم التي تتخطى الحدود الجغرافية بسهولة.

كما يُعدّ تفعيل القانون رقم 09-04 في الجزائر خطوة مهمة في سبيل حماية الفضاء السيبراني، خاصة فيما يتعلق بجرائم الدخول والبقاء غير المشروعين التي يقوم بها ما يُعرف بالهاكرز. فمواجهة هذه الظاهرة تتطلب تضافر جهود الدولة، والمؤسسات، والأفراد، لبناء بيئة رقمية آمنة قائمة على الوعي والمسؤولية واحترام القوانين. فالمستقبل الرقمي الواعد لن يتحقق إلا بتوظيف التكنولوجيا في خدمة التنمية والأمن، والحد من توظيفها في ارتكاب الأفعال الإجرامية التي تهدد استقرار المجتمعات.

ومن خلال هذه الدراسة المعمقة للموضوع نستخلص بدورنا جملة من النتائج التي تعكس أهم ما تم التوصل إليه من الجانبين المفاهيمي والإجرائي:

الخـاتمـة

القرصنة الإلكترونية هي كل فعل غير مشروع يتم من خلال استخدام الأنظمة أو الشبكات المعلوماتية بهدف الوصول غير المصرح به إلى البيانات أو البرامج أو الأنظمة، سواء بغرض التلاعب بالمعلومات أو سرقتها أو تعطيلها أو استغلالها لأغراض شخصية أو مالية أو سياسية، ومنه هي الجرائم الحديثة التي يصعب ضبط مفهومها بدقة بسبب تطور وسائل ارتكابها وتعدد صورها.

تختلف جريمة القرصنة الإلكترونية عن بعض الجرائم والمفاهيم المشابهة لها، من خلال طبيعة السلوك الإجرامي والهدف منه، فالقرصنة الالكترونية تعد أوسع من مجرد الدخول غير المشروع الى الأنظمة المعلوماتية، لأنها قد تشمل تعديل البيانات او سرقتها أو تعطيل الأنظمة او استغلالها بطرق غير مشروعة.

توصلنا من خلال الدراسة السابقة أن القرصنة الالكترونية تختلف عن الغش المعلوماتي، حيث يهدف الغش إلى تحقيق منفعة مالية عبر التلاعب بالمعطيات، بينما قد تكون دوافع القرصنة التخريب أو التجسس أو الوصول غير المشروع إلى المعلومات.

وكذا الامر بين القرصنة الإلكترونية والتجسس الإلكتروني، إذ يقتصر التجسس على جمع المعلومات السرية دون المساس بالأنظمة، في حين قد تتضمن القرصنة التخريب أو التعطيل أو السيطرة على النظام المعلوماتي.

و بين القرصنة الإلكترونية وسرقة البيانات، فهذه الأخيرة تقوم على الاستيلاء غير المشروع على المعلومات، بينما قد تتحقق القرصنة حتى دون سرقة البيانات، بمجرد اختراق النظام أو العبث به.

وبينا أن القرصنة الإلكترونية تختلف عن الإرهاب الإلكتروني، لأن هذا الأخير يتجاوز مجرد الاختراق ليهدف إلى بث الرعب وتهديد أمن الدولة أو استقرار المجتمع من خلال استخدام الوسائل المعلوماتية وعليه استنتجنا أن:

1-القراصنة هم أشخاص يمتلكون مهارات تقنية متقدمة في نظم المعلومات والشبكات، يستخدمون هذه المهارات لاختبار الأنظمة أو اختراقها، ويختلف هدفهم وطبيعة أفعالهم باختلافهم، فمنهم من يسعى لتحسين الأمن ومنهم من يسعى للإضرار أو الربح غير المشروع.

2-تعتبر القرصنة الإلكترونية من أبرز التحديات التي تواجه حماية حقوق الملكية الفكرية في العصر الرقمي، عن طريق تسهيل عملية نسخ وتبادل المصنفات الفكرية دون إذن من أصحابها.

3-خصائص جرائم القرصنة الالكترونية على اختلافها تخلق عرقلة في إثبات هذا النوع المستحدث من الجرائم.

4-أظهرت الدراسة أن النصوص القانونية رغم أهميتها، لا تزال تعاني من قصور نسبي في مواكبة التطور التكنولوجي المتسارع.

5-يشكل الدليل الرقمي الركيزة الأساسية في إثبات هذه الجرائم، غير أنه يثير إشكالات تتعلق بحجيته وسلامته وإجراءات جمعه.

6-تبين أن فعالية إجراءات التحقيق والمحاكمة تعتمد بشكل كبير على مدى توفر الوسائل التقنية والخبرة الفنية لدى الجهات المختصة.

7_لا يمكن تحقيق مكافحة فعالة لجريمة القرصنة الإلكترونية دون تطوير مستمر للإطارين التشريعي والإجرائي بما يتلاءم مع طبيعتها المتغيرة.

8_إن التوازن بين متطلبات مكافحة الجريمة وحماية الحقوق والحريات يعد ضرورة أساسية في هذا المجال، خاصة فيما يتعلق بسرية المعطيات والخصوصية.

9_تعتمد فعالية المواجهة بشكل كبير على تكامل الجهود بين مختلف الجهات، سواء على المستوى الوطني أو الدولي.

وعلى سياق هاته النتائج والاستنتاجات أقدم جملة من التوصيات تتمثل في التالي:

1_سد الفراغ التشريعي في مجالات البيئة الرقمية، وإصدار مذكرات توضيحية للتشريعات الخاصة بمكافحة الجريمة الإلكترونية.

2_ الإسراع في رقمنة الإدارة العمومية، مع تكثيف برامج تكوين الموظفين وتدريبهم على استخدام التقنيات الرقمية، بما يضمن مواكبة التحول الرقمي وتحسين أداء المرافق العمومية

3_إنشاء مراكز وطنية للاستجابة لطوارئ الحاسب وتعزيز الأمن المعلوماتي.

4_دعم الجهات القضائية والنيابة العامة بالمساعدة الفنية والوسائل التقنية لمكافحة الجريمة الإلكترونية.

5_ تعزيز وتطوير المضامين التعليمية المتعلقة بالحاسب الآلي والشبكات المعلوماتية ضمن مناهج كليات الحقوق، بما يتماشى مع التطورات التكنولوجية المستجدة.

6_ تعزيز قدرات أجهزة الشرطة القضائية المختصة بالجرائم المعلوماتية، وتطوير كفاءاتها التقنية بما يتماشى مع التطورات المستمرة في هذا المجال..

7_ تكثيف الجهود الوطنية لنشر الوعي الرقمي والوقاية من مخاطر الجرائم الإلكترونية.

8_ تعزيز الجهود الدولية الرامية إلى مكافحة الجريمة المعلوماتية، من خلال صياغة إطار شامل ومتعدد الأطراف يضع معالجات قانونية دولية في مجالات التجريم، والصلاحيات الإجرائية، والآليات القضائية، والتعاون الدولي

9_مراجعة الأحكام القانونية المتعلقة بجريمة القرصنة الإلكترونية في التشريع الجزائري، بما يضمن وضوح الأفعال المجرّمة وتحديد نطاق التجريم وفقًا لمبدأ الشرعية الجنائية

10_تعزيز فعالية إجراءات التحري والتحقيق في جرائم القرصنة الإلكترونية، بما يتلاءم مع الطبيعة التقنية للاختراقات غير المشروعة لأنظمة المعالجة الآلية للمعطيات

11_تطوير آليات جمع الأدلة الرقمية وحفظها وفحصها، بما يضمن سلامتها وإمكانية الاستناد إليها في إثبات جرائم القرصنة الإلكترونية أمام الجهات القضائية

12_تعزيز التكوين المتخصص للقائمين على التحقيق في جرائم القرصنة الإلكترونية، لا سيما في مجال الكشف عن أساليب الاختراق وتحليل الآثار الرقمية المرتبطة بها

13_تعزيز التنسيق بين الجهات القضائية والجهات التقنية المختصة في التعامل مع جرائم القرصنة الإلكترونية، بما يسهم في تسهيل كشف هذه الجرائم وتحديد المسؤولين عنها

14_تقييم مدى كفاية الأحكام الجزائية المقررة لجريمة القرصنة الإلكترونية في التشريع الجزائري، بما يحقق التناسب بين خطورة الأفعال المرتكبة والعقوبات المقررة لها

15_تعزيز التعاون القضائي الدولي في جمع الأدلة الرقمية وتحديد مرتكبي جرائم القرصنة الإلكترونية عندما تتجاوز الأفعال المرتكبة حدود الإقليم الوطني.

16_استحداث تشريعات نموذجية لمكافحة الجريمة المعلوماتية قابلة للتطبيق عالميًا، مع مراعاة التشريعات الوطنية والإقليمية القائمة، على أن يتم ذلك برعاية الأمم المتحدة وبمشاركة مختلف الفاعلين في هذا المجال.

17_تعزيز الجهود الدولية الرامية إلى مكافحة الجريمة المعلوماتية، من خلال صياغة إطار شامل ومتعدد الأطراف يضع معالجات قانونية دولية في مجالات التجريم، والصلاحيات الإجرائية، والآليات القضائية، والتعاون الدولي.

18_حثّ الدول العربية على إبرام اتفاقية عربية مشتركة على غرار الاتفاقية الأوروبية، بهدف تعزيز التعاون القضائي والشرطي بمختلف أشكاله، لمواجهة التحديات الإجرائية الناتجة عن الجرائم المعلوماتية العابرة للحدود.

19_توحيد التشريعات الخاصة بالفضاء المعلوماتي وتشجيع الاستخدام الآمن للإنترنت داخل المنطقة العربية، لضمان انسجام القواعد القانونية وتفعيل الحماية الرقمية.

20_توسيع آليات التعاون العربي في مجال مكافحة الجريمة المعلوماتية، من خلال فتح قنوات فعالة لتبادل المساعدة القانونية المتبادلة وتسريع الاستجابة في القضايا ذات الطابع العابر للحدود.

21_ تكييف القانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها من أجل مواكبة التطورات التكنولوجية في مجال البيئة الرقمية، ومنه سن قوانين جديدة وخاصة تتناسب مع هذه الجرائم وخاصة جريمة القرصنة الإلكترونية باعتبارها أخطر الجرائم الإلكترونية

22_ عدم الاكتفاء بالنصوص القانونية المنصوص عليها في قانون العقوبات ومنه استحداث قانون خاص ومتكامل لمكافحة القرصنة الالكترونية، يتضمن تعريفا دقيقا لمختلف صور الاعتداء مع التحديد الدقيق لأركان الجريمة وعقوبات المقررة لها وكذا تجريم الأفعال المستحدثة الناتجة عن التطور التكنولوجي خاصة

23_ استحداث أحكام جزائية خاصة بجرائم القرصنة الالكترونية والتلاعب بالبيانات والمحررات الرقمية، مع تشديد العقوبات متى استهدفت هذه الأفعال المرافق العمومية أو المؤسسات الحيوية أو ترتب عنها المساس بالأمن المعلوماتي للدولة.

24_ مراجعة النصوص الحالية بصفة دورية لتكييفها مع المستجدات التقنية والجرائم السيبيرانية المستحدثة، بما يضمن سد الفراغ التشريعي وتحقيق حماية قانونية فعالة للبيانات والأنظمة المعلوماتية.

قائمة المصادر والمراجع

قائمة المراجع

قائمة المصادر والمراجع:

أولاً: المصادر الشرعية

- صحيح مسلم، كتاب البر والصلة والآداب، باب تحريم الظن والتجسس والتناجي .

ثانياً: التشريعات الوطنية الجزائرية

- الأمر رقم 66-155 المؤرخ في 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم .(الملغى)
- الأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم .
- القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .
- القانون رقم 04_15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.المعدل بموجب القانون رقم 24_06
- الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة.
- القانون رقم 2000_03 المؤرخ في 2000/08/05م المحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.
- الأمر رقم 03-07 المتعلق ببراءة الاختراع .
- القانون رقم 05-18 المتعلق بالتجارة الإلكترونية .
- القانون رقم 18_07 المتعلق بحماية المعطيات ذات الطابع الشخصي.المعدل بموجب القانون25_11 الموافق 2025
- القانون رقم 20-04 المعدل لقانون الإجراءات الجزائية .
- القانون رقم 26_02 المتضمن قانون التوقيع الالكتروني.
- المرسوم الرئاسي رقم 15-261 المتعلق بالهيئة الوطنية للوقاية من الجرائم المعلوماتية .
- المرسوم الرئاسي رقم 19-172 المتعلق بالهيئة الوطنية للجرائم المعلوماتية .
- المرسوم الرئاسي رقم 20-50 المتعلق بمنظومة أمن الأنظمة المعلوماتية .
- القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية المؤرخ في3 غشت2025.

ثالثاً: التشريعات المقارنة والاتفاقيات الدولية

- قانون العقوبات الفرنسي، المادة 323-1 المعدل بموجب القانون رقم 2023_22
- قانون الجرائم الإلكترونية الفلسطيني رقم 38 لسنة 2021 .
- قانون الاحتيال المعلوماتي البلجيكي 2000.
- معاهدة بودابست لمكافحة الجريمة المعلوماتية 2001.
- معاهدة الويبو WIPO لحقوق المؤلف1996/12/20 .
- مشروع القانون العربي الموحد لمكافحة الجرائم المعلوماتية 2009.
- الاتفاقية الدولية حول الاجرام المعلوماتي التي أبرمت بتاريخ: 2001/11/18، من طرف المجلس الأوروبي وتم التوقيع عليها منذ تاريخ 2001/11/23.
- اتفاقية برن الدولية لحماية المصنفات الأدبية والفنية المؤرخة في: 1886/06/09.

رابعاً: المعاجم والمراجع العامة

- مجمع اللغة العربية، معجم القانون، 1999 .
- الرازي، مختار الصحاح، المكتبة العصرية، بيروت .

خامساً: الكتب والمؤلفات العربية

- أحمد مختار عمر، المعجم العربي المعاصر، عالم الكتب، القاهرة، 2004 .
- امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار همة، الطبعة الثانية، الجزائر، 2007.
- أبو الفتوح درويش، عبد الكريم، *الإدارة الاستراتيجية لمكافحة الجرائم المستحدثة*، أكاديمية شرطة دبي، 2003.
- أحمد فتحي سرور، *الوسيط في قانون الإجراءات الجنائية*، دار النهضة العربية، القاهرة، 1981.
- أسامة عبد الله قايد، شرح قانون الإجراءات الجنائية، 2007 .
- أمير فرج يوسف، العالم ما وراء التقليدي ميتافريس ومستقبل العالم الافتراضي وتطور الجريمة الرقمية والمعلوماتية الالكتروني، مركز المحمود لتوزيع الكتب القانونية، الطبعة الاولى، 2024.

قائمة المراجع

- أمير فرج يوسف البلطجة الالكترونية كشكل من أشكال التهديد الابتزاز الالكتروني ووسائل مكافحتها القانونية دراسة قانونية مقارنة، مركز المحمود لتوزيع الكتب القانونية، الطبعة الألى 2024.
- أحسن بوسقيعة الوجيز في القانون الجزائي العام، الطبعة الثانية والعشرون، دار بلقيس، الجزائر،2025.
- أرزقي سي حاج محند، حماية المعطيات ذات الطابع الشخصي، في القانون الجزائري والقانون المقارن، منشورات بغدادي،2023
- أحمد حسين خميس، الهاكرز: طرق الاختراق وأساليب الحماية، المركز المصري لتبسيط العلوم، الاسكندرية، 2001 .
- أشرف السعيد أحمد، القرصنة الإلكترونية، مطابع الشرطة للطباعة والنشر والتوزيع، مصر، 2013 .
- إسماعيل محمود الرزاز، الهجمات والجرائم السيبيرانية، مركز المحمود لتوزيع الكتب القانونية، الطبقة الاولى، مصر، 2023
- بشرى حسين الحمداني، القرصنة الإلكترونية: أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، الأردن_ عمان، الطبعة الأولى، 2014.
- باسم محمد فاضل، حماية الخصوصية عبر البيئة الرقمية، دراسة تحليلية، دار الفكر الجامعي، الاسكندرية، 2021.
- حاتم عبد الرحمان منصور الشحات، الإجرام المعلوماتي، دار النهضة العربية، القاهرة، 2002 .
- حسين طاهري، جرائم القرصنة الإلكترونية (دراسة مقارنة)، دار الخلدونية، الطبعة الأولى، 2023 .
- حسين طاهري، إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية، المحاكمة الإلكترونية _دراسة تحليلية مقارنة مدعمة بالفقه والقضاء المقارن، دار العلا، الجزائر.
- حسين طاهري، *جرائم القرصنة الإلكترونية*، دار الخلدونية، الجزائر، 2023.
- حسين طاهري، إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية، المحاكمة الالكترونية، دراسة تحليلية مقارنة مدعمة بالفقه والقضاء المقارن، دار الأولى، الجزائر، 2023.
- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، 2014.
- خالد حسن أحمد لطفي، *الأمن المعلوماتي*، دار الفكر الجامعي، 2021.

قائمة المراجع

- خالد حسن أحمد لطفي، *جرائم الإنترنت بين القرصنة والابتزاز الإلكتروني*، دار الفكر الجامعي، 2018.
- خالد ممدوح إبراهيم، *الجرائم المعلوماتية*، دار الفكر الجامعي، 2009.
- خالد ممدوح إبراهيم، *أمن المستندات الإلكترونية*، الإسكندرية، 2008.
- خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني، 2007 .
- دليلة خنيش، الجريمة الإلكترونية والأمن الاجتماعي، ديوان المطبوعات الجامعية، الجزائر، 2023 .
- تاجر كريمة، للقانون والعلوم السياسية، المجلد 19، العدد 02، 2024
- شريفة كلاع، الأمن السيبيراني وأشكال التهديد، تحديات عالمية، ألفا للوثائق، قسنطينة، الجزائر، 2003.
- سيد علي السيد محمد، الجرائم الإلكترونية، ماهيتها وصورها، دار التعليم الجامعي، الاسكندرية، 2023.
- طارق إبراهيم الدوسقي عطية، مرجع سابق، الأمن المعلوماتي نظام قانون الحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2009، 2017.
- طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، ألفا للوثائق، قسنطينة، الجزائؤ
- منال البلقاسي، الغواصات الروبوتيكية القاتلة ذات الطابع السبيراني، مركز المحمود لتوزيع الكتب القانونية، الطبعة الأولى، 2025.
- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة للطباعة والنشر والتوزيع، 2008.
- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنيت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007 .
- عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل للنشر والتوزيع، الطبعة الأولى، الأردن، عمان ،2005.
- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الاولى،
- عبد الصبور عبد القوي على المصري، الجريمة الالكترونية، دار العلوم، القاهرة، 2008.

قائمة المراجع

- غانم مرضى الشمري، الجرائم المعلوماتية (ماهيتها-خصائصها-كيفية التصدي لها قانونيا)، دار الثقافة، عمان، الأردن، 2016.
- غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، دراسة مقارنة، الدار الجزائرية، 2015 .
- فاروق علي الحفناوي، قانون البرمجيات، دراسة معمقة في الأحكام القانونية لبرمجيات الكمبيوتر، دار الكتاب الحديث القاهرة، 2001.
- فراس جمال شاكر، السيبيرانية وتحولات القوة في النظام الدولي، دار أمجد للنشر والتوزيع، الطبعة الأولى، الأردن، 2023.
- لخاز صلاح بوقاني، الحماية الجنائية الموضوعية للمعلوماتية، دراسة مقارنة، الفكر الجامعي، الإسكندرية، الطبعة الأولى.
- محمد عبد الله العواء، جرائم الأموال عبر الإنترنت، جرائم الأموال عبر الانترنت، دار الفتح، الاسكندرية، الطبعة الاولى، 2013 .
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع للإنترنت .
- محمد مصطفى يوسف، مشروعية الدليل في المسائل الجنائية، 2011 .
- منير محمد الجنيهي، ممدوح محمد الجنيهي، جرائم الإنترنيت والحاسب الآلي، دار الفكر الجامعي، مصر، 2005.
- مروة زين العابدين، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، 2012.
- محمد حزيط، الإثبات في المواد الجزائية في القانون الجزائري، دار الجامعة الجديدة، 2019.
- محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الالكتروني، مجلة الحقوق، العدد 02، البحرين، 2012
- محمد أمين الشوابكة، جرائم الحاسوب والانترنت، درا الثقافة للنشر والتوزيع، عمان، 2011.
- محمد حماد مرهج الهيتي، الجريمة المعلماتية، دراسة مقارنة في التشريع الإماراتي السعودي و البحري والقطري والعماني، دار الكتب القانونية_ دار شتات للنشر والبرمجيات مصر.
- محمد حزيط، الوجيز في قانون الاجراءات الجزائية الجزائري، الطبعة الاولى، دار بلقيس، 2025.
- محمد علي محمد التوني، استراتيجية مكافحة الهجمات السيبيرانية، دار الفكر الجامعي، الاسكندرية،2023.

- محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الإنترنت، دراسة مقارنة، مركز المحمود لتوزيع الكتب القانونية، الطبعة الأولى، 2023.
- مصطفى الفؤاد، القرصنة وأمن البحر الأحمر، دار أمجد للنشر والتوزيع، الطبعة الأولى، عمّان، 2020.
- محمد أمين الشهاوي، الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2010.
- هبة مصطفى كافي، التجارة الإلكترونية، ألفا للوثائق، قسنطينة، الجزائر ،2017.
- نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة،2003.
- نسيسة فاطمة الزهراء، الجريمة الإلكترونية وأثرها على الفرد والمجتمع، دراسة سوسيولوجية، الفا للوثائق، الجزائر، 2020.
- علي زياد العلي، *الأمن الجيوسيبراني في السياسة الدولية*، دار أمجد للنشر والتوزيع، الطبعة الأولى، الأردن، 2018.
- عبد الرحمان خلفي، الإجراءات الجزائية في القانون الجزائري والمقارن، دراسة تحليلية تأصيلية مقارنة، الطبعة الثامنة، دار بلقيس، الجزائر، 2025.
- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الالية للمعطيات، دار الخلدونية ،2018.
- يوسف مناصرة، شرعية حجب المواقع الإلكترونية بين التشريع الجزائري والمقارن وأثره على حرية التعبير، دار الخلدونية، 2022.
- يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي، الطريق نحو أدلة الإثبات في المادة الجزائية، دراسة مقارنة، دار الخلدونية، 2021.

سادساً: الرسائل الجامعية

أ _الاطروحات الجامعية:

- بدري فيصل، مكافحة الجريمة المعلوماتية، دكتوراه، جامعة الجزائر 1، 2017 .
- بوربابة صورية، قواعد الأمن المعلوماتي، دكتوراه، جامعة سيدي بلعباس، 2015 .
- مليكة عطوي، حماية الملكية الفكرية على الإنترنت، دكتوراه، جامعة الجزائر 3، 2010 .
- ميرفت محمد حبايبه، مكافحة الجريمة الإلكترونية (مقارنة)، دكتوراه، 2021 .

- سليمان أيمن، عبد الحفيظ عبد الحميد، استراتيجية مكافحة الجرائم الناشئة عن استخدام الإنترنيت، رسالة دكتورا، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، (بدون سنة)، ص 287_289.
- سميرة معاشي، آليات مكافحة الجريمة المعلوماتية–دراسة مقارنة، أطروحة دكتورا علوم في الحقوق تخصص قانون الأعمال جامعة محمد خيضر بسكرة،2019–2020.
- عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، أطروحة دكتوراه، جامعة عين شمس، القاهرة، 2004.
- ميرفت محمد حبايبه، مكافحة الجريمة الالكترونية "دراسة مقارنة" في التشريع الجزائري والفلسطيني، أطروحة لنيل شهادة دكتوراه في الحقوق: تخصص القانون العام، جامعة عمَّار ثليجي–الأغواط، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2021

ب_المذكرات الجامعية:

- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة مقدمة لنيل شهادة الماجستير، في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة لخضر، باتنة، الجزائر. 2012–2013
- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، رسالة قدمت استكمالا للحصول على درجة الماجيستير في القانون العام، جامعة الشرق الأوسط، الأردن 2014.
- فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة ماجيستير، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011–2012.

سابعاً: المقالات والمؤتمرات العلمية

- أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات .
- إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، العدد10، 2017، ص195.
- بالطة مريم اسيا برغيث،" الأمن المعلوماتي في مواجهة القرصنة الإلكترونية "، مجلة دراسات في الحقوق الإنسان، المجلد 6، العدد 1، 2022.
- بن شريف أحلام، القرصنة الإلكترونية، 2012.

قائمة المراجع

- جميل زكريا محمود، الجريمة المعلوماتية وأساليب التأمين، 2005 .
- فتيحة عمارة، جريمة التزوير الإلكتروني، مجلة القانون والمجتمع بتاريخ 28/05/2019، العدد 01 جامعة سعيدة، سنة 2019.
- حمزة خضري، خصوصية أركان الجريمة المعلوماتية، 2020 .
- حزام فتيحة، حماية الأنظمة الرقمية، 2020 .
- سليمان العامري، جريمة الدخول غير المشروع، 2022 .
- رضا همسي، تفتيش المنظومات المعلوماتية، 2012 .
- ربحي امحمد، لعروسي أحمد، قراءة في اتفاقية تريبس، 2022 .
- كهينة آيت حمودة، البحث والتحري الجنائي، 2023 .
- كزيز صباح، سمير قط، أثر الجرائم الالكترونية على أمن واستقرار الدول: قرصنة الموقع الالكتروني لوكالة الأنباء القطرية نموذجا، مجلة الناقد للدراسات السياسية، بسكرة، الجزائر، 2018
- لواعر فاطمة، بوهنتالة إبراهيم، الاعتداء على العلامة التجارية في المجال الإلكتروني، المجلة العربية للعلوم القانونية، العدد 12، 2019.
- لورنس سعيد الحوامدة، الجريمة المعلوماتية أركانها وآلية مكافحتها، الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، السعودية، 2016-2017،
- محمد حمادة الهيتي، البحث عن حماية جنائية للبيانات والمعلومات الشخصية المخزنة في الحاسب الآلي مجلة الشريعة والقانون، جامعة الامارات العربية، العدد27، يوليو، 2006.
- نشناش مينة، الركن المفترض في الجريمة المعلوماتية، مداخلة ألقيت بمناسبة انعقاد الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، بسكرة، 16-17 نوفمبر 2015.
- تاجر كريمة، التسرب الالكتروني كآلية لمكافحة الجريمة الالكترونية (دراسة مقارنة بين القانون الجزائري والفرنسي)، المجلة النقدية للقانون والعلوم السياسية، المجلد 19، العدد 02، 2024.
- عبد الكريم بلعزوق،دراسة في ماهية الاجرام الالكتروني ومجرم الانترنت، مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريرج، الموسوم بعنوان، الاجرام السيبيراني المفاهيم والتحديات، 2017.

ثامناً: المراجع الأجنبية

1. Code pénal français, article 323-1.

2. Le petit la rousse illustré, Dictionnaire de la langue française Paris, 2012, mot « piraterie ».

3. Michel Vivant, Cybercriminalité et droit pénal presse Universitaire de France, paris, 2001.

4. Indira Carr, Computer Crime, 2009.

5. Nathan. Fisk: Digital piracy, New York, NY: Chelsea house, c 2011.

6.Donny B. Parker, Fighting Computer Crime, A New Frame work for Protect in informatique, 1 edition, john Wiley & Sons 1998.

7. Tamrab Orr, Privacy and Hacking, cyber Citizen Stipend Cyber Safety, the Rosen Publishing Group, Inc., 2008.

8. Papa Assante Touré, Cybercriminalité et juge, le traitement de la cybercriminalité, le traitement de la cybercriminalité de vante le juge, Paris, le harmattan, 2014.

9. Abd-el-Kader Fellah, Procedural Developments in Cybercrime, Stages of preliminary Investigation and trial, 2025.

10. Convention de Budapest sur la cybercriminalité, 2001.

Anti-Cybersquatting Consumer Protection Act (ACPA), 1999.

11. Ghernaouti, Solange, *La cybercriminalité*, les nouvelles Armes De pouvoir, 2eme édition, Press Polytechnique et universitaire romandes, 2018.

12. Parker, Combattre la criminalité informatique, édoros 1987.

13. Carr, Indira, *Computer Crime*, International Library of Criminology, Criminal Justice and Penology_ Second Series, Ash gate 2009.

14. Bunn, Edward Devi, Op

15. Angelis, Gina, *Cyber Crimes*, Chelsea house Published, USA, 2000.

16. Vivant, Michel, *Cybercriminalité et droit pénal*, 2001.

17. Fisk, Nathan W., *Digital Piracy*, 2011.

18. Zetter, Kim, *Countdown to Zero Day*, 2014.

19. Anti_cyber squatting Consumer Protection Act (ACPA), 1999.19

20. Nicolas Arpégeant, le cyber sécurité, éditions l'héritier, 2014.

21. R. Gassin la protection pénal d'une nouvelles universalité de rait « en droit français des STAD », commentaire de la loi n 88/19 du 05/01/1988 relative à la fraude informatique, Dalloz, 1988.

22. Jean François castille.

23. Kevin Beaver, Joseph Steinberg, Hacking et Cybersécurité pour les nuls, First Interactive 2024.

24. WIPO Copyright Treaty (WCT).

25. Mutter Maler (C.J.A).Traite de la prévue en matière criminelle. Trad. Alexander. IMP. Librairie général de jurisprudence .Parise.1884

تاسعاً: المواقع الإلكترونية

www.doraraliraq.net

www.legifrance.gouv.fr

Législations belge, loi du 20-11-2000 sur la fraude informatique circonstances, www.ejustice.just.fgov.be

الفهرس

الإهداء:

شكر وعرفان

قائمة المختصرات

..مقدمة 1

أهمية الدراسة.....3

إشكالية الدراسة: 4

صعوبات الدراسة 6

الدراسات السابقة:.....6

تقسيمات الدراسة:.....7

منهج الدراسة:.....8

الباب الأول: الأحكام الموضوعية لجريمة القرصنة الإلكترونية 11

الفصل الأول : الإطار المفاهيمي والقانوني للقرصنة الإلكترونية..... 14

المبحث الأول: مفهوم القرصنة الإلكترونية 15

المطلب الأول: مفهوم القرصنة الإلكترونية 17

الفرع الأول: تاريخ وتطور القرصنة الإلكترونية 17

أولا: مرحلة النشأة من سنة 1971 إلى سنة 1989 17

ثانيا: مرحلة الانتشار 1990 إلى 1994 18

ثالثا: مرحلة الاحتراف ما بعد1994 18

الفرع الثاني: تعريف القرصنة الالكترونية..... 22

أولا: التعريف اللغوي والفقهي للقرصنة الإلكترونية..... 22

ثالثا: التمييز بين القرصنة الإلكترونية والجرائم الإلكترونية الأخرى 36

المطلب الثاني: خصائص جريمة القرصنة الالكترونية وأنواعها ودوافعها 38

الفرع الأول: خصائص القرصنة الإلكترونية 40
أولا: خصائص الجريمة 40
ثانيا: مميزات القرصان الإلكتروني..... 44
ثالثا: أنماط المجرم الإلكتروني 46
الفرع الثاني: أنواع القرصنة الإلكترونية..... 47
أولا: أنواع القراصنة من حيث المدة (الزمن) 47
ثانيا: الأنواع من حيث الغاية..... 48
ثالثا: انواع القراصنة المعلومات من حيث الخطورة 50
الفرع الثالث: دوافع القرصنة الإلكترونية..... 53
أولا: الدوافع الفردية المرتبطة بالفاعل (الهاكر)..... 54
ثانيا: الدوافع ذات الطابع غير الفردي (المؤسساتي أو الجماعي) 55
المبحث الثاني: طرق وأساليب القرصنة الإلكترونية وانعكاساتها..... 56
المطلب الأول: طرق القرصنة الإلكترونية 56
الفرع الأول: الاعتداء على المواقع الإلكترونية والحسابات الشخصية 57
أولا: تقنيات الإعتداء على المواقع الإلكترونية..... 58
ثانيا: تقنيات الاعتداء على الحسابات الشخصية 59
الفرع الثاني: الاعتداء على البرامج والأنظمة المعلوماتية 64
أولا: الاعتداء على سير عمل الأنظمة المعلوماتية 65
ثانيا: الاعتداء على سلامة البرامج والبيانات..... 65
الفرع الثالث: الاعتداء على التجارة الإلكترونية..... 68
أولا:الاستيلاء على أرقام البطاقات الائتمانية..... 69
ثانيا: التعدي على التوقيع الالكتروني 72

ثالثا: قرصنة العلامة التجارية 76
المطلب الثاني: انعكاسات القرصنة الالكترونية 78
الفرع الأول: الانعكاسات الاقتصادية للقرصنة الالكترونية 80
أولا: آثار القرصنة الالكترونية على الاقتصاد الوطني 80
ثانيا: زيادة الاعباء المالية على الدولة 81
الفرع الثاني: الانعكاسات السياسية والقانونية للقرصنة الالكترونية 81
أولا: تأثير القرصنة الالكترونية على سيادة الدول وعلى الامن القومي 81
ثانيا: انعكاسات القرصنة الالكترونية على الملكية الفكرية 82
ثالثا: الاستراتيجية الجزائرية في مواجهة القرصنة الالكترونية في مجال الفكرية الوطنية 85
خاتمة الفصل الأول: 87
الفصل الثاني: الإطار القانوني لجريمة القرصنة الإلكترونية 89
المبحث الأول: الطبيعة والتكييف القانوني لجريمة القرصنة الإلكترونية 90
المطلب الأول: الطبيعة القانونية لجريمة القرصنة الالكترونية 91
اولا: مفهوم نظام المعالجة الالية للمعطيات 93
ثانيا: عناصر نظام المعالجة الآلية للمعطيات: 95
الفرع الثاني: الحماية الفنية لنظام المعالجة الالية للمعطيات 96
ثانيا: الجدل الفقهي حول إشتراط الحماية الفنية 98
ثالثا: مبررات الحماية الجنائية 100
المطلب الثاني: التكييف القانوني لجريمة القرصنة الإلكترونية 100
الفرع الأول: أساس التكييف القانوني لجريمة القرصنة الإلكترونية في التشريع الجزائري 101

الفهرس

أولًا: التكييف القانوني للقرصنة الإلكترونية باعتبارها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات 101

ثانيًا: التكييف القانوني لأفعال القرصنة بحسب محل الاعتداء 102

الفرع الثاني: نطاق التكييف القانوني لجريمة القرصنة الإلكترونية في التشريع الجزائري 103

أولًا: القرصنة الإلكترونية باعتبارها اعتداءً على النظام المعلوماتي 103

ثانيًا: القرصنة الإلكترونية باعتبارها وسيلة للاعتداء على مصالح أخرى 105

ثالثا: التنظيم القانوني لجريمة القرصنة الإلكترونية 106

المبحث الثاني: صور جريمة القرصنة الإلكترونية وأحكامها القانونية 112

المطلب الأول: صورة الدخول والبقاء غير المشروعين 113

الفرع الأول: جريمة الدخول غير المشروع 115

أولا: الركن الشرعي لجريمة الدخول غير المشروع 115

ثانيا: الركن المادي لجريمة الدخول غير المشروع 116

ثانيا الركن المعنوي لجريمة الدخول غير المشروع 125

الفرع الثاني: جريمة البقاء غير المشروع 128

أولا: الركن الشرعي لجريمة البقاء غير المشروع 128

ثالثا: العلاقة بين الدخول والبقاء 130

ثالثا: الركن المعنوي لجريمة البقاء 131

الفرع الثالث: جريمة الاعتداء على النظام المعلوماتي 133

ثانيا: الركن المادي لجريمة الاعتداء على النظام المعلوماتي 133

ثانيا: الركن المعنوي لجريمة الإعتداء على النظام المعلوماتي 135

الفرع الرابع: جريمة المساس العمدي بسلامة المعطيات المعلوماتية 135

أولا: الركن المادي لجريمة المساس العمدي بسلامة المعطيات المعلوماتية 135

ثانيا: الركن المعنوي لجريمة المساس العمدي بسلامة المعطيات المعلوماتية 137
المطلب الثاني: المسؤولية الجزائية في جريمة القرصنة الالكترونية 138
الفرع الأول: المسؤولية الجزائية للشخص الطبيعي عن جرائم القرصنة الإلكترونية ..139
الفرع الثاني: مسؤولية الشخص المعنوي جريمة القرصنة الإلكترونية 140
المطلب الثالث: العقوبات المقررة لجريمة القرصنة الإلكترونية 141
الفرع الأول: العقوبات الأصلية لجريمة القرصنة الإلكترونية 141
أولا: العقوبات المقررة للدخول والبقاء غير المشروعين في النظام المعلوماتي 142
ثانيا: العقوبات المقررة للإعتداء على المعطيات وسير النظام المعلوماتي 142
الفرع الثاني: تشديد العقوبات المقررة لجريمة القرصنة الإلكترونية 143
أولا: جريمة المساس بالمعطيات (حذف أو تغيير معطيات النظام الآلي) 144
ثانيا: جريمة المساس بسلامة النظام (تخريب نظام اشتغال النظام المعلوماتي) 144
ثالثا: جريمة المساس بمؤسسات الدولة 145
الفرع الثالث: عقوبة الاشتراك والشروع في الجريمة 145
أولا: عقوبة الاشتراك 145
ثانيا: عقوبة الشروع 146
الفرع الرابع: العقوبات التكميلية 146
أولا: المصادرة 147
ثانيا: غلق المحل أو مكان الاستغلال 147
الفرع الخامس: العقوبات المقررة للشخص المعنوي 147
أولا: الغرامة المالية 147
ثانيا: العقوبات التكميلية 147
خاتمة الفصل الثاني 149

الباب الثاني: الأحكام الجزائية ومكافحة جريمة القرصنة الإلكترونية في التشريع الجزائري 151

الفصل الأول : خصوصية الإجراءات الجزائية 155

المبحث الأول: خصوصية الإجراءات الجزائية في جرائم القرصنة الإلكترونية 156

المطلب الأول: إجراءات البحث والتحري في الجرائم المعلوماتية 157

الفرع الأول: اختصاص الشرطة القضائية المختصة في الجرائم المعلوماتية 158

أولا: صلاحيات الشرطة القضائية المنصوص عليها في المواد 20 إلى 28 من قانون الإجراءات الجزائية. 159

ثانيا: صلاحيات البحث والتحري في البيئة الرقمية 160

ثالثا: توسيع نطاق تشكيل الشرطة القضائية وضباطها 160

الفرع الثاني: وسائل التحري 160

أولا: تفتيش الأنظمة المعلوماتية وحجز المعطيات 161

ثانيا: حجز البيانات الرقمية والنسخ الإلكتروني للمعطيات 167

ثالثا: المعاينة 168

المطلب الثاني: إجراءات المتابعة الجزائية في جرائم القرصنة الإلكترونية 169

الفرع الأول: خصوصية تحريك الدعوى العمومية في جرائم القرصنة الإلكترونية 171

أولا: خصوصية الدعوى العمومية لجرائم القرصنة الإلكترونية 172

ثانيا: الجهات المختصة بتحريك الدعوى في جرائم القرصنة الالكترونية.....173

ثالثا: الاختصاص الإقليمي لوكيل الجمهورية. 176

الفرع الثالث: امتداد الاختصاص الإقليمي إلى كامل الإقليم الوطني 177

أولا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال 178

ثانيا: النقل الوجوبي للملف من المحكمة المختصة إقليميا للقطب الجزائي.....178

المبحث الثاني: النظام القانوني للإثبات في جرائم القرصنة الالكترونية 179

المطلب الأول: خصوصية الإثبات في جرائم القرصنة الإلكترونية 180
الفرع الأول: مفهوم الإثبات الجزائي 181
أولا: مفهوم الاثبات الجزائي في اللغة 181
ثانيا: مفهوم الاثبات الجزائي اصطلاحا 181
ثالثا: مفهوم الإثبات قانونيا 182
الفرع الثاني: خصائص الإثبات في الجرائم المعلوماتية 182
أولا: الطابع القضائي للإثبات 182
ثانيا: مبدأ تقيد الإثبات بضوابط قانونية 182
ثالثا: حجية الأمر المقضي 183
رابعا: مبدأ حرية الإثبات في المواد الجزائية.....183
الفرع الثالث: الصعوبات التي تواجه جريمة القرصنة الإلكترونية في الإثبات 183
أولا: صعوبات مرتبطة بطبيعة الجريمة نفسها.....183
ثانيا: صعوبات الاثبات تواجه جهات التحقيق الابتدائي.....183
ثالثًا: صعوبات ذات بعد قانوني ودولي 184
رابعا: ضعف الإبلاغ وصعوبة المتابعة 184
المطلب الثاني: خصوصية الدليل الرقمي كوسيلة إثبات 185
الفرع الأول: مفهوم الدليل الرقمي.....185
أولا: الدليل في اللغة 185
ثانيا: التعريف الاصطلاحي للدليل الإلكتروني 186
الفرع الثاني: أنواع الدليل الرقمي.....187
أولا: أدلة أُعدت لتكون وسيلة إثبات (أدلة رقمية مباشرة) 187
ثانيا: أدلة لم تعد لتكون وسيلة إثبات (أدلة رقمية غير مباشرة): 187

الفرع الثالث: خصائص الدليل الرقمي 187
أولا: الدليل الرقمي قابل للتغيير أو الإتلاف 188
ثانيا: الدليل الرقمي دليل عابر للحدود 188
ثالثا: الدليل الرقمي يعتمد على الخبرة التقنية 188
الفرع الرابع: الوسائل التقنية المستحدثة لجمع الدليل الرقمي 189
أولا: التسرب 190
ثانيا: اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور 193
ثالثا: التسجيل الصوتي والمرئي 194
رابعا: المراقبة الإلكترونية.....195
خامسا: الآثار التقنية الناتجة عن الوسائل المستحدثة.....196
المطلب الثالث: سلطة القاضي الجزائي في تقدير الدليل الرقمي واشكالات اثبات الجريمة 197
الفرع الأول: حجية الدليل الرقمي في الإثبات الجنائي 197
أولا: مبدأ مشروعية الدليل الرقمي 198
ثانيا: مبدأ يقينية الدليل الجنائي الرقمي 199
ثالثا: مبدأ وجوب مناقشة الدليل الإلكتروني.....200
الفرع الثاني: سلطة القاضي الجزائي في تقدير الدليل الرقمي 202
أولا: مبدأ الإقتناع الشخصي للقاضي في تقدير الدليل الالكتروني.....202
ثانيا: القيود الواردة على سلطة القاضي الجزائي في تقدير الدليل الإلكتروني 205
ثالثا: الضمانات القانونية المقيدة لسلطة القاضي الجزائي 207
الفرع الثالث: صعوبات الإثبات في جريمة القرصنة الإلكترونية.....207
أولا: الدليل الرقمي دليل غير مرئي 208

ثانيا: الآثار الرقمية المترتبة عن الجريمة الالكترونية 209
ثالثا: استخلاص الأدلة يعد تحديا لرجال الأمن 209
خاتمة الفصل الأول:.....210
الفصل الثاني: الفصل الثاني: التحقيق والمحاكمة في جرائم القرصنة الإلكترونية وآليات مكافحتها 212
المبحث الأول: التحقيق القضائي والمحاكمة في الجرائم المعلوماتية 213
المطلب الأول: اختصاصات قاضي التحقيق في جريمة القرصنة الالكترونية.....213
الفرع الأول: إجراءات التحقيق في جريمة القرصنة الالكترونية.....214
أولا: المعاينة من طرف قاضي التحقيق 214
ثانيا: التفتيش الالكتروني 215
ثالثا: الإنابة القضائية 216
رابعا: الخبرة التقنية 216
الفرع الثاني: قواعد الاختصاص الإقليمي لقاضي التحقيق في جرائم القرصنة الالكترونية 216
أولا: تمديد الاختصاص الإقليمي لقاضي التحقيق في جريمة القرصنة الالكترونية ..217
ثانيا: توسيع صلاحيات أجهزة التحقيق 218
ثالثا: تمديد الاختصاص الٍإقليمي لغرفة الاتهام 219
الفرع الثالث: طرق اتصال قاضي التحقيق بالدعوى 219
أولا: الإحالة عن طريق طلب افتتاحي لإجراء التحقيق 220
ثانيا: الإحالة عن طريق الادعاء المدني 221
ثالثا: الاحالة في حالة التلبس أو الاجراءات الخاصة 221
المطلب الثاني: الاختصاص القضائي والمحاكمة في جرائم القرصنة الإلكترونية....221
الفرع الأول: إشكالات الاختصاص القضائي في جرائم القرصنة الالكترونية.....222

أولا: صعوبات تحديد الاختصاص القضائي في الجرائم الالكترونية 222
ثانيا: قواعد الاختصاص القضائي في الجرائم الالكترونية 224
الفرع الثاني: اختصاص الجهات القضائية الجزائرية في مكافحة جرائم القرصنة الالكترونية 228
أولا: الأقطاب الجزائية المتخصصة في جريمة القرصنة الالكترونية 229
ثانيا: تعريف القطب الجزائي المتخصص 230
الفرع الثالث: إجراءات المحاكمة في جرائم القرصنة الإلكترونية.....234
أولا: خصوصية إجراءات المحاكمة في جرائم القرصنة الإلكترونية 235
ثانيا: تنازع الاختصاص القضائي في الجرائم الالكترونية 236
ثالثا: تحديد القانون الواجب التطبيق 238
المطلب الثالث: ضمانات المحاكمة العادلة في مواجهة الدليل الرقمي 238
الفرع الاول: الإشكاليات التقنية في المحاكمة 239
أولا: دور القاضي في إدارة المحاكمة الرقمية 239
ثانيا: آليات تكريس المحاكمة العادلة في ظل الأدلة الرقمية 240
ثالثا: مبدأ الوجاهية والحضورية 240
رابعا: مبدأ العلانية 240
خامسا: مبدأ الشفاهية 241
سادسا: تدوين التحقيق 241
سابعا: مبدأ عدم مشاركة القاضي في النظر في الدعوى على مستوى الدرجتين ...242
الفرع الثاني: الضمانات الأمنية لتحقيق العدالة الجنائية الرقمية 242
أولا: الحماية المادية، التأمين المادي للأجهزة(Physical Security) 243
ثانيا: الحماية التقنية 243

المبحث الثاني: آليات مكافحة جريمة القرصنة الإلكترونية 246
المطلب الأول: الجهود الدولية والاتفاقيات.....246
الفرع الأول: اتفاقية تربس 247
أولا: مبدأ المعاملة الوطنية.....247
ثانيا: مبدأ الدولة الأولى بالرعاية 248
ثالثا: وضع حد أدنى من الحماية القانونية.....248
رابعا: إنفاذ اتفاقية تريبس 248
خامسا: المعاملة التفضيلية للدول النامية 249
الفرع الثاني: معاهدة بودبست 2001.....249
أولا: أهم ما جاءت به المعاهدة.....250
ثانيا: الاتفاقية الدولية 252
الفرع الثالث: الاتفاقية العربية لمكافحة الجريمة 254
المطلب الثاني: الجهود الوطنية في مكافحة جريمة القرصنة الالكترونية 254
الفرع الأول: الآليات القانونية والقضائية.....255
أولا: الاليات القضائية.....255
ثانيا: الاليات القانونية.....256
الفرع الثاني: الآليات المؤسساتية والهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام والاتصال.....256
أولا: المجلس الوطني لأمن الأنظمة المعلوماتية.....256
ثانيا: وكالة أمن الأنظمة المعلوماتية.....258
ثالثا: الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال 259
الفرع الثالث: الآليات التقنية للحماية لأمن النظم المعلوماتية ضد القرصنة الالكترونية 265

أولا: الجدران النارية آلية تأمين الأنظمة المعلوماتية Firewalls.....265
ثانيا: البصمة الإلكترونية.....266
ثالثا: آليات منع إفشاء المعلومات 267
خاتمة الفصل الثاني: 272
خاتمة: 274
قائمة المصادر والمراجع:.....280
أولاً: المصادر الشرعية.....280
ثانياً: التشريعات الوطنية الجزائرية.....280
ثالثاً: التشريعات المقارنة والاتفاقيات الدولية 281
رابعاً: المعاجم والمراجع العامة 281
خامساً: الكتب والمؤلفات العربية 281
سادساً: الرسائل الجامعية.....285
سابعاً: المقالات والمؤتمرات العلمية.....286
تاسعاً: المواقع الإلكترونية 290
الفهرس: 291
الملخص:.....295

الملخص

تناولت هاته الدراسة نوع خاص من الجرائم الإلكترونية المتمثلة في القرصنة الإلكترونية المسؤولية الناشئة عنها في ظل التشريع الجزائري، باعتبارها ظاهرة حديثة أين تناولت فصول هاته الأطروحة ماهيتها وخصائصها وتمييزها عن باقي الجرائم الالكترونية ليتم الطرق في الفصل الثاني للقرصنة الإلكترونية في ظل التشريع الجزائري.

على الرغم من الفوائد الكبيرة للتطور التقني إلا أن على هاته الدراسة تمثل تحديا خطيرا للدول والمجتمعات لما تسببه من تهديدات أمنية واقتصادية واجتماعية، فقد أتاح التقدم الرقمي للمجرمين فرصا جديدة لارتكاب أفعال مخالفة للقانون بطرق يصعب تعقبها نتيجة الاستخدام غير المشروع لشبكات المعلومات والتقنيات الحديثة لتصبح جريمة القرصنة الإلكترونية تشكل خطرًا متزايدًا على الأفراد والمؤسسات والدول، الأمر الذي جعل من الضروري إيجاد أطر قانونية وتشريعية فعالة للحد من هذه الظاهرة المتنامية.

وفي هذا الإطار، سعت العديد من الدول إلى سن تشريعات وطنية وتنظيمات خاصة لمكافحة الجرائم الإلكترونية، كما بادرت المنظمات الدولية إلى وضع اتفاقيات ومعايير قانونية موحدة تسهم في تعزيز التعاون الدولي لمواجهة الجرائم السيبرانية العابرة للحدود.

ومن أبرز الجهود في هذا المجال نجد المعاهدات والاتفاقيات الدولية منها: معاهدة بودابست وكذلك الجهود العربية المتمثلة في المشروع العربي الموحد للقانون رقم (9-4)، الذي تضمن القواعد المتعلقة بمكافحة الجرائم المتصلة بتقنيات الإعلام والاتصال. وقد أقره مجلس وزراء العدل العرب عام 2009 بهدف توحيد السياسات العربية وتعزيز التعاون الإقليمي في مواجهة الجريمة الإلكترونية.أما على المستوى الوطني وعلى الرغم من صعوبة حصر أهم صور الجريمة المعلوماتية، إلا أن المشرع الجزائري قد وضع تصورا يشمل أهم مظاهر السلوك الذي يشكل اعتداء على أنظمة المعالجة الآلية للمعطيات.

وتشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري جريمتي الدخول والبقاء غير المشروع للنظام المعلوماتي، وجريمة إتلاف النظام الآلي بوسائل وتقنيات محددة وهذا عن طريق فيروس الحاسب الآلي من قبل الهاكرز، وعلى هذا النحو يكون المشرع الجزائري قد ساير مختلف التشريعات المقارنة في مجال استحداث نصوص قانونية لمواجهة هذا النوع من الجرائم ضمن إطار قانون العقوبات على رأسها القانون رقم 09-04

الكلمات المفتاحية:

الجرائم الالكترونية، القرصنة الالكترونية، القانون09-04، جريمتي الدخول والبقاء الغير مشروع، الحاسب الآلي، الهاكرز.

الملخص

Abstract

This study examines a specific type of cybercrime, namely electronic piracy (Hacking), and the resulting legal liability under Algerian legislation. Given its nature as a contemporary phenomenon, the chapters of this thesis explore the essence, characteristics, and distinctions of electronic piracy from other cybercrimes. The second chapter specifically addresses electronic piracy within the framework of Algerian law.

Despite the significant benefits of technical advancement, this study highlights a serious challenge to states and societies due to the security, economic, and social threats it poses. Digital progress has provided criminals with new opportunities to commit illegal acts in ways that are difficult to track, resulting from the illicit use of information networks and modern technologies. Consequently, electronic piracy has become an escalating danger to individuals, institutions, and states alike, necessitating the establishment of effective legal and legislative frameworks to curb this growing phenomenon.

In this context, many countries have sought to enact national legislation and specific regulations to combat cybercrime. Furthermore, international organizations have initiated unified legal agreements and standards to enhance international cooperation in facing Tran's boundary cybercrimes. Among the most prominent efforts in this field are international treaties, such as the Budapest Convention, as well as Arab efforts represented by the Unified Arab Draft Law No. (09-04). This draft includes rules related to combating crimes connected to information and communication technologies, approved by the Council of Arab Ministers of Justice in 2009 to unify Arab policies and strengthen regional cooperation.

At the national level, and despite the difficulty of categorizing all forms of cybercrime, the Algerian legislator has developed a framework covering the most significant behaviors that constitute an assault on automated data processing systems. Under Algerian legislation, crimes affecting automated data processing systems include the illegal access and remaining within an information system, as well as the destruction of automated systems through specific means and techniques, such as computer viruses deployed by hackers. Accordingly, the Algerian legislator has kept pace with various comparative legislations by introducing legal texts to confront this type of crime within the Penal Code, most notably Law No. 09-04.

Keywords:

Cybercrimes, Electronic Piracy (Hacking), Law 09-04, Illegal Access and Remaining, Computer, Hackers.

تم بحول الله وعونه