وزارة التعليـم العالــي والبحـث العلمي

المركز الجامعي عبد الحفيظ بوالصوف –ميلة

معهد الحقوق

الشعبة : حقوق

القسم: القانون العام

التخصص: قانون جنائي

الرقم التسلسلي:.....

الرمـــــــــز : .....

مكافحة جريمة القرصنة الإلكترونية في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة ماستر في الحقوق

تخصص قانون جنائي

إعداد الطالبتين:

- **بوسنة شميسة**
- **جمعة إكرام**

إشراف الأستاذ:

د/ حمدوني علي

السنة الجامعية: 2025/2024

وزارة التعليـم العالــي والبحـث العلمي

المركز الجامعي عبد الحفيظ بوالصوف –ميلة

معهد الحقوق

الشعبة: حقوق الرقم التسلسلي:.....

القسم: القانون العام الرمـــــــــز: .....

التخصص: قانون جنائي

مكافحة جريمة القرصنة الإلكترونية في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة ماستر في الحقوق

تخصص قانون جنائي

إعداد الطالبتين:

- **بوسنة شميسة**
- **جمعة إكرام**

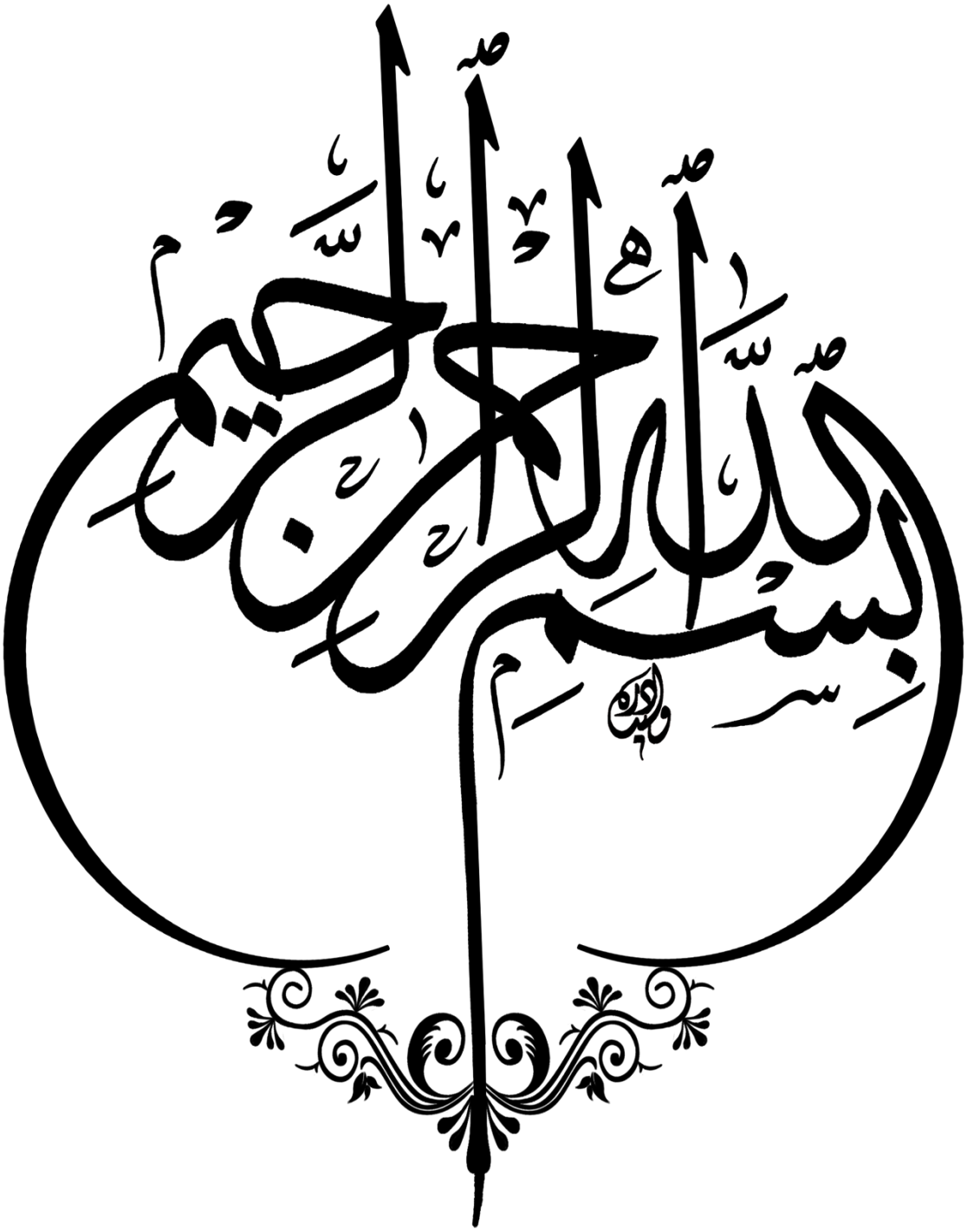
إشراف الأستاذ:

د/ حمدوني علي

أعضاء لجنة المناقشة

د/ بن تومي صحر	**المركز الجامعي ميلة**	**أستاذ محاضر ب**	**رئيسا**
د/ حمدوني علي	**المركز الجامعي ميلة**	**أستاذ محاضر ب**	**مشرفا ومقررا**
أ/ شباح بوزيد	**المركز الجامعي ميلة**	**أستاذ مساعد أ**	**عضوا مناقشا**

السنة الجامعية : 2025/2024


بسم الله الرحمن الرحيم

{اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ ❷ خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ ❸ اقْرَأْ وَرَبُّكَ الْأَكْرَمُ ❹ الَّذِي عَلَّمَ بِالْقَلَمِ ❺ عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ {❻

[سورة العلق: 1- 5]

شكروتقدير

"شكري اولاً إلى الله عزوجل، الذي هدانا ووفقنا لتحقيق طموحنا"

ثم شكروعرفان لأستاذي الفاضل: حمدوني علي

بكل فخروامتنان، نتقدم إليك بجزيل الشكروالتقديرعلى ما بذلته من جهد في تعليمنا وتوجيهنا، وعلى دعمك المتواصل وتشجيعك المستمر الذي كان له بالغ الأثر في مسيرتنا.

لقد كنت دائمًا مثالًا يحتذي به في الإخلاص والعطاء، ولم تبخل يومًا علينا.

لك منا كل الاحترام والعرفان، وأسأل الله أن يجعل ما قدمته في ميزان حسناتك، وأن يوفقك الله في مسيرتك العلمية والعملية.

إهـداء

الحمد لله حبا وشكرا وامتنانا على البدء والختام

"وآخر دعواكم ان الحمد لله رب العالمين"

..الى من زين اسمي بأجمل الألقاب، من دعمني بلا حدود وأعطاني بلا مقابل الى من غرس في روحي مكارم الأخلاق داعمي الأول في مسيرتي وقوتي وسندي بعد الله، اليك يا من سقى دربي دعاء، وزرع في طريقي نورا، يا من كلل العرق جبينه كي لا أشعر بالتعب، أبي الغالي

الى سيدة الحنان ورفيقة الدرب وصاحبة القلب الأعظم، اليك يا من كنت دائما النور الذي ينير لي الطريق، كل يوم كنت تضحين من أجلي تزرعين في القوة وتزرعين في روحي الأمل، أنت النعمة التي لا يمكنني أن أعيش بدونها، أمي الغالية

الى اخوتي وأخواتي شكرا لكم على دعمكم لي طيلة مسيرتي الدراسية أدامكم الله لي

شميسة

إهـداء

الحمد لله حبا وشكرا وامتنانا على البدء والختام

"وآخر دعواكم ان الحمد لله رب العالمين"

..الى من رحل عن دنيا الفناء، وترك في القلب اثرا لا يمحى، الى من غرست في القيم، وربيتني على حب العلم والعمل، اتمنى ان تصلك مشاعري وتفتخر بمن حملوا اسمك واثبتوا أنك خير مربي وخير معلم وخير أب ابي الغالي رحمك الله بواسع حمته، وغفر لك بقدر ما أحببت لنا من خير.

..إلى من سقت أحلامي بدعائها، وسهرت الليالي لأجل أن أستيقظ على نور النجاح..إليكِ يا أمي أزف فرحة تخرجي، فكل خطوة في هذا الطريق كانت بفضل الله ثم بدفء يديكِ، كنتِ السند حين تعبت، والدافع حين ضعفت، والدعاء الذي لا يخيب حين ضاقت السبل، "رضاكِ جنتي، وابتسامتكِ أجمل من كل شهاداتي".

الى أخي العزيز وأخواتي الغاليات، كل التقدير والامتنان لوقوفكم بجانبي ودعمكم الدائم، فبكم أفتخر وبكم تكتمل سعادتي.

إكرام

قائمة المختصرات

ص: صفحة

ص. ص: من الصفحة الى الصفحة

ج. ر: الجريدة الرسمية

ق ع ج: قانون العقوبات الجزائري

ق ا ج: قانون الإجراءات الجزائية

ط: طبعة

د ط: دون طبعة

مقدمـة

مقدمة

شهد العالم اليوم تطورًا هائلًا في مجال تكنولوجيا الإعلام والاتصال، خاصة مع الانتشار الواسع للإنترنت، مما أدى إلى ظهور انتهاكات إلكترونية ناجمة عن سوء استخدام هذه التقنيات الحديثة، وقد ترتب على ذلك بروز نوع جديد من الجرائم يُعرف بالجرائم المعلوماتية، نظراً لارتباطه بالوسط الرقمي الذي ينشأ فيه، وهو ما يميّزه عن الجرائم التقليدية.

وتعد الجريمة الإلكترونية من التحديات المستجدة التي فرضتها الثورة التكنولوجية والمعلوماتية، نتيجة لما تشهده من تغير دائم ومستمر في أنماطها وأساليبها. وقد رافق هذا التغير بروز مخاطر وتهديدات جسيمة تمس الأفراد، وتمتد آثارها إلى المؤسسات، بل وحتى إلى استقرار الدول وأمن شعوبها، ومع تفاقم هذه الظاهرة عبر مختلف أنحاء العالم، أصبحت الجزائر –كغيرها من الدول – عرضة لها، حيث لم تسلم منها الأفراد ولا الهيئات المتنوعة، مما أثر على الأمن والاستقرار بمختلف أبعاده: السياسي، الاقتصادي، والثقافي اذ ان أشكال الاعتداءات التي تمس الانظمة المعلوماتية وهي ما تعرف بالقرصنة الإلكترونية وهي من أخطر الجرائم المعلوماتية، لما تنطوي عليه من تهديد مباشر لأمن المعلومات، وسرية البيانات، واستقرار البنية التحتية الرقمية للدول والمؤسسات والأفراد، وهي كل فعل عمدي يُرتكب باستخدام الوسائل الإلكترونية أو الأنظمة المعلوماتية بهدف اختراق الأنظمة والشبكات أو التلاعب بالمعلومات أو الوصول غير المشروع إلى البيانات أو تعطيلها أو تدميرها، وهي متعدية الحدود وصعبة الاكتشاف والاثبات وغالباً ما تكون مدفوعة بأغراض إجرامية، سياسية، اقتصادية أو حتى لمجرد التسلية والانتقام.

وقد أولى المشرع الوطني أهمية كبيرة لهذه الجريمة، فأدرجها ضمن الأفعال المجرّمة في القوانين المتعلقة بمكافحة الجرائم المعلوماتية، وحرص على تقديم تعريفات دقيقة، وتقسيمات واضحة لأنواعها، مع توفير آليات قانونية وفنية للتحقيق والمكافحة. ويُعد التصدي لجريمة القرصنة الإلكترونية من خلال الوسائل التقنية الحديثة أحد التحديات المعاصرة التي تواجه أجهزة إنفاذ القانون، وخاصة في ظل الانتشار الواسع لتكنولوجيا المعلومات والاتصالات، إذ يصعب في كثير من الأحيان تتبع مرتكبي هذه الجرائم وتحديد هويتهم، مما يستدعي استخدام وسائل وآليات جديدة كاعتراض المراسلات والتسرب والتي تتناسب مع طبيعة هذه الجرائم.

أمام هذا التهديد المتزايد للأمن المعلوماتي، كان لا بد من تدخل المشرع لوضع أطر قانونية مناسبة تحد من هذه الظاهرة، وذلك من خلال سن قوانين موضوعية على المستويين الدولي والوطني، تجرّم هذا النوع من الأفعال وتعاقب مرتكبيها. كما تم إنشاء مراكز ووحدات متخصصة تعمل ميدانيًا على مكافحة

الجرائم الإلكترونية والحد من انتشارها، بالإضافة إلى تحديث التشريعات لتشمل الأفعال المستجدة كما أن التعاون الدولي بين الجهات المعنية وتبادل المعلومات بين الدول يُعد أمرًا ضروريًا للحد من انتشار هذه الجرائم، لا سيما أن الجريمة الإلكترونية لا تعترف بالحدود الجغرافية، مما يزيد من أهمية التنسيق الدولي في مكافحتها.

جريمة القرصنة الإلكترونية تندرج ضمن الجرائم المعلوماتية وتنطبق عليها نفس الأحكام العامة للجريمة المعلوماتية وهنا يطرح التساؤل، ما مدى فعالية النصوص التشريعية التي اقرها المشرع الجزائري لمكافحة جريمة القرصنة الإلكترونية؟

وتندرج على هذه الإشكالية تساؤلات فرعية وهي كالتالي:

-ما هي جريمة القرصنة الإلكترونية؟

-وفيما تتمثل صور هذه الجريمة؟

-ما هي إجراءات التحقيق فيها؟

-وما هي أهم العقوبات التي جاء بها المشرع الجزائري؟

-وفيما تتمثل الجهود الأمنية لمحاربة هذه الجريمة؟

ان اختيارنا لدراسة هذا الموضوع هو التطور الهائل والتقدم في الأنظمة المعلوماتية الذي ساهم بشكل مباشر في تطور الجرائم المعلوماتية بصفة عامة وجريمة القرصنة الالكترونية التي تعتبر احدى صور تلك الجرائم، وكذلك ندرة الدراسات التي تناولت جريمة القرصنة الإلكترونية، ولقد جاء اختيارنا لموضوع القرصنة الالكترونية انطلاقا من اهتمامنا الشخصي بالجريمة الالكترونية ورغبتنا في التعمق في فهم التحديات التي تواجه الأفراد والمجتمعات في الفضاء الرقمي.

ان الهدف من دراستنا هو تسليط الضوء على جريمة القرصنة الإلكترونية، اذ ان اغلب الدراسات تطرقت الى الجرائم الإلكترونية بصفة عامة، كما ان هذا البحث يهدف الى التعرف على

اهم الآليات الوطنية والدولية لمكافحتها باعتبارها انها من الموضوعات الحديثة التي فرضت نفسها بقوة على المستويين الوطني والدولي، والتي تطرح على المشرع الجنائي ضرورة مواجهتها بإجراءات قانونية حاسمة ورادعة لمكافحتها وعقاب مرتكبيها.

اعتمدنا في دراستنا على المنهج التاريخي من خلال نشأة القرصنة الالكترونية ومراحل تطورها، إضافة الى ذلك المنهج الوصفي من خلال وصفنا لهذه الجريمة المستحدثة وتبيان خصائصها وصورها التي تختلف

عن الجريمة التقليدية، ومنهج تحليل المضمون من خلال تحليل النصوص القانونية التي جاء بها المشرع الجزائري.

ومن بين الدراسات السابقة لموضوع القرصنة الإلكترونية قمنا بالاستعانة بأطروحات دكتوراه الى جانب رسائل الماجستير من بينهم:

أطروحة دكتوراه تحت عنوان الإطار القانوني والمؤسساتي لمكافحة التقليد والقرصنة الالكترونية من اعداد الطالب عمر يوسف عبد الله واستعنا في موضوعه ببعض المفاهيم التي تخص القرصنة الالكترونية أساليب مكافحة هذه الجريمة، وكذلك أطروحة الدكتوراه تحت عنوان الأسرار المعلوماتية وحمايتها الجزائية من اعداد الطالبة رابحي عزيزة حيث تطرقت الى صور الاعتداء على اسرار المعلومات والمعطيات في العصر الحالي وعرفت كل صورة على حدى ومن بين هذه الجرائم جريمة الدخول والبقاء غير المصرح بهما، وأيضا رسالة الماجستير تحت عنوان جرائم المساس بأنظمة المعالجة الالية للمعطيات من اعداد الطالبة جدي نسيمة استعنا بها في إجراءات مكافحة هذه الجريمة.

من بين الصعوبات التي واجهتنا في دراستنا لموضوع مكافحة جريمة القرصنة الالكترونية هي موضوع البحث وذلك لان اغلب الدراسات تناولت دراسة الجرائم المعلوماتية بصفة عامة ولم تسلط الضوء على دراسة جريمة القرصنة بشكل خاص، كذلك من بين الصعوبات قلة المراجع المتخصصة التي تفيد بحثنا.
وقد قمنا بتقسيم موضوع دراستنا الى فصلين حيث تناولنا في الفصل الأول ماهية جريمة القرصنة وذلك بإبراز مفهوم جريمة القرصنة ومختلف الدوافع والأساليب التي تدخل في ارتكابها إضافة الى صورها اما الفصل الثاني قد خصصناه لمكافحة جريمة القرصنة الإلكترونية الذي يتمحور في مختلف أساليب ووسائل التحقيق بالإضافة الى العقوبات التي اقرها المشرع الجزائري والى مختلف الجهود منها الوطنية والتشريعية، وختمنا بحدثنا الى اهم النتائج التي توصلنا لها من خلال دراساتنا لهذا الموضوع وقمنا بتقديم توصيات تعالج هذه الجريمة.

الفصل الاول:

الإطار المفاهيمي لجريمة القرصنة الإلكترونية

الفصل الأول: الإطار المفاهيمي لجريمة القرصنة الإلكترونية

تعتبر الجرائم المعلوماتية من الظواهر الحديثة، وذلك لارتباطها بالتكنولوجيا الحديثة والمتطورة والحاسب الآلي، وهي تقسم إلى عدة جرائم، من بين هذه الجرائم "جريمة القرصنة الالكترونية".

عندما يتبادر على أسماعنا كلمة قرصنة، فإننا نتخيل عصابات سرقة السفن البحرية والسطو عليها، ونهب ما فيها واسر طاقمها، وهو ذاته ما يفعله قرصان الأنظمة الإلكترونية بالضبط، لكن بوسائل حديثة، ودون أن يعرض نفسه للخطر.

إن موضوع القرصنة يعتبر بحد ذاته موضوع الساعة، وهو مرتبط بمعطيات التقييم العلمي في مجال تكنولوجيا الاتصالات والمعلومات، وظهور الحاسب الآلي وتقنياته وأهم أطواره –شبكة الانترنت– مما تترتب عنه انتقال حر داخل الشبكة العنكبوتية، وما ينجر عن ذلك الإبحار والانتقال الحر من إمكانات العدوان على المنظومة المعلوماتية والاستيلاء على البيانات بطريقة غير مشروعة، قد يترتب عليها كذلك الاعتداء على القيم الاقتصادية، بل الثقافية والاجتماعية جديرة بالحماية الجنائية. وسنحاول التطرق في هذا الفصل إلى مفهوم الجريمة الالكترونية والأسباب التي ادت إلى ارتكابها هذا فيما يخص **(المبحث الأول)**، وصور القرصنة الالكترونية واركانها في القانون الجزائري من خلال **(المبحث الثاني)**.

المبحث الأول: ماهية جريمة القرصنة الالكترونية.

أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية لجريمة القرصنة الإلكترونية، ويرجع السبب في ذلك إلى تعدد وجهات النظر بخصوص مفهوم هذا النوع المستجد من الجرائم، حيث ظهرت عدة اتجاهات فقهية في محاولة فهم المقصود بالجريمة القرصنة وتحديد تعريف لها مع تبيين طبيعتها القانونية، وعليه سنحاول من خلال هذا المبحث أن نتطرق إلى مختلف التعريفات الفقهية والقانونية لجريمة القرصنة الالكترونية وكذا النشأة والتطور، ودوافع هذه الجريمة وخصائصها.

وتم تقسيم هذا المبحث الى **(المطلب الأول)** مفهوم جريمة القرصنة وخصائصها، و**(المطلب الثاني)** دوافع جريمة القرصنة واساليبها.

المطلب الأول: مفهوم جريمة القرصنة الالكترونية وخصائصها

ان عملية القرصنة الإلكترونية عرفت كظاهرة عالمية غير مشروعة تتضمن في معظم الأحيان أكثر أشكال الجريمة المنظمة تقدما. وقد نمت جرائم القرصنة الإلكترونية–باعتبارها من الجرائم الإلكترونية–في العقد الماضي بشكل لم يسبق له مثيل على شبكة الانترنت ووسائل التواصل الاجتماعي. سنتطرق الى نشأة وتطور القرصنة الالكترونية، ومختلف تعريفاتها.

وقسمنا هذا المطلب الى فرعين، نشأة وتطور القرصنة الالكترونية في **(الفرع الأول)**، وتعريف القرصنة الالكترونية في **(الفرع الثاني)** وخصائص جريمة القرصنة الالكترونية في **(الفرع الثالث)**.

الفرع الأول: نشأة وتطور القرصنة الالكترونية

ارتبط ظهور القرصنة واختراق رموز أنظمة الحاسوب مع ظهور أول الحواسيب الالكترونية إلا أن تاريخ القرصنة واختراق أنظمة اختراق الحاسوب يشمل الهجوم السيئ الذكر على شبكات الحاسوب من قبل مخترقي نظم الحاسوب ومنتهكي القوانين، كما يبين التقدم في مجال سرية المعلومات التي تغطي الانترنت بالإضافة إلى تكنولوجيات أخرى كالاتصالات[1].

القرصنة أو المعلوماتية في عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الانترنت غالبا لأن اغلب حواسب العالم مرتبطة عبر هذه الشبكة[2] حيث مرت جريمة القرصنة في تطورها بعدة مراحل، كما يرتبط تاريخ قرصنة الحاسوب مع الأحداث التي غيرت النظرة إلى سرية المعلومات كما نراها اليوم.

ولقد بدأت ظاهرة القرصنة والاختراق مع بداية ظهور الحاسبة الالكترونية وازدادت بشكل كبير مع استخدام تقنية الشبكات، حيث يشمل الاختراق هجوم على شبكات الحاسوب من قبل مخترقي الأنظمة والمواقع الالكترونية ومنتهكي القوانين، غير ان القرصنة لا تمس الشبكة العنكبوتية فقط، بل تمتد الى تقنيات أخرى كالاتصالات والبرمجيات، ذلك ان عمليات القرصنة تطورت بسرعة فائقة، وأصبح من الشائع جدا العثور على مواقع بالأنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي[3].

ويمكن تقسيم نشأة القرصنة الالكترونية إلى ثلاث مراحل أساسية:

---

[1] بشرى حسين الحداني، **القرصنة الالكترونية أسلحة الحرب الحديثة، الطبعة الأولى**، دار أسامة للنشر والتوزيع، الأردن–عمان، 2014، ص 20، 21.

[2] عمر يوسف عبد الله، **الإطار القانوني والمؤسساتي لمكافحة التقليد والقرصنة الالكترونية**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة وهران2، 2021–2022، ص 190.

[3] دحو نجاة واولاد علي فاطمة، **جريمة القرصنة الإلكترونية في التشريع الجزائري**، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2021–2022، ص 08 ،09.

أولا: المرحلة الأولى ما قبل 1979

في هذه السنوات لم تكن للكمبيوتر وجود ولكن كانت هناك شركات الهواتف التي كانت المكان الأول لظهور ما نطلق عليهم في الوقت الحاضر "القراصنة" ، لكن نلقي الضوء على ما كان يحدث في الولايات المتحدة الأمريكية، وفي إحدى شركات الهواتف المحلية كان اغلب العاملين في تلك الفترة من الشباب المتحمسين لمعرفة المزيد عن هذه التقنية الجديدة، والتي حولت مجرى التاريخ فكان هؤلاء الشباب يسعون إلى المكالمات التي تتم في هذه المؤسسة وكانوا يقومون بتغيير الخطوط الهاتفية، ولهذا قامت الشركة بتغيير الكوادر العاملة بها إلى كوادر نسائية، في الستينات من هذا القرن ظهر الكمبيوتر الأول ولكن هؤلاء القراصنة كانوا لا يستطيعون الوصول لهذه الأجهزة، ولذلك لأسباب كثيرة منها كبر حجم هذه الأجهزة ووجود حراسة مشددة عليها لأنها كانت تابعة لوزارة الدفاع الأمريكية.

ثانيا: المرحلة الثانية 1980 – 1989 العصر الذهبي للهاكرز

في عام 1981 أنتجت شركة (IBM) جهاز أسمته بالكومبيوتر الشخص الذي يتميز بصغر حجمه ووزنه الخفيف مقارنة مع الكومبيوترات القديمة الضخمة و أيضا سهولة استخدامه و نقله إلى أي مكان و إمكانية وصله بالأنترنت، عندما بدأ الهاكر عملهم الحقيقي بتعلم كيفية عمل هذه الأجهزة، و كيفية برمجة أنظمة التشغيل فيها و كيفية تخزينها، و في هذه الفترة ظهرت مجموعات من الهاكرز كانت تقوم بمعطيات التخريب في أجهزة المؤسسات و اختراق الشبكات و الأنظمة و كذلك الحصول على الأسرار الصاغية في المجالات الرئيسية و خصوصا في صناعته الكومبيوتر نفسها، و تطوير فيروسات يمكنها أن تلحق اكبر قدر من الأضرار في البرنامج و المعدات المعلوماتية.

ثالثا: المرحلة الثالثة ما بعد 1990 حرب الهاكرز العظمى

البدايات الأولى لحرب الهاكرز العظمى التي دارت رحالها بين عامي 1990 إلى 1994 بين فريقين الهاكرز المحترفين MOD وLOD حيث يقومون بالقرصنة على أجهزة الآخرين وكانا يعتبرون من أذكى الهاكرز في تلك الفترة وكان هدفهم الولوج إلى أجهزة الحاسوب الآلي والعبث فيها.

ومهما يكن من امر فإن القرصنة الالكترونية او الكمبيوترية التي يطلق عليها اسم التسلل خطيرة جدا ومركبة في أحيان كثيرة وقد تستفيد من الجهد والمال الشيء الكثير دون أن تصل أحيانا إلى القضاء على " القرصان " ولا تنحصر خطورتها في دولة معينة بمفردها بل ستطال دون غيرها كما شعوبا أخرى أيضا[1].

[1] عمر يوسف عبد الله، مرجع سابق، ص 193، 194.

الفرع الثاني: تعريف القرصنة الالكترونية

الجرائم الالكترونية استخدمت من أجلها عدة مصطلحات للدلالة عليها وتحديد مفهومها، فهناك من يطلق عليها جرائم الحاسب الآلي وإساءة استخدام الحاسب الآلي، وهناك من يطلق عليها مصطلح جرائم الكمبيوتر أو الجرائم الإلكترونية، وهناك من يسميها بالجرائم المعلوماتية، لهذا قال البعض أنها جريمة مستعصية على التعريف ويستدلون في ذلك بالمحاولات العديدة التي بدلت لتعريفها[1] ومن بين الجرائم الالكترونية جريمة القرصنة وهي محل دراستنا.

اولا: تعريف جريمة القرصنة

ان القرصنة الالكترونية أو التخريب الإلكتروني تقع في المستوى الأول من النزاع في الانترنت وتتضمن هذه العمليات القيام بتعديل أو تخريب أو إلغاء المحتوى[2]، وسنتطرق الى تعريفها من الناحية اللغوية، والفقهية ثم القانونية.

1-التعريف اللغوي

"القرصنة: هي السطو على السفن في البحار" [3]

و "القرصنة" مصدر الفعل " قرصن"، فيقال:" نشطت القرصنة على الشواطئ قديم"، ومن يمتهنها يسمى قرصان، وهذا المصطلح مشتق من كلمة "pirate" اللاتينية.

والقرصان هو لص البحر، ويعتبره البعض لفظة مفردة، ويجمعونه على قراصنة، ولفظ "قرصان" غير عربية فهي مأخوذة من اللغة الإيطالية "CURSARA" بمعنى لص البحر وهي مأخوذة بدورها من اللاتينية "CURSARIUS" المشتقة من الفعل جرى، لأنهم كانوا يهربون بعد نهب السفينة[4].

2-التعريف الفقهي

ظهرت عدة تعاريف فقهية تناولت هذه الجريمة المستحدثة، قد طار خلاف فيما بين هذه التعريفات والأمر راجع لحداثة هذا النوع من الاجرام، ضف الى ذلك الاختلاف الذي طال تسمية هذه الجريمة، فهناك من يسميها بجريمة القرصنة الالكترونية وهناك من ينعتها بالجريمة الرقمية.

---

[1] رابحي عزيزة، **الأسرار المعلوماتية وحمايتها الجزائية**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بالقايد، تلمسان، 2017-2018، ص 89.

[2] فيصل محمد عبد الغفار، **الحرب الإلكترونية**، الجندارية للنشر والتوزيع، الاردن-عمان، 2015، ص 10.

[3] عبد الهادي ثابت، **اللسان العربي الصغير قاموس عربي**، دار الهداية، الجزائر، 2001، ص349.

[4] عجري زهرة، **القرصنة في العهد العثماني في البحر الأبيض المتوسط في القرن 16م**، مجلة عصور جديدة، جامعة وهران احمد بن بلة، المجلد14، العدد2، اكتوبر 2024، ص 171.

الاتجاه الأول: جانب من الفقه عرفها على أنها عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الانترنت.

الاتجاه الثاني: عرفها هذا الاتجاه بأنها ليست سوى عملية دخول غير مصرح به الى أجهزة الغير وشبكاتهم الإلكترونية[1].

وقد عرفها الفقيه الألماني " تديمان" بأنها: شكل من أشكال السلوك الإجرامي الغير المشروع أو الضار بالمجتمع باستخدام الحاسب الآلي كما عرفها لأنها كل نشاط إجرامي يوحد قيمه نظام الحاسب الآلي، دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية وفي ذلك الاتجاه عرفها بأنها الجرائم التي يكون فيها دور الحاسب ايجابيا أكثر من سلبيا[2] .

3-التعريف القانوني لجريمة القرصنة الالكترونية

سنعرفه من ناحية اتفاقية بودابست ثم التعريف القانوني الذي جاء به المشرع الجزائري.

1.3تعريف اتفاقية بودابست

عرفتها اتفاقية بودابست في المادة 4 منها تحت مصطلح التدخل في البيانات حيث جاء في نصها:" تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير حق: إتلاف، محو، أو إفساد، أو تعديل، أو تدمير بيانات موجودة على كومبيوتر".

ان جريمة القرصنة الالكترونية تشمل جرائم الإدخال، الإتلاف المحو، الطمس لبيانات أو برامج الحاسب الآلي، الإضرار ببيانات وبرامج الحاسبات ويشمل المحو والإتلاف ، التعطيل أو الطمس غير المشروع لبيانات وبرامج المعلومات، تخريب الحاسبات ويحتوي على: الإدخال، الإتلاف، المحو، الدخول غير المصرح به: الدخول غير المشروع لنظام معلوماتي أو مجموعة نظم، الاعتراض غير المصرح به وهو: الذي يتم بدون وجه حق عن طريق استخدام وسائل فنية للاتصال، وفي تعريف آخر تعرف بأنها: " الدخول أو إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات والمعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام ألمعلوماتي"[3].

2.3التعريف القانوني للمشرع الجزائري

تعتبر جريمة القرصنة الالكترونية في القانون الجزائري الجرعة التقليدية بحسب خطورتها إلى جناية وهي أخطر الجرائم وجنحة وهي متوسطة الخطورة ثم مخالفة وهي اقل خطورة وتصنف بحسب طبيعتها إلى

---

[1] مزوري اكرام، **القرصنة الرقمية كعائق تقني لنظام التقاضي**، مجلة البصائر للدراسات القانونية والاقتصادية، المركز الجامعي مغنية، الجزائر، العدد الخاص، 2021، ص 312.

[2] عمر يوسف عبد الله، مرجع سابق، ص 186.

[3] دحو نجاة، مرجع سابق، ص 9، 10.

جريمة عادية وجريمة سياسية، عسكرية وأخرى إرهابية، و قد تدارك المشرع الجزائري الفراغ الذي كان موجودا بخصوص تجريم بعض الاعتداءات على النظم المعلوماتية حيث اصدر القانون رقم 24-06 [1] المعدل لقانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن لقانون العقوبات[2] و من خلال استقراء نصوصه فإننا لا نجد مصطلح جريمة القرصنة، بل الأكثر من ذلك لم يستعمل المشرع الجزائري لفظ الجريمة المعلوماتية او الالكترونية بل اعتمد تسمية جرائم المساس بأنظمة المعالجة الآلية للمعطيات و ذلك من المادة 394 مكرر الى غاية المادة 394 مكرر7[3].

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة. لذلك فقد آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابه، وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 04/09[4] المتضمن الوقاية من هذه الجرائم ومكافحتها[5].

الفرع الثالث: خصائص جريمة القرصنة الإلكترونية

تتميز جريمة القرصنة الإلكترونية بصفة عامة عن الجريمة التقليدية في عدة نواحي، كما أن تقنيات ارتكاب هذه الجرائم بدورها تتميز عن هذه الأخيرة لأن جريمة القرصنة الإلكترونية ترتكب بواسطة تقنيات تكنولوجيا الإعلام والاتصال (الأنترنت) والجهاز المستعمل في هذه الجريمة هو الكمبيوتر أو عدة أجهزة،

---

[1] القانون رقم 24- 06، المؤرخ في 19 شوال 1445، الموافق ل 28 ابريل 2024، المعدل والمتمم للأمر66-156، المتضمن قانون العقوبات، الج.ر، العدد 30، الصادرة في 30 ابريل 2024.

[2] معتوق عبد اللطيف، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، رسالة ماجيستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص122.

[3] مزوري اكرام، مرجع سابق، ص 313.

[4] القانون رقم 09-04، مؤرخ في 5 اوت 2009، **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها**، ج. ر العدد 47، الصادر بتاريخ 16 اوت 2009.

[5] سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجيستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013، ص 41.

ولهذا تتسم جريمة القرصنة الإلكترونية بمجموعة من الخصائص يمكن تلخيصها فيما يلي[1] سنتطرق الى السمات الخاصة بالجريمة ثم سمات المجرم المعلوماتي:

أولا: السمات الخاصة بالجريمة

تتميز جريمة القرصنة الالكترونية بعدة خصائص وهي:

1-أنها ترتكب من مجرم غير تقليدي وهي جرائم ناعمة

يختلف المجرم مرتكب جريمة القرصنة عن المجرم في الجرائم التقليدية ذلك لان له سمات مختلفة عن غيره كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنه أيضا فسمات هذا المجرم عموما هو إنسان اجتماعي، أي أنه متوافق مع مجتمعه وغالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة في هذا المجال، أو عن طريق الخبرة و الاحتكاك بالآخرين كما أن هذا المجرم إنسان ذكي ويستغل ذكائه في تنفيذ جريمته ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا[2].

كما تعتبر جريمة القرصنة جريمة ناعمة ينعدم فيها العنف والجهد العضلي اذ لا تتطلب مجهودا جسديا عنيفا لتنفيذها والتي يمكن ان ترتكب بمجرد الضغط على زر لإعطاء امر لإتلاف النظام وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك[3].

2-صعوبة اكتشاف وإثبات جرائم القرصنة الإلكترونية

تتميز جريمة القرصنة الالكترونية بأنها خفية ومستترة في أغلبها، وغير مرئية لأن الضحية لا يلاحظها رغم أنها تقع أثناء وجود الشبكة والجهاز، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة، مثلا عند إرسال الفيروسات وسرعة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم.

تكتشف الجرائم الالكترونية عن طريق الفحص والتدقيق أو عن طريق الشكاوى التي يقدمها المجني عليهم.

---

[1] عمر يوسف عبد الله، مرجع سابق، ص 195.

[2] رابحي عزيزة، مرجع سابق، ص 94.

[3] جدي نسيمة، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، رسالة ماجستير، كلية الحقوق، جامعة وهران، وهران، 2014، ص 27.

وترتكب الجريمة الالكترونية بالأرقام والبيانات تعتبر او تمحى من السجلات المخزنة في ذاكرة الكمبيوتر، ولأنها لا تترك أثرا خارجيا مرئيا، تكون صعبة الاكتشاف وما يزيد في هذه الصعوبة ارتكابها عادة في خفاء، وعدم وجود أثر كتابي ما يجري خلال تنفيذها من عمليات.

وتقع جريمة القرصنة في مجال المعالجة الآلية للمعطيات وتستهدف المعنويات لا الماديات، وهي بالتالي اقل عنفا وأكثر صعوبة في الاثبات، لأن الجاني مرتكب هذه الجريمة لا يترك وراءه اي أثر مادي خارجي ملموس يمكنه قبعة وهذا يعسر اجراءات اكتشاف الجريمة ومعرفة مرتكبها.

ويصعب في جريمة الالكترونية العثور على دليل مادي وذلك راجع الى استخدام الجاني وسائل فنية يتم فيها دليل وتلاعب به[1].

3-جريمة عابرة للحدود

هي جرائم عابرة للحدود ذات طابع دولي لا تعترف بالحدود اذ تقع بدولة ليمتد أثرها لدولة أخرى أو أكثر، ولعل هذه الخاصية اهم خصائصها قمع وجود الشبكات المعلوماتية الغير مرئية الحدود فان تبادل المعلومات[2] يتم في فضاء الكتروني معقد وهي عبارة عن شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لاي شخص في العالم، يتجاوز فيها السلوك المرتكب معناه التقليدي[3].

إذ تمتاز جريمة القرصنة بتخطيها للحدود الجغرافية وثم اكتسابها طبيعة دولية أو كما ذهب البعض إلى وصفها بجريمة ذات طبيعة متعدية الحدود بسبب ظهور شبكات المعلومات إذ لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات.

ومما ساعد على انتشار الجرائم الالكترونية هو ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والانترنت، جعل الانتشار الثقافي وعولمة الثقافة، والجريمة أمر ممكن وشائع، لا يعترف بالحدود الإقليمية للدول ولا بمكان ولا بزمان أصبحت ساحتها العال[4].

4-جريمة وسيلتها ونطاق أهدافها الشبكة العنكبوتية (الأنترنت)

إن حوسبة معظم القطاعات والمؤسسات (الاقتصادية، المالية، العسكرية والأمنية) منذ النصف الثاني من القرن الماضي بالإضافة إلى استعمال هذه البنى للاتصالات الحديثة وأنظمة المعلومات المتطورة

---

[1] عمر يوسف عبد الله، مرجع سابق، ص 195.

[2] جدي نسيمة، مرجع سابق، ص 27.

[3] شنتير خضرة، **الاليات القانونية لمكافحة الجريمة الالكترونية**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة احمد دراية، ادرار، 2021، ص 16.

[4] عمر يوسف عبد الله، مرجع سابق، ص 197.

والمرتبطة بالأنترنت، والتي أصبحت تغطي النطاق ألمعلوماتي والخدماتي، حيث أصبح الفضاء السيبيري مكان خصب لانتشار الجرائم المعلوماتية، إذ تستعمل للعثور على الأهداف المطلوبة وذلك بغية تخريبها أو قرصنتها أو اختلاسها أو سرقة المعلومات منها: الاقتصادية، العسكرية، الفكرية أو الشخصية[1].

5-سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه

تكون البيانات والمعلومات المتداولة عبر شبكة الأنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا لاسيما وأن الجاني يتعمد إلى عدم ترك أثر لجريمته ضف إلى ذلك ما يتطلبه من فحص دقيق لموقع الجريمة من قبل مختصين في هذا المجال للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة.

تتم جريمة القرصنة الالكترونية خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة ففي هاته البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة.

يعيق المجرم في جريمة القرصنة الالكترونية سلطات التحقيق الوصول إلى الدليل بشتى الوسائل، كمسح برامج أو وضع كلمات سرية ورموز وقد يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه.

يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم ذلك عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب، على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز وما إن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هاته الأوامر الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمرا في غاية الصعوبة[2].

6-أنها تتم عادة بتعاون أكثر من شخص

تتميز جريمة القرصنة أنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالجهة المجني عليها. وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب

[1] دحو نجاة، مرجع سابق، ص 24،25.

[2] صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 18.

والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك يتمثل في مساعدة فنية أو مادية[1].

7-نقص الخبرة لدى الأجهزة الأمنية والقضائية وعدم كفاية القوانين السارية

تتميز جريمة القرصنة بالكثير من السمات التي جعلتها تختلف عن غيرها من الجرائم، الأمر الذي أدى إلى تغيير شامل في آلية التحقيق وطرق جمع الأدلة المتبعة من الجهات التي تقوم بعملية التحقيق، وإضافة أعباء تتعلق بكيفية الكشف عن هذه الجريمة وأدلتها، وكذا القضاء من خلال تعديل الكثير من مفاهيمه التقليدية سواء فيما يتعلق بالأدلة أو لقوتها في الإثبات.

ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبه لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه الظاهرة.

لم تعد قادر القوانين التقليدية على مواكبة هذه السرعة الهائلة في التكنولوجيا، والتي أدت إلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها، مما تطلب تدخل المشرع لسن قوانين حديثة لمواجهة هذه الجرائم حفاظا على مبدأ الشرعية الجنائية، مع تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها[2].

ثانيا: السمات الخاصة بالمجرم

يتميز بعدة خصائص نذكرها كالاتي:

1-المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء

يتمتع مجرمو القرصنة الالكترونية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والأنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا. فتنفيذ

[1] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 58.

[2] صغير يوسف، مرجع سابق، ص 19.

الجريمة المعلوماتية يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.

إن المجرم المعلوماتي يمكن ان يكون تصورا كاملا لجريمته، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته، وذلك حتى لا يفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها[1].

2-مجرم غير عنيف

أي انه يرتكب نوعا من الجرائم ينتمي إلى إجرام الحيلة، فهو لا يلجأ إلى استخدام القوة والعنف في ارتكاب جريمته، لا سيما وأنه لا يتعامل مع أشخاص حقيقين، بل يتعامل في مقومات غير مادية متمثلة في البيانات والمعلومات المخزنة في جهاز الحاسب الآلي، ولهذا فليس هناك مبرر للجوئه إلى العنف[2].

3-مجرم محترف

يتصف مرتكب الجريمة الالكترونية بانه على درجة عالية من الخبرة والمهارة في استخدام الحاسب الآلي، والتكنولوجيا الحديثة[3].

4-شخصية اجتماعية

المجرم المعلوماتي لا يضع نفسه دائما في حالة عداء مع المجتمع الذي يحيط به، بل إنه إنسان متكيف معه، ويساعده ذكاؤه على سرعة التكيف، وقد تزداد خطورته الإجرامية كلما زاد تكيفه الاجتماعي مع توافر النزعة الإجرامية لديه[4].

5-مجرم الأنترنت يبرر ارتكاب جريمته

يوجد شعور لدى مرتكب فعل إجرام الأنترنت أن يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث مرتكبو هذه الجرائم بين الأضرار بالأشخاص، الأمر الذي يدعونه غاية في الأخلاقية وبين الاضرار بمؤسسة او جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.

---

[1] نهلا عبد القادر المومني، مرجع سابق، ص 77.

[2] الطاهر ياكر، **مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية**، مجلة الهدى للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، المجلد4، العدد4، 2022، ص 9.

[3] مرجع نفسه، ص 9.

[4] طاهر محمود أبو القاسم، **الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية مواجهتها**، المنظمة العربية للتنمية الإدارية، القاهرة، 2019، ص 55.

فهؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب، ويبدو ان الاستخدام المتزايد للأنظمة المعلوماتية قد أنشأ مناخا نفسيا موائما لتصور استبعاد فكرة الخير والشر قد يساعد على وجود احتكاك مباشر بالأشخاص، ومما لا شك فيه أن هذا التباعد في العلاقة الشائعة بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل[1].

6-الخوف من كشف الجريمة

يتصف مجرم القرصنة الالكترونية بالخوف من كشف جرائم وافضاح أمرهم، بالرغم هذه الخشية التي تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمين الأنترنت بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان.

وتساعد طبيعة الأنظمة المعلوماتية نفسها مجرمي القرصنة على الحفاظ على سرية أفعالهم، ذلك أن في كثير من الحالات ما يتعرض إلى اكتشاف أمره هو ان يطرأ في اثناء تنفيذه عوامل غير متوقعة لا يمكن التنبؤ بما في أن أهم الأسباب التي تساعد على نجاح الجريمة المرتكبة عبر الأنترنت هي الحواسيب انما تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم مرة أخرى[2].

7-الميل إلى التقليد

يبلغ الميل إلى التقليد أقصاه حينما يوجد الفرد وسط جماعة، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير الغير عليه، ويظهر ذلك في مجال الجريمة المرتكبة عبر الأنترنت لأن اغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه مما يؤدي به الأمر إلى ارتكاب الجرائم.

ولا شك أن ذلك نتيجة لعدم الاستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط، وينتهي به الأمر إلى التقليد وارتكاب الجريمة[3].

[1] عمر يوسف عبد الله، مرجع سابق، ص 204.

[2] مرجع نفسه، ص205.

[3] صغير يوسف، مرجع سابق، ص 35.

المطلب الثاني: دوافع وأساليب جريمة القرصنة الإلكترونية

يختلف مرتكبو جرائم القرصنة المعلوماتية عن مرتكبي الجرائم الاعتيادية من حيث المبدأ وطريقة القيام بالعمل الاجرامي، لكن في النهاية يبقى الطرفان مخالفان للقانون لذا يستحقان للعقاب بما اقترفوا من جرائم.

وهناك عدة اسباب تدفع الى ارتكاب جريمة القرصنة سنشير اليها في **(الفرع الأول)**، وأساليب الجريمة سنشير اليها في **(الفرع الثاني)**.

الفرع الأول: دوافع جريمة القرصنة الإلكترونية

ان الباعث او الدافع هو العامل المحرك للإرادة التي توجه السلوك الاجرامي، وغالبا ما تتجه التشريعات العقابية الى عدم اعتبار الدافع عنصرا من عناصر التجريم الا في الأحوال التي يحددها القانون صراحة، سنتطرق في هذا الفرع الى دوافع رئيسية ودوافع خارجية.

أولا: الدوافع الرئيسية

ان الدوافع الرئيسية على ارتكاب الجريمة المعلوماتية تتنوع وتتباين تبعا لطبيعة ودرجة خبرة المجرم في مجال المعلوماتية.

1-الدافع المادي

يعتبر الدافع المادي أهم وأخطر أسباب ارتكاب جريمة القرصنة، وذلك لما تحققه الجرائم المعلوماتية من ثراء فاحش مع تعرض الجاني إلى اقل قدر من الخطورة في إمكانية تعرضه للقبض عليه وتقديمه للمحاكمة، وذلك بسبب الصعوبات المرتبطة بخصائص الجرائم المعلوماتية في كونها ترتكب عن بعد وصعوبة استخراج الأدلة والقصور التشريعي لمواجهتها، ولكن يلزم لذلك ان يكون لديه مهارات فنية في التعامل في اختراق أنظمة المواقع المراد اختراقه لارتكاب الجريم. وقد يكون المحرك الأساسي الارتكاب تلك الجرائم هو الغرق في الديون المستحق، اول مشاكل العائلية الراجعة لأسباب مادية، او خسائر التي يتعرض لها لاعب القمار، او إدمان المخدرات، وقد يكون عند البعض منهم جميع هذه الوسائل لارتكاب الجريمة هي وسائل مشروعة، فالغاية تبرر الوسيلة[1].

[1] طاهر محمود أبو القاسم، مرجع سابق، ص 44.

2-دافع الرغبة في التعلم

يعتبر حب التعلم والاستطلاع من الأسباب الرئيسية التي تدفع الى ارتكاب مثل هذه الجرائم، لان المخترق يعتقد ان أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب ان لا تبقى المعلومات حكرا على أحد، أي أن للجميع الحق في التعرف والاستفادة من هذه المعلومات[1].

3-دوافع ذهنية

تتمثل هذه الدوافع في الشعور بالمتعة والتحدي، بالإضافة إلى الرغبة في فهم الأنظمة المعلوماتية وإثبات الذات. قد يكون مرتكب الجريمة الإلكترونية شخصًا مهووسًا بالتكنولوجيا، يسعى إلى اختبار قدراته من خلال تحدي الأنظمة والتفوق عليها. وغالبًا ما تتطلب هذه التحديات اختراق الأنظمة الإلكترونية وتجاوز الحواجز الأمنية المحيطة بها.

في بعض الحالات، قد تتسم هذه الأنظمة بدرجة عالية من التعقيد، مما يجعل اختراقها إنجازًا بحد ذاته بالنسبة للمجرم الإلكتروني، خاصة إذا كان ذلك وسيلته لشغل وقت فراغه. من جهة أخرى، قد يكون الدافع وراء ارتكاب الجريمة الإلكترونية هو الرغبة في قهر الأنظمة والتغلب عليها، كنوع من إثبات التفوق التقني. وفي هذه الحالة، لا يكون الدافع الأساسي تحقيق مكاسب مالية أو تدمير الأنظمة، وإنما ينبع من الشعور بالتحدي وإثبات المقدرة[2].

ثانيا: الدوافع الخارجية

قد يتأثر المجرم المعلوماتي ببعض المواقف قد تكون دافعة له على اقتراف الاجرام المعلوماتي يسعى فيها الى التسلية والمتعة أحيانا الى الانتقام، ويمكن ابراز اهم هذه الدوافع فيما يلي.

1-دافع التسلية

يعد المزاح والتسلية من العوامل التي قد تدفع بعض الأفراد إلى القيام بتصرفات غير مسؤولة، دون نية حقيقية لارتكاب جريمة. ومع ذلك، قد تؤدي هذه التصرفات إلى نتائج خطيرة تصل إلى حد الجريمة، حتى وإن كان الدافع الأساسي مجرد المزاح أو الترفيه[3].

---

[1] بن شريف أحلام، بوغرارة الصالح، **القرصنة الالكترونية أنواعها أشكالها وطرق التصدي لها**، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، جامعة تيارت، المجلد05، العدد01، جوان 2012، ص 39.

[2] رحراح شهرزاد، بوكر رشيدة، **جريمة القرصنة في التشريع الجزائري**، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة بن باديس، مستغانم، 2022، ص 15.

[3] صغير يوسف، مرجع سابق، ص 41.

2-دافع الانتقام

قد يكون الباعث على ارتكاب جريمة القرصنة الرغبة في الانتقام، فالانتقام من الغرائز البشرية، فكثير من الأفراد يفصلون من مناصب عملهم تعسفيا وبدون وجه حق، فاذا كان ذلك الشخص حائزا على معلومات متعلقة بسير النظام المعلوماتي وكان على قدر من الكفاءة في مجال المعلوماتية، فتجده يرتكب جريمته رغبة منه في الانتقام من الشركة والمؤسسة التي فصلته، ليجعلها تتكبد الخسائر المالية الكبيرة جراء ما يسببه لها من ضرر يحتاج إصلاحه الى وقت، يعتبر ضائعا من وقت نشاط المؤسسة أو الشركة[1].

الفرع الثاني: أساليب ارتكاب جريمة القرصنة الإلكترونية

تتشابه جرائم القرصنة الالكترونية مع الجرائم التقليدية من حيث اعتماد الجاني على وسائل وأساليب غير مشروعة لارتكاب جريمته. ومع ذلك، فان هذه الجريمة تتميّز بكون مرتكبيها يستخدمون تقنيات معقدة تهدف إلى خداع أنظمة الحاسب الآلي والتحايل على بنيتها المعلوماتية. وتتعدد أساليب تنفيذ هذه الجرائم، حيث يعتمد الجناة على أدوات تقنية متنوّعة لتنفيذ مخططاتهم. ورغم إمكانية تصنيف هذه الأساليب في الوقت الراهن، فإن التطور السريع في مجال تكنولوجيا المعلومات يجعل من الصعب التنبؤ بما قد يستجد من وسائل وأدوات تقنية في المستقبل.

ومن أبرز هذه الأساليب التقنية المستخدمة: الاختراق "**Hacking**" والبرمجيات الخبيثة مثل الفيروسات " **Virus** " ، وسنقوم فيما يلي بتوضيح هاتين الطريقتين بشيء من التفصيل.

أولا: الاختراق: « haking »

تعتمد معظم الجرائم المعلوماتية على تقنيات الاختراق، بهدف الوصول غير المشروع إلى أنظمة المعالجة الآلية للبيانات، والاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة.

يتطلب اختراق جهاز الضحية دون علمه استخدام مجموعة من الأدوات والوسائل التقنية، حيث يمكن تنفيذ هذا الاختراق عن طريق استغلال الثغرات الأمنية الموجودة في أنظمة التشغيل أو من خلال البروتوكولات المستخدمة في الشبكات. ويبدأ المخترق بمحاولة تحديد عنوان IP الخاص بالضحية، وهو العنصر الأساسي للوصول إلى الجهاز. ويتم ذلك عبر خطوات محددة ينفذها المخترق على جهازه، بشرط

[1] ربيعي حسين، **المجرم المعلوماتي شخصيته وأصنافه**، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 40، جوان 2015، ص 292.

أن يكون متصلًا بالإنترنت في نفس الوقت الذي يكون فيه جهاز الضحية متصلًا أيضًا، نظرًا لأن عنوان "**IP** " يتغير تلقائيًا مع كل اتصال جديد.

وقد يتم الاختراق باستخدام البرامج، ويشترط في هذه الطريقة وجود برنامجين أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم لأنه يأتمر بأوامر المخترق وينفذ المهام الموكلة إليه داخل جهاز الضحية وبرنامج آخر يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، وأخطر هذه البرامج برنامج "حصان طروادة"، وتتجلى خطورته لتميزه بالقدرة على الاختراق دون إمكانية كشفه وتتبعه والقضاء عليه واحتلال هذا البرنامج مكانا داخل النظام المخترق حتى ولو قام الضحية بحذفه فلا فائدة من ذلك، كما أنه يكفي أن يعمل البرنامج هذا لمرة واحدة فقط حتى يقوم بمهامه.

ويمكن إرساله للضحية عن طريق رسائل إلكترونية أو عن طريق استخدام برامج الدردشة. كما قد يتم اللجوء في عملية الاختراق إلى أسلوب التفتيش في مخلفات التقنية وذلك بالبحث في مخلفات الحواسيب من القمامات والمواد المتروكة على مستوى الجهاز عن أي شيء يساعد على النظام، كالبرامج المدون عليها كلمة السر أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، ومن خلال الأساليب أيضا في عملية الاختراق أسلوب المحاكات وذلك عن طريق التخفي بانتحال شخصية وصلاحيات شخص مفوض ومسموح له بالدخول إلى نظم المعلوماتية عن طريق استخدام وسائل التعريف الخاصة به، وفيها يتم إعطاء حزم عناوين **(IP)** شكلا معينا لتبدو و انها صادرة من جهاز حاسوب مسموح له بالدخول إلى تلك الأجهزة[1].

ثانيا: البرامج الخبيثة « les Verus »

تُعتبر الفيروسات نوعًا من الأمراض المعدية التي تصيب البيانات، فتؤدي إما إلى تدميرها أو تشويهها، مما يفقدها قيمتها في كلتا الحالتين، وفيروس الحاسب الآلي يشبه إلى حد كبير الفيروس الذي يصيب الإنسان لقدرته على الانتقال من حاسب إلى آخر والفيروس في مجال المعلوماتية هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي يصمم بشكل يجعل منه قادرا على التكاثر ونسخ نفسه إلى نسخ كثيرة والانتشار من نظام لآخر عبر شبكات الاتصال والقدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافه، كما أنه قد يكون مصمما لتدمير برامج أخرى أو تغيير معلومات ثم يقوم بتدمير نفسه ذاتيا دون أن يترك أي أثر يدل عليه.

[1] سعيداني نعيم، مرجع سابق، ص56، 57.

ويمكن أن يصاب الحاسب الآلي بالفيروس عند تشغيل الجهاز بواسطة أسطوانة مرنة مصابة وكذا عند نسخ برنامج أو تحميل ملفات أو برامج من الإنترنت، وكذلك عند تبادل البريد الإلكتروني المحتوي على الفيروسات.

وتتمتع الفيروسات بقدرة فائقة على مهاجمة أجهزة الحاسوب والشبكات المعلوماتية وتعطيل الاتصالات وتشويه البيانات وأحيانا تضلل المستخدم ببيانات خاطئة. ويستخدم الفيروس بشكل عام لتحقيق أحد الغرضين :

1-الغرض الحمائي

يُستخدم هذا النوع من الفيروسات بهدف حماية النسخة الأصلية من البرمجيات من النسخ غير القانوني. فعند محاولة نسخ البرنامج بشكل غير مرخص، يتم تفعيل الفيروس تلقائيًا، مما يؤدي إلى إتلاف نظام الحاسوب المستخدم، وذلك كعقوبة لمرتكب عملية النسخ غير المشروعة.

2-الغرض التخريبي

يتم تطوير هذه الفيروسات من قبل مبرمجين محترفين بهدف التخريب المتعمد، سواء بدافع التسلية أو إثبات المهارات أو لتحقيق مكاسب شخصية، مثل الوصول إلى بيانات حساسة أو تعطيل أنظمة معينة[1].

[1] سعيداني نعيم، مرجع سابق، ص 58،59.

المبحث الثاني: صور القرصنة الالكترونية وأركانها.

لقد أفرز التطور التكنولوجي المتسارع مظاهر جديدة من الإجرام، أبرزها ما يُعرف بـ"القرصنة الإلكترونية"، وهي جرائم ترتكب في الفضاء السيبراني من خلال استهداف الأنظمة المعلوماتية والمعطيات الرقمية بطرق غير مشروعة. وتمثل هذه الجرائم انتهاكاً خطيراً لسرية وأمن المعلومات، مما يهدد الأفراد، المؤسسات، بل والدول في استقرارها وأمنها الرقمي.

تُعدّ دراسة صور الجرائم وتحديد أركانها القانونية ضرورة ملحة لفهم طبيعتها وتمييزها عن غيرها من الجرائم التقليدية، وتمكين الأجهزة القضائية والأمنية من مكافحتها بفعالية. فمن الناحية القانونية، تستند هذه الجرائم إلى أركان أساسية، في مقدمتها الركن القانوني الذي يُجسد وجود نص يجرّم الفعل، والركن المادي الذي يتمثل في النشاط الإجرامي (كالدخول غير المشروع أو الإتلاف)، والركن المعنوي الذي يقوم على القصد الجنائي، سواء كان عاماً أو خاصاً حسب طبيعة الجريمة.

وعليه، فإن هذا المبحث يسعى إلى تحليل هذه الجريمة الإلكترونية من خلال مطلبين أساسيين: **(المطلب الأول)** المتمثل في صور القرصنة الالكترونية و**(المطلب الثاني)** متمثل في اركان جريمة القرصنة الالكترونية

المطلب الأول: صور القرصنة الالكترونية في الجزائر وتصنيفها

تطورت جرائم القرصنة بشكل متسارع بفعل التقدم التكنولوجي. وقد أدرك المشرع الجزائري خطورة هذه الأفعال على الأمن الوطني والمصالح الاقتصادية والاجتماعية، فسعى إلى وضع إطار قانوني للحد منها ومعاقبة مرتكبيها. وفي هذا السياق، تضمّنت التشريعات الجزائرية، خاصة قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، نصوصًا واضحة تُجرّم مختلف صور القرصنة الإلكترونية، مثل اختراق الأنظمة المعلوماتية، وإتلاف البيانات الإلكترونية. وتأتي هذه النصوص القانونية في ظل التزامات الجزائر الدولية، وحرصها على ملائمة قوانينها مع المعايير العالمية لمكافحة الجريمة الالكترونية.

ولقد تطورت جرائم القرصنة الإلكترونية بتطور التكنولوجيا، ونتج عن هذا التطور الاجرامي ظهور فئات جديدة من الجناة، لهم سمات مختلفة بشكل كبير من الجناة التقليديين، سنتطرق في الفرع الاول الى اهم صور القرصنة التي جاء بها المشرع الجزائري وفي الفرع الثاني تصنيف الجناة.

الفرع الأول: صور القرصنة الإلكترونية

تختلف القرصنة حسب الدافع والغاية منها فنجد القرصنة الانتقامية[1] والقرصنة السياسية[2]، القرصنة الذاتية[3] والقرصنة المالية.

ولقد نص المشرع الجزائري على أنواع أخرى جاءت في القانون رقم 04-15[4] الصادر في اكتوبر 2004، المتضمن قانون العقوبات بتجريم كل انواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، لقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر الى 394 مكرر 07، وتأخذ صور الاعتداء صور وهم: الدخول والبقاء في نظام المعالجة الآلية، جريمة ادخال معطيات غير موجودة، التعامل في معطيات غير مشروعة.

---

[1] القرصنة الانتقامية: والتي غالبا ما تكون بين الدول على خلاف سياسي وهو ما يمكن رؤيته بين إيران وكوريا الشمالية أو حتى مجموعات مؤيده للقضية الفلسطينية من جهة وبين دول الاحتلال الصهيوني.

[2] القرصنة السياسية: استخدام القرصنة الالكترونية لتحقيق اهداف ومخططات سياسية وليس لدافع شخصيمن قبل مجموعات ناشطة في مجال القرصنة السياسية.

[3] القرصنة الذاتية: القرصنة تقوم بعض الدول بقرصنة نفسها لتكون هذه العملية مقدمه لاتهام دول اخرى بهذه القرصنة.

[4] القانون رقم 04-15، المتضمن تعديل ق ع، لسنة 2004، المؤرخ في 10 نوفمبر 2004، المعدل والمتتم للامر 66-156، الصادر في الج.ر. رقم:71.

أولا: جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

ان المشرع الجزائري تطرق إلى هذه الجريمة في المادة 394 مكرر[1] إلى الدخول غير المشروع أو حذف أو تغيير المعطيات أو تخريب نظام المعالجة الآلية للمعطيات وسواء كانت الجريمة تامة أو شرع في ارتكابها ويتضح ذلك من خلال كلمة أو يحاول ذلك.

ويعني بمحاولة الدخول أو البقاء في النظام المعلوماتي الشروع في ارتكاب الجريمة دون تحقيق النتيجة، وفي هذه الحالة يعاقب الجاني بنفس العقوبة الذي تمكن من ارتكاب الفعل، ويتمثل الشروع في جملة من التصرفات أو لها مادية من خلال ارتكاب الشروع في جملة من التصرفات أو لها مادية من خلل ارتكاب الجاني للسلوك الإجرامي وثانيها توفر النية الإجرامية.

والصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيها، والصورة المشددة تتحقق بتوفر الطرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام استعمال المنظومة وهذا ما نصت عليه المادة 394 مكرر2[2] .

ثانيا: جريمة ادخال او إزالة معطيات

يمكن تعريف هذه الجريمة بانها كل فعل او نشاط يقوم به الجاني في نظام الحاسوب ومن شانه الدخول او الازالة او التعديل في المعطيات المتعلقة بنظام الحاسوب، هذا من جهة و من جهة أخرى يطلق على هذه الجريمة بالقرصنة المعلوماتية لأن هدف الجاني فيها هو تحقيق النظام المعلوماتي لنتائج ومعطيات غير تلك التي كان يجب ان يحققها[3].

نصت المادة 394 مكرر1[4] من قانون العقوبات 04-15 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية أو إزالة أو عدل هذه المعطيات وذلك عن طريق استعمال الغش، هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوفر الركن المادي، وأفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء إضافة

---

[1] انظر القانون رقم 04-15، السابق الذكر.

[2] عمر يوسف عبد الله، مرجع سابق، ص 250.

[3] دردور نسيم، **جرائم المعلوماتية على ضوء القانون الجزائري**، رسالة ماجستير، كلية الحقوق، جامعة منتوري، قسنطينة، 2013، ص 25.

[4] انظر القانون رقم 04-15، السابق الذكر.

معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك ادخال فيروس المعلوماتية في البرامج من أجل افسادها[1].

ثالثا: التعامل في معطيات غير مشروعة

تعد جرائم المعطيات من أخطر الجرائم وأكثرها ضررا، خاصة إذا تعلقت هذه المعطيات بأمن الدولة او الحياة الخاصة ولهذا حرص المشرع الجزائري على مكافحة هذه الجريمة وفرض عقوبة لها.

حيث يمكن تعريف جريمة التعامل في معطيات غير مشروعة بانها كل اشكال وأنواع التعامل الواقعة والواردة على معطيات الحاسب الالي السابقة لعملية استعمال هذه المعطيات لارتكاب جريمة ما، بداية من تخطيط المعطيات والبحث فيها وتجميعها وصولا الى نشرها، من أجل جعلها في متناول الغير او الاتجار بها[2].

وقد جرمت المادة 394 مكرر 02[3] من قانون العقوبات السابق الذكر الأعمال الآتية: تصميم أو بحث أو تجميع أو توفير أو نشر معطيات مخزنه أو معالجة مرسلة عن طريق منظومة معلوماتية، يمكن ان ترتكب بها إحدى جرائم الغش المعلومات السابقة الذكر[4]، ويقصد بتصميم عمليات هذه الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية أو المعطيات المعلوماتية في حد ذاتها[5]، كما جرم المشرع كذلك افعل الحيازة أو إفشاء أو نشر أو استعمال المعطيات متحصلة في إحدى جرائم الغش المعلوماتي لأي غرض.

الفرع الثاني: أصناف القراصنة

حصرهم تحت طوائف محددة، ولكن هذا لا يعني انه لا توجد محاولات في تحديد مختلف أصناف مجرمي الانترنت، بل على العكس هناك عدة دراسات وأبحاث حاولت وضع قواعد يصنف بها المجرمون على حسب خطورتهم الاجرامية ويمكننا حصرهم الى:

---

[1] رحراح شهرزاد، مرجع سابق، ص 31.

[2] بودواب سمير، لبديوي فؤاد، **جرائم المساس بأنظمة المعالجة الالية للمعطيات**، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 20 اوت 1955، سكيكدة، 2024، ص 31.

[3] انظر القانون رقم 04-15، السابق الذكر.

[4] رحراح شهرزاد، مرجع سابق، ص 32.

[5] دردور نسيم، مرجع سابق، ص 32.

أولا: القراصنة

هناك صنفان من القراصنة:

1-القراصنة الهواة (الهاكرز)

هم بارعون في استخدام الحاسب الآلي وبرمجته لديهم فضول في استكشاف حواسيب الآخرين بطرق غير مشروعه متطفلون يتخذون إجراءات امن نظم الشبكات لكن لا تتوفر الطائفة في الغالب دوافع تخريبية، انما ينطلقون من دوافع التحدي واثبات الذات، تتشكل هذه الطائفة في الغالب من مراهقين وشباب متمدرس البرمجة وأنظمة التشفير.

غير انه بالنسبة لعامه الناس يبقى الهاكرز فتيا يقومون بالسطو على المواقع والشبكات متسببين بالأذى والخسائر الماديةوالأمنية والمعنوية إلى جانب تشويهم صورة جراء هزيمتها أو عدسها عن صدر هجمات ينفذها مراهقون.

من مهاراتهم أنهم يستطيعون اختراق مواقع الشركات واختراق وفك كلمه السر سواء الخاصة بالبريد الالكتروني أو موقع شركه على الانترنت[1].

2-المحترفون أو المخترقون:

وهي كلمه مستمده من الانجليزية من الفعل (crack) ويعني التحطيم أو الكسر أو السطو على او السحق، وهذه هي الصفات التي يتميز بها هذا النوع[2]. هذه الفئة تعكس اعتداءاتهم ميولا إجرامية خطرة تنبئ عن رغبتها في إحداث التخريب، وهم أكثر خطورة من الصنف الأول[3]، وتنظم هذه الطائفة نفسها بعقد مؤتمرات المخترق الكمبيوتر يدعى لها الخبراء منهم لتشاور حول وسائل الاختراق ووسائل تنظيم عملهم، وقد يحمل هؤلاء في مجموعات، ولكن العديد منهم يعمل بمفرده. وبالرغم من ذكائهم قد يكونون مختلفين في مدارسهم او غير منتظمين بالدراسة، وقد يكون لبعضهم القليل من الأصدقاء. ويقومون بإتلاف البيانات والمعلومات من الأنظمة الآلية. وعادة ما يعود هؤلاء المجرمون للجريمة، حيث أنهم لا يمتلكون فكرا متطرفا، ولكن تسيطر عليهم الأفكار التي تعود عليهم بالربح المادي، حيث اعتاد من عوائد جرائمهم[4] .

[1] بن الشريف احلام، بوغرارة الصالح، مرجع سابق، ص 30.

[2] طاهر محمود ابو القاسم، مرجع سابق، ص 51.

[3] مزوري اكرام، مرجع سابق، ص 315.

[4] طاهر محمود ابو القاسم، مرجع سابق، ص 51.

ثانيا: المخادعون:

ويتمتعون بقدرات فنية عالية وذكاء باعتبارهم أصحاب كفاءات وأخصائيين في النظام المعلوماتية، جرائمهم على شبكات تحويل الأموال، ويمكنهم التحايل والتلاعب بحسابات المصارف او فواتير الكهرباء أو تزوير بطاقات الائتمان وما شابه. وتهدف اعتداءاتهم بالأساس إلى الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم، وقد يعملون في الليل، مشغولين بعملهم في النهار، ويخترقون الأجهزة المستهدفة في أي منطقه وأي زمان، وقد يكونون مراهقين، ورغم صغر سنهم ينجحون في اختراق كل أنواع النظم، والبنوك، والشركات، والنظم العسكرية.

ثالثا: الجواسيس:

يهدفون الى جمع معلومات لمصلحة دولهم لأسباب سياسية، او لمصلحة بعض الاشخاص او الشركات التي تنافس فيما بينها ويطلق عليهم لصوص نظم المعلومات[1]. ولقد تحولت وسائل التجسس من الطرق التقليدية إلى طرق حديثة استخدمت فيها التقنية الحديثة خاصة مع وجود الانترنت، وذلك من خلال اختراق هذه الشبكات والمواقع من قبل الهاكر، فيقوم هؤلاء بالعبث او إتلاف محتويات تلك الشبكة هذا من جانب، ومن جانب آخر وهو الأهم والذي يشكل الخطر الحقيقي على تلك المواقع، إذ يمكن في عمليه التجسس التي يقوم بها الأجهزة الاستخبارية للحصول على أسرار ومعلومات الدولة، ومن ثم إفشائها الى دولة أخرى معادية أو استغلالها لما يضر المصلحة الوطنية[2].

ومن أهم أهداف هذه الطائفة في استخدام الأنظمة المعلوماتية، الحصول على معلومات الأعداء والأصدقاء على حد سواء، بغيات تفادي شرها أو التفرق عليها، ولم تعد المعلومات العسكرية هي الهدف الرئيسي، بل أصبحت تشمل المعلومات الاقتصادية والتقنية[3] .

رابعا: طائفة القراصنة مخترقي الأنظمة:

تتبادل أفراد هذه الطائفة المعلومات فيما بينهم، بغية إصلاح بعضهم على مواطن الضعف في الأنظمة المعلوماتية، وتجري عمليه التبادل للمعلومات بينهم بواسطة النشرات الإعلامية الالكترونية مثل المجموعات الأخبار بل أن أفراد هذه الطائفة يتولون عقد المؤتمرات بكافة محترفي الأنظمة المعلوماتية بحيث يدعى إليها الخبراء من بينهم للتشاور حول وسائل الاختراق وآليات نجاحها، العمل فيما بينها، ويتبع

[1] طاهر محمود أبو القاسم، مرجع سابق، ص 52.

[2] صغير يوسف، مرجع سابق، ص 29.

[3] عمر يوسف عبد الله، مرجع سابق، ص210.

المحترفون أساليب في عمليات تشويه صفحات المواقع، وتختلف هذه الأساليب من موقع لآخر حول نوع النظام الذي يعتمد عليه الموقع.

وتبرز سمات هذه الطائفة أيضا، في أنهم ينطلقون من دوافع التحدي واثبات المقدرة على اختراق الأنظمة المعلوماتية، نشاطاتهم ليست تخريبا، بل أن العديد من الجهات تستعين بهم، في عمليه فحص وتدقيق مستوى امن الأنظمة المعلوماتية فيها، وأفراد هذه الطائفة ليس لهم فئة عمرية محددة أيضا، فمنهم الصغار والكبار وهم في الغالب لا ينتمون إلى طائفة مجرمين التقنية والكسب المادي ليس من أولوياتهم، وإنما مجرد المتعة والإشباع الشخصي في إثبات قدراته وكفاءاتهم على اختراق الأنظمة المعلوماتية، الى درجه أنهم ينصبون أنفسهم اوصياء على امن الأنظمة المعلوماتية في المؤسسات المختلفة[1].

المطلب الثاني: أركان جريمة القرصنة الإلكترونية

تتكون الجريمة من مجموعة من الأركان الأساسية التي يشترط القانون توافرها لقيام المسؤولية الجنائية، وتنقسم هذه الأركان الى نوعين، اركان عامة وهي عناصر لا غنى عنها في أي جريمة بغض النظر عن نوعها او طبيعتها، اركان خاصة وهي العناصر التي يحددها المشرع لكل جريمة على حدى وفقا لخصوصيتها.

ومن المعروف ان الجريمة في صورتها التقليدية تتكون من ثلاث اركان رئيسية، الركن الشرعي والركن المادي، الركن المعنوي، وتعد جريمة القرصنة الالكترونية واحدة من التي تندرج ضمن نطاق الجريمة المعلوماتية وتتوفر فيها الأركان العامة للجريمة كما في سائر الجرائم، وتم تقسيم هذا المطلب الى ثلاثة فروع، في **(الفرع الأول)** الركن الشرعي، و**(الفرع الثاني)** الركن المادي، و**(الفرع الثالث)** الركن المعنوي

الفرع الأول: الركن الشرعي:

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضح العقوبة المترتبة عليه، لا جريمة ولا عقوبة ولا تدابير أمن إلا بنص قانوني، فلا يعتبر الفعل الإجرامي مجرما إلا إذا وجد نص قانوني يقضي بذلك والجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه[2].

[1] صغير يوسف، مرجع سابق، ص 32

[2] مرجع نفسه، ص 59،60.

أولا: جريمة الدخول او البقاء غير المصرح بهما الى نظام المعالجة الآلية للمعطيات:

قبل التعديل:

تنص المادة 394 مكرر من ق 04-15[1] أن يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج.

بعد التعديل:

تنص **المادة 394 مكرر من** القانون رقم **24-06**[2] **بأن يعاقب** بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000 دج إلى 300.000 دج.

ثانيا: ادخال أو إزالة المعطيات

قبل التعديل:

تنص المادة 394 مكرر 1 من ق 04-15[3] بأن يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

[1] انظر القانون رقم 04-15، السابق الذكر.

[2] انظر القانون رقم 24- 06، السابق الذكر.

[3] انظر القانون رقم 04-15، السابق الذكر.

بعد التعديل:

تنص المادة 394 مكرر 1 من ق 24-06 [1] **أن** يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

ثالثا: جريمة التعامل في المعطيات غير المشروعة:

قبل التعديل:

تنص المادة 394 مكرر 2 من ق 04-15[2] أن يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم .

بعد التعديل:

تنص المادة 394 **مكرر2 من ق 24-06**[3] **أن يعاقب** بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

الفرع الثاني: الركن المادي

يتمثل في كافة الاعتداءات المادية وانتهاك كل ما هو محل حماية قانونية ويعتمد على ثلاث عناصر أساسية تتمثل في الفعل او السلوك الاجرامي، النتيجة والعلاقة السببية، وتوفر الركن المادي في جريمة

[1] انظر القانون رقم 24-06، السابق الذكر.

[2] انظر القانون رقم 04-15، السابق الذكر.

[3] انظر القانون رقم 24-06، السابق الذكر.

القرصنة الالكترونية يفترض بيئة رقمية واتصال بالشبكة المعلوماتية، ويتطلب معرفة النشاط الاجرامي وبداية الشروع فيه وصولا لموعد حدوث النتيجة.

اولا: جريمة الدخول او البقاء:

انطلاقا من نص المادة 394 مكرر من قانون العقوبات الجزائري و النصوص القانونية السابقة فإن تحقق الركن المادي لجريمة الدخول او البقاء بغش غير المصرح به، يتسم بسلوك اجرامي يرتكبه الجاني قد يتخذ صورة الدخول المنطقي وذلك لفتح باب يؤدي الى نظام المعالجة الآلية بمكوناته المختلفة، و احيانا يتخذ صورة البقاء و ينصب هذا السلوك على محل معين هو المعلومات و نظم معالجتها و هذا السلوك قد يلحق اضرار في بعض الحالات بهما اذا فالركن المادي هو عبارة عن نشاط اجابي من جانب الجاني، و يكون الاتصال بطريق الغش متى كان الجاني لا يحق له الدخول لأي سبب من الأسباب، و هو تعبير يتسع لاستعمال كل الوسائل المتاحة للدخول الى النظام و لكن الضابط و المعيار في ذلك هو انعدام حقه في الخول بهذا النظام المعلوماتي كله او جزء منه، فمدلول كلمة دخول تشير الى كل الأفعال التي تسمح بالولوج الى نظام معلوماتي و الإحاطة و السيطرة على المعطيات و المعلومات التي يتكون منها.

و يتحقق الركن المادي بإحدى الصور التالية: اولهما: اختراق الاجهزة الرئيسية بطريق الغش الى نظام المعالجة الآلية للمعطيات، و ثانيهما: البقاء او الوجود بطريق الغش في نظام المعالجة الآلية او جزء منه، فمن الواضح من خلال نص المادة 394 مكرر انه هناك صورة بسيطة للدخول الى النظام او البقاء فيه و أخرى شدد فيها المشرع للعقوبة اذ نصت المادة 394 مكرر من قانون العقوبات انه " تضاعف العقوبة اذا ترتب على ذلك حذف او تغيير لمعطيات المنظومة و اذا ترتب على الأفعال المذكورة اعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 6 اشهر الى سنتين، و الغرامة من 50.000 دج الى 150.000 دج .

من خلال استقراء نص المادة 394 مكرر نجد انها قد نصت الى ظرفين تشدد بهما عقوبة الدخول، او البقاء داخل النظام، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول والبقاء غير المشروع محو او تعديل البيانات التي يحتويها النظام، او عدم تأدية النظام او عدم قدرة النظام على تأدية وظيفته، ويكفي لتوفير هذا الظرف المشدد ان تكون هناك علاقة سببية بين الدخول او البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام، او عدم قدرته على أداء وظيفته، او تعديل البيانات[1].

[1] رابحي عزيزة، مرجع سابق، ص 162.

1-فعل الدخول غير المصرح به:

ان الدخول الغير مشروع يتم بمجرد الاتصال بالنظام المعلوماتي[1] وفعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد بها الدخول المادي الى المكان الذي يتواجد به الحاسوب نظامه بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية الى النظام المعلومات أي الدخول المعنوي.

ويتخذ الدخول صورا مختلفة؛ فمنها ان يقوم الفاعل بتشغيل جهاز مغلق وبالتالي الاطلاع على ما به من بيانات. ومنها ما يقوم به الفاعل باستخدام برامج للدخول في النظام بدون اذن صاحبه فيطلع على ما يقوم به صاحب الجهاز او ينتقل الى اجزاء الجهاز ليطلع على ما يحتويه اقسام هذا الجهاز من معلومات[2].

2-فعل البقاء غير المصرح به:

البقاء هو المرحلة التي تلي الدخول الى النظام[3]، ويتحقق الركن المادي لهاته الجريمة أيضا إذا اتخذ صورة البقاء في النظام ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[4].

ثانيا: الركن المادي جريمة ادخال او إزالة المعطيات:

الركن المادي لجريمة المساس بالمعطيات او التلاعب بها يتحقق بإتيان الجاني لفعل من الصور الثلاث التالية:

-الإدخال

-المحو أو الازالة

-التعديل

وهي الصور المنصوص عليها بالمادة 394 مكرر واحد من قانون العقوبات السالفة الذكر والمنصوص عليها بالمواد3،4,8 من الاتفاقية الدولية للإجرام المعلوماتي وتقابلها المادة 323 الفقرة الثالثة من قانون العقوبات الفرنسي الجديد.

ولا يشترط الركن المادي توفر الصور الثلاث بل يكفي أن يدخل الجاني معطيات مغلوطة جديدة لم تكن موجودة أو محو معطيات موجودة أو تعديل أخرى كانت موجودة أصلا يحتويها النظام، فغاية الامر أن يرد الأمر على معطيات بإحدى الصور وكل هذه الأفعال تؤدي إلى تغيير في الحالة التي كانت عليها

---

[1] دردور نسيم، مرجع سابق، ص 25.

[2] رابحي عزيزة، مرجع سابق، ص 163.

[3] دردور نسيم، مرجع سابق، ص 27.

[4] رابحي عزيزة، مرجع سابق، ص 166.

المعطيات محل الاعتداء وتؤدي إلى المساس بسلامتها وتكاملها وعليه وبهذا المفهوم لا تتحقق الجريمة بالنسبة للمعطيات التي لم تتم معالجتها بعد في نظام معين ولم تدخله بعد، إذ تتمتع المعالجة بالحماية متى بدأت ومتى تضمنت المعطيات بنظام معين يخضع لحماية كالمعطيات المحفوظة على روابط تخزين كالأقراص أو الوسائط خارج النظام، وهنا بهذه الصورة يفتح المجال لدراسة الجريمة التامة والشروع فيها.

وهذه الصورة اصطلح عليها بعد الفقه بالقرصنة المعلوماتية فهذه الجريمة لا تستهدف النظام بل يستهدف فيها الجاني الوصول للمعلومات الموجودة أو اختراق النظام المعلومات لم تكن موجودة او لمحو وتعديل المتضمنة .

ولا يشترط في هذه الجريمة ان تتم بطريقة مباشرة من الجاني فقد تتم عن بعد وهذه هي الصورة المثالية للقرصنة أو بتدخل شخص آخر

1-الإدخال

يتحقق الإدخال بإضافة معطيات جديدة على الدعامة الأساسية للنظام سواء كانت خالية أم توجد عليها معطيات من قبل وهنا يستوي أن يقوم بفعل الإدخال شخص أجنبي لا يحق له التواجد واستعمال النظام وأن يكون من المصرح لهم باستعمال النظام إلا أنه يعمد لإدخال معطيات خاطئة تخرج عن الاستعمال المنوط بمهامه[1].

2-المحو

يقصد بالمحو:" اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق ضغط خصائص أخرى فوقها أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة."

وعملية المحو هي عملية لاحقة على إدخال المعطيات فلمحو يفترض الوجود السابق لعملية الإدخال. لعل هذا ما قصده المشرع الجزائري من خلال صياغة نص المادة الذي لم ينص على كيفية محددة للمحو كما لم يتضمن شرحا لمفاهيم صور الجرائم بل اقتصر على تعدادها، و عليه يتحقق المحو بأي صورة كانت حسب رأينا، فيكفي أن تخفي المعطيات من المنظومة التي أدخلت اليها بصفة شرعية بداية لنكون أمام محو سواء تم الاحتفاظ بها من قبل الجاني أو أزال مباشرة نهائيا[2].

[1] جدي نسيمة، مرجع سابق، ص 63،64.

[2] مرجع نفسه، ص 66، 67.

3-التعديل

يقصد بالتعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بأخرى جزئيا أو كليا، كذلك يتم التلاعب بالمعطيات عن طريق استبدالها أو التلاعب بالبرنامج بإمداده بمعطيات مغايرة عن تلك التي صمم لأجلها مما يؤدي لنتائج مغايرة عن تلك المنتظرة.

ثالثا: جريمة التعامل في المعطيات غير المشروعة:

بقراءة المادة 394 مكرر 2 من قانون العقوبات فان الركن المادي لهذه الجريمة يتمثل في مجموعة من الأفعال المذكورة على سبيل الحصر.

وما يلاحظ أوليا انه طبقا للقواعد العامة مساهمه المنصوص عليها بقانون العقوبات فان الأفعال المجرمة بهذه الفئة لا تتعدى كونها من أعمال الاشتراك طبقا للمادة 42 من قانون العقوبات.

فهي ليست مساهمة مباشرة في الجريمة انما اعمال مساعدة ومعاونة جعل منها المشرع جريمة كاملة وتامة بنص خاص وعليه اصبحت فعل مجرم مستقل عن الجريمة الاصلية، والفائدة في امكانية عقاب افعال المساعدة في غياب الجريمة الاصلية.

وسندرس الركن المادي لهذه الفئة من الجرائم في نقطتين:

-محل الجريمة

-السلوك المجرم والمتمثل في فئتين: تعامل في معطيات صالحه لارتكاب جريمة، التعامل في المعطيات متحصله من جريمة.

1-محل الجريمة:

محل الجريمة طبقا للمادة 394 مكرر 2 من قانون العقوبات اما:

-معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية.

-معطيات متحصل عليها من احدى الجرائم المنصوص عليها بالمواد من 394 مكرر 394 مكرر 1.

وبهذا التعداد فان المشرع هدف لتوسيع دائرة التجريم اذ شمل بالحماية المعطيات مهما كانت حالتها، اذ لم تقتصر على الموجودة بنظام المعالجة الالية كجرائم السابقة بل وسع المجال الى مختلف المعطيات مهما كانت حالتها مخزنة، مرسلة، معالجة على اعتبار امكانيه ارتكاب جرائم حتى باستعمال معطيات موجودة على وسائل تخزين خارجية.

كما لم يخص المشرع بتجريم المعطيات المعدة لارتكاب جريمة بالتحديد في ان تكون صالحة او قابلة لان ترتكب بها جريمة وهذا ما نصت عليه المادة 394 مكرر 2 بالفقرة الاولى بعبارة "...يمكن او ترتكب بهذا الجرائم[1].

2-السلوك المجرم:

السلوك المجرم طبقا للمادة 394 مكرر 2 من قانون العقوبات هو:

1.2 التعامل في معطيات صالحة لارتكاب الجريمة:

وهي الجريمة المنصوص عليها بالفقرة الأولى من المادة 394 مكرر 2 من قانون العقوبات وورد فيها أفعال على سبيل الحصر والتي تشمل كافة أشكال التعامل على المعطيات السابقة لعملية استعمالها في ارتكاب جريمة والمتمثلة في ست أفعال (التصميم- البحث – التجميع – التوفير – النشر – الإتجار)

2.2 التعامل في معطيات متحصلة من جريمة:

وهي الجريمة المنصوص عليها بالفقرة الثانية من المادة 394 مكرر 2 من قانون العقوبات وهي الجريمة التي تتحقق بأربع سلوكات ذكرت على سبيل الحصر المتمثلة في (الحيازة – الإفشاء- النشر – الاستعمال)[2].

ثالثا: الركن المعنوي:

جرائم المعلوماتية هي في اغلبها جرائم عمدية، حيث يستوجب المشرع فيها توفر القصد الجنائي بركنيه العلم والإرادة، اذ يجب ان تتجه إرادة المجرم الى ارتكاب سلوك يحظره القانون، كالاعتداء على نظام المعالجة الالية للمعطيات، بما يشمله من صور كفعل الدخال لبيانات او المحو او التعديل، او الى نسخ البرامج بوجه غير شرعي[3]. وتتعدد الجرائم المرتكبة في جريمة القرصنة ونحن في هذه الدراسة سنقوم بالتطرق الى الركن المعنوي في الجرائم التي تدخل في نطاق جرائم التي تمس نظام المعالجة الآلية للمعطيات:

إن جريمة الدخول أو البقاء إلى نظام المعالجة الآلية بطريق غير مشروع، يتطلب القصد فيها علم الجاني بأنه يدخل إلى نظام المعالجة الآلية للمعطيات الخاصة بالغير، وأن تتجه إرادته إلى ارتكاب هذه الجريمة، أي أن اكتمال هذه الجريمة يستدعي توفر الركن المعنوي.

---

[1] جدي نسيمة، مرجع سابق، ص 71.

[2] مرجع نفسه، ص. ص 71، 74.

[3] معتوق عبد اللطيف، مرجع سابق، ص 24.

وبتوافر سوء نية الجاني، إذا كان دخوله الى نظام نتيجة اختراقه لجهاز الأمن الذي يحمي النظام او معرفة الرقم السري أو الشيفرة بطريق غير مشروع ودخل بواسطتها الى النظام، اما إذا كان الجاني سبق له الاشتراك في النظام، ولكن انتهت مدة الاشتراك ودخل الى النظام معتقدا خطأ بأنه مازال له الحق في الدخول اليه. فان ذلك يعد جهلا بالواقع مما ينفي القصد الجنائي لديه، اما إذا دخل بطريق الخطأ ولكنه بقي يتجول داخل النظام مع علمه بذلك فانه يقع تحت طائلة المسؤولية[1].

اما جريمة ادخال او إزالة المعطيات تتطلب قصد جنائي عام و هو ما نستشف من نص المادة 394 مكرر : " كل من أدخل أزال عدل بطريق الغش " فمصطلح الغش يدل على ضرورة توفر قصد جنائي عام بعنصريه، و عليها يجب أن تتجه إرادة الجاني إلى ارتكاب السلوك الإجرامي بإحدى الصور على النحو السالف بيانه، و لا تتطلب المادة 394 مكرر 1 قصد خاص إنما يكفي توافر قصد عام إذ لا تشترط نية الإلحاق الضرر بالغير و لا يشترط أن يتصرف الجاني بنية إلحاق الضرر إذ تقوم الجريمة متى قصد الجاني التلاعب بالمعطيات المتضمنة بنظام المعالجة الآلية للمعطيات.

جريمة التعامل في معطيات غير مشروعة جريمة عمدية لا بد من توافر عنصري القصد الجنائي من علم وارادة[2]، ويستفاد ذلك من عبارة المادة 394 مكرر2 " عمدا وعن طريق الغش" وفي هذه المادة عمد المشرع لتجريم مجموعة من الافعال التي تمس بالمعطيات الموجودة داخل نظام المعالجة الآلية، ولدينا ان الجريمة في صورتها الاولى " التعامل في معطيات صالحة لارتكاب جريمة " تتطلب قصدا خاصا هو قصد الاعداد او التمهيد لاستعمالها في ارتكاب جريمة.

اما الجريمة في صورتها الثانية " التعامل في معطيات متحصلة من جريمة " فلدينا انه يكفي لقيامها توافر القصد الجنائي العام[3].

[1] رابحي عزيزة، مرجع سابق، ص 167،168.

[2] جدي نسيمة، مرجع سابق، ص. ص 68، 75.

[3] مرجع نفسه، ص 70.

ملخص الفصل الأول:

نستخلص من مختلف التعريفات التي تطرقنا اليها في هذا الفصل ان القرصنة الإلكترونية هي الدخول غير المشروع او ادخال وإزالة معطيات في الحواسيب او الشبكات الرقمية وذلك بهدف اختراق وتدمير بيانات الغير، اذ غالبا ما تتم دون اذن من صاحب النظام او الجهات المالكة للمعلومات.

ويتبين من خلال التعرف على ماهية جريمة القرصنة، ان هذا النوع من الجرائم يتميز بطبيعة فريدة ومميزة، اذ هي جريمة لا تعترف بالحدود الجغرافية، وسيلتها ونطاق أهدافها الشبكة العنكبوتية، انها تتم عادة بتعاون أكثر من شخص. كذلك مرتكب هذه الجريمة هو شخص ذو خبرة بمجال الحوسبة ويتمتع بالمهارة والذكاء كما انه غير عنيف، كما ان هذا المجرم المعلوماتي تدفعه أسباب لارتكاب هذه الجريمة كدافع الرغبة في التعلم ودافع الانتقام.

واستخلصنا من القانون 04-15 ثلاث صور ذكرها المشرع الجزائري الا وهي جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وجريمة ادخال او إزالة معطيات والتعامل في معطيات غير مشروعة. ولقيام هذه الجريمة ثلاث اركان شأنها شأن الجرائم التقليدية، الركن الشرعي والركن المادي والركن المعنوي.

الفصل الثاني:

مكافحة جريمة القرصنة الالكترونية في التشريع الجزائري

الفصل الثاني: مكافحة جريمة القرصنة الالكترونية في التشريع الجزائري

يُعد التحقيق الجنائي في جريمة القرصنة أحد أبرز مجالات العدالة الجنائية الحديثة، نظراً لتطور أساليب الجريمة الإلكترونية وتعقيدها. ويُقصد بالتحقيق الجنائي في هذا السياق مجموعة الإجراءات القانونية والفنية التي تتخذها الجهات المختصة للكشف عن مرتكبي جريمة القرصنة الإلكترونية، وجمع الأدلة ضدهم، في إطار من الشرعية القانونية. وتتميّز هذه التحقيقات بخصائص فريدة، منها السرعة في التتبع، والاعتماد على تقنيات رقمية متطورة، والتعاون عبر الحدود، بسبب الطابع العالمي لهذه الجريمة. وتشمل أساليب ووسائل التحقيق في جريمة القرصنة استخدام أدوات تحليل البيانات الرقمية، والتتبع الإلكتروني، وتقنيات استرجاع المعلومات، إلى جانب التنسيق مع مزودي الخدمات التقنية. وقد بذلت الدول جهوداً كبيرة، سواء على المستوى الوطني عبر سنّ تشريعات خاصة بجريمة القرصنة وانشاء مراكز ووحدات متخصصة لمكافحتها وعلى المستوى الدولي من خلال اتفاقيات وتعاون قضائي وأمني، لمكافحة هذه الظاهرة العابرة للحدود وضمان حماية الفضاء المعلوماتي، وقد قسم هذا الفصل الى مبحثين: **(المبحث الأول)** يتمثل في ماهية التحقيق الجنائي في جريمة القرصنة، و**(المبحث الثاني)** العقوبات ودور التعاون الدولي والوطني.

المبحث الأول: ماهية التحقيق الجنائي في جريمة القرصنة

التحقيق الجنائي هو مواجهة بين المحقق والمجرم، حيث يسعى المحقق للوصول إلى الحقيقة وكشف الجريمة، بينما يحاول المجرم التهرب والتضليل، وتتطلب هذه المواجهة مهارات وخبرات ومعرفة بالقانون وعلم النفس الجنائي، ويتميز التحقيق الإلكتروني بخصوصية تجعله مختلفاً عن التحقيق التقليدي، إذ يتطلب أدوات وأساليب حديثة تتماشى مع طبيعة الجرائم الإلكترونية

فالتحقيق في الجرائم الإلكترونية لا يعتمد فقط على الأجهزة الإلكترونية، بل يشمل تحليل النظام والحركات التي قام بها المخترق، لتحديد كيفية وقوع الجريمة والأدلة المرتبطة بها. ويحتاج المحقق في هذا المجال إلى مهارات تقنية عالية لفهم البرمجيات والملفات المعقدة واستخدام أدوات متطورة لتحليل البيانات. كما أن تنوع أساليب الجرائم الإلكترونية يفرض على المحققين اتباع طرق متعددة ومتكاملة للكشف عنها، حسب الحالة ونوع الجريمة، وتم تقسيم هذا المبحث الى مطلبين **(المطلب الأول)** مفهوم التحقيق الجنائي الإلكتروني، و**(المطلب الثاني)** في وسائل وأساليب التحقيق في جريمة القرصنة الإلكترونية.

المطلب الأول: مفهوم التحقيق الجنائي الإلكتروني

التحقيق الجنائي في الجرائم الالكترونية عبارة عن فحص جهاز الجاني او المشتبه به من قبل المحققين فمثلا إذا تمت جريمة عن طريق الحاسوب او الأجهزة الذكية المختلفة، يأتي المحقق المتخصص ليفحص ما به وذلك باستخدام أدوات خاصة ودراسات سابقة وكل ما هو ممكن والهدف منها جمع الأدلة المطلوبة، وقد قسم هذا المطلب الى فرعين: **(الفرع الأول)** المتمثل في تعريف التحقيق الجنائي في جريمة القرصنة الالكترونية وخصائصه، و **(الفرع الثاني)** المتمثل في الاختصاص القضائي.

الفرع الأول: تعريف التحقيق الجنائي في جريمة القرصنة الالكترونية وخصائصه

تعتبر مرحلة جمع الاستدلالات مرحلة تمهيدية لكشف الغموض، ومرحلة التحقيق الابتدائي مرحلة ثانية التي تلي مرحلة جمع الاستدلالات وهي مرحلة سابقة للمحاكمة، وسنبين في هذا الفرع مراحل التحقيق والخصائص المتعلقة بكلا من التحقيق والمحقق.

أولا: تعريف التحقيق الجنائي

يُعدّ التحقيق إجراءً أساسياً يُباشر بعد وقوع الجريمة، نظراً لأهميته في التحقق من صحة وقوعه وتحديد المسؤول عنها من خلال جمع الأدلة المادية بمختلف أنواعها لإثبات الواقعة وإسنادها إلى مرتكبها.

يعرف بأنها استخدام الطرق المثبتة علميا، لحفظ، جمع، عرض، تحديد، تحليل، ترجمة، توثيق والتحقيق من صحة الأدلة الرقمية المستخرجة من المصادر الرقمية، بهدف تسهيل او تعزيز بناء الأحداث الجنائية، او المساعدة في احباط العمليات غير الشرعية المرتقبة.

عموما يعتبر التحقيق من اهم الإجراءات التي تتخذ بعد وقوع الجريمة، لماله من أهمية في التثبيت من حقيقة وقوعها، وإقامة الاسناد المادي على مرتكبها بأدلة الاثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول الى ادانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة والثابت ان الدعوى الجزائية تمر على ثلاث مراحل أساسية وهي مرحلة الاستدلالات ومرحلة التحقيق والمرحلة النهائية وهي المحاكمة[1].

–مرحلة جمع الاستدلال : وهي مرحلة البحث التمهيدي وهي مرحلة هامة لبناء الدعوى الجنائية لأنها هي المرحلة التي تسبقها ويطلق هذا المصطلح على الإجراءات التي ينفذها أعضاء الضبط القضائي عند ارتكاب

[1] بوحزمة نصيرة، **التحقيق الجنائي في الجرائم الالكترونية (دراسة مقارنة)**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس،2022، ص 92، 93.

جريمة معينة وذلك تمهيدا لوضع تم التوصل اليه بين يدي الجهة المختصة وهي النيابة العامة لتقرير ما تراه مناسبا بشأنها.

-مرحلة التحقيق الابتدائي: وتعتبر أولى مراحل الخصومة، وهي المرحلة التي وان كانت تسبق المحاكمة، فهي المرحلة التي تمهد لها أي لمرحلة الفصل في الدعوى الجنائية، وقد وصف التحقيق في هذه المرحلة بانه ابتدائي، لان غايته ليست كامنة فيه، وانما سيهدف التمهيد لمرحلة المحاكمة، وليس من شانه الفصل في الدعوى لا بالإدانة ولا حتى بالبراءة، وانما مجرد استجماع العناصر التي تتيح لسلطة أخرى ذلك، وهي مرحلة هامة في سبيل التحري عن الجرائم فالبعض يعرفها بانها مرحلة قضائية تتمثل في قيام المحقق بالتحقيق في القضايا الهامة التي أقيمت بها الدعوى وهو مرحلة وسطى تلي المرحلة الأولى وتسبق مرحلة التحقيق النهائي او المحاكمة[1].

ثانيا: خصائص التحقيق

تميز التحقيق في الجريمة الإلكترونية بمجموعة من الخصائص، من أبرزها:

1- السرية

تُعد السرية من المبادئ الأساسية التي تحكم سير التحقيق، حيث يُمنع إطلاع غير المخولين على مجريات التحقيق، وذلك لضمان سلامة الإجراءات وعدم التأثير على الأدلة أو الشهود. وقد كرس المشرع هذا المبدأ في المادة 11 من قانون الإجراءات الجزائية.

2- التدوين:

تُدوَّن كافة إجراءات التحقيق في محاضر رسمية، ويتم التصديق عليها وفق الأطر القانونية المعتمدة، لتُشكّل دليلاً معتبراً في الإثبات أمام الجهات القضائية، وتُعتبر هذه المحاضر وثائق ذات حجية قانونية مهمة.

3- وضع خطة للتحقيق:

يتطلب التحقيق في الجرائم الإلكترونية إعداد خطة منهجية دقيقة تبدأ بجمع الاستدلالات وتحليل الأدلة. وبما أن هذه الجرائم تتسم بطابع تقني معقد، فإن المحقق يعاونه فريق فني متخصص، يملك الكفاءة اللازمة للتعامل مع الأدلة الرقمية وتحليلها وفق الأطر القانونية والتقنية[2].

---

[1] بوحزمة نصيرة، مرجع سابق، ص 94، 95.

[2] فلاح عبد القادر، ايت عبد المالك نادية، **التحقيق الجنائي للجرائم الإلكترونية واثباتها في التشريع الجزائري**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، المجلد04، العدد02، جانفي 2020، ص 7.

الفرع الثاني: تعريف المحقق الجنائي وخصائصه

وكما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والانترنت وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات سنعرض تعريف المحقق الجنائي وخصائصه:

أولا: تعريف المحقق الجنائي

ذهب جانب من الفقه الى تعريف المحقق انه:" كل من عهد اليه القانون لتحري الحقيقة في البلاغات والحوادث الجنائية، والتحقيق فيها ويساهم بدوره في كشف غموضها وصولا الى معرفة حقيقة الحادث وكشف مرتكبه.

كما عرف البعض المحقق او الباحث الجنائي بانه المكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها او اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها"[1].

ثانيا: خصائص المحقق الجنائي

يتطلب المحقق الجنائي في الجرائم المعلوماتية تقريبا ذات الصفات الواجب توافرها في أي محقق جنائي وهي كالتالي:

1- أن يكون هدفه هو الوصول إلى الحقيقة ولديه موهبة فن التحقيق ذلك أن المحق ق يكون مؤمنا، يكون لديه اعتقادً برسالته في استظهار الحقيقة، واتخاذ كل الوسائل الكاشفة عنها أن الوصول إلى الحقيقة وتحقيق العدالة هما هدفه وغايته المنشودة.

فينبغي عليه أن يكون مؤمنا بأنه يؤدي رسالة إنسانية مؤتمن عليها أمام الله وأمام المجتمع، فلا تؤثر فيه أي روايات يستمع إليها خارج إطار التحقيق الذي يجريه، ولا تؤثر فيه أيضا كتابات يطلع عليها في الصحف، وإنما يجب عليه أن يجرد نفسه من كل تأثير يقع عليه من جراء الحادث الذي يقوم عليه تحقيقه فيباشر إجراءاته على أساس أنه خالي الدهن ومجرد من أي علم سابق على أول إجراء يبدأ به.

2- أن يكون سريع التصرف بمعنى أنه يقع على عاتقه تسير إجراءات التحقيق بالسرعة الواجبة لإنجازه دفعة واحدة، أوفي جلسات قريبة متلاحقة، وعدم التباطؤ في جمع الأدلة، كذلك يجب أن تكون لديه قوة

[1] بن عنطر سيهام، **التحقيقي الجنائي في الجرائم الالكترونية**، مذكرة ماستر، كلية الحقوق والعلوم السياسية جامعة مولود معمري، تيزي وزو، 2023، ص 23.

الملاحظة وسرعة البديهة، وهي تعني القدرة على حفظ المعلومات والمشاهدات التي تقع تحت أحد حواسه واستدعائها عند الحاجة وه ام ي يمكنه من ربط الحوادث بعضها مع بعض الآخر.

3- أن يكون محايد أثناء التحقيق وملتزم الهدوء وضبط النفس، وذلك يعني عدم تحيزه وتحري الحق أينما كان سواء أدى إلى إقامة الدليل قبل المتهم أو إلى نفي التهام عنه.

وينبغي عليه أيضا أن يعامل جميع أطراف القضية على قدم مساواة فلا تفرقة بينهم بسبب الجنس أو الطبقة أو الثروة أو بسبب وظيفتهم الاجتماعية أو الاقتصادية أو المهنية في المجتمع.

4- كما يجب أن يلتزم المحقق بضبط النفس، ولا يستسلم للغضب أو لسيطرة الميول والغرائز، وأن يتحلى بالصبر والمثابرة في الكشف عما يدق أو يغمض من أمور التحقيق، وأن يتأتى في الحكم على قيمة الدليل، مقلبا قته لمقتضىً الرأي على مختلف وجوهه حتى يتيقن من مطاب الحال دون التزام بالتأثير الأول الذي يتبادل إلى ذهنه عن الحادث.

5- عدم التأثر باتجاهات الرأي العام، إذ يجب على المحقق أن يبتعد عن أي مؤثرات من شأنها التأثير على سير العدالة، فتأثر المحقق قد يجعله قاسيا عنيف أو متعاطفا ودود، فلابد ألا يتأثر مثلا بإعجاب المحيطين به لأن الغرور من الصفات القاتلة التي من شأنها أن تؤخر ولا تقدم في التحقيق، كما يلتزم بحفظ أسرار التحقيق[1].

6- العلم التام بالقوانين الجنائية حيث، يجب أن المحقق يكون على علم تام بأحكام القانون الجنائي، وبعلم الإجرام وبعلم العقاب، وأن يكون على دراسة بمبادئ الطب الشرعي وعلم النفس الجنائي، وأن يكون ملما العامة التيً بمختلف الظروف المحيطة بالمجتمع وبالمعلومات تتصل بالوقائع التي يتولى تحقيقها، كما يجب أن يكون على جانب كبير من الثقافة العامة متنوع الاطلاع والمعارف التي تتصل بالحياة البشرية على مختلف صورها وطبائعها.

ان المهارات التي سبق الإشارة إليها تُعد ضرورية لكل محقق جنائي، إلا أن المحقق في الجرائم المعلوماتية يحتاج، بالإضافة إلى ذلك، إلى امتلاك مهارات إضافية تُمكّنه من التعامل بفعالية مع هذا النوع من الجرائم، ويستوجب عليه الإلمام بمجالات معرفية أخرى، وعلى رأسها علم الحاسوب والأدلة الرقمية[2].

[1] رابحي عزيزة، مرجع سابق، ص 258، 259.

[2] مرجع نفسه، ص259.

الفرع الثالث: الاختصاص القضائي

الاختصاص مباشرة سلطة المتابعة والتحقيق والحكم في الجريمة وفقا للقواعد التي رسمها القانون والحدود التي تبنها المشرع لهذه السلطات اثناء ممارسة مهامهم سنتطرق أولا الى القاعدة العامة في الاختصاص وثانيا الى تمديد الاختصاص.

أولا: القاعدة العامة في الاختصاص

حدد المشرع الجزائري معايير الاختصاص المحلي في قانون الإجراءات الجزائية في المواد 37، 40، 329.

1-الاختصاص المحلي لوكيل الجمهورية

بالنسبة لوكيل الجمهورية تنص المادة 37 فقرة أولى من قانون الإجراءات الجزائية على أن الاختصاص المحلي لها يتحدد بمكان وقوع الجريمة أو بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرتها القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر.

2-الاختصاص المحلي لقاضي التحقيق

وأما بالنسبة لقاضي التحقيق تنص المادة 40 الفقرة الأولى على أن اختصاصها المحلي يتحدد بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.

وعن ضباط الشرطة القضائية طبقا للمادة 1/16 من قانون الإجراءات الجزائية فانهم يمارسون اختصاصهم المحلي في حدود الدائرة التي يباشرون فيها وظائفهم المعتادة، وفي حالات الاستعجال لهم مباشرة مهامهم في كافة اختصاص المجلس القضائي الملحقين به أو كافة الإقليم الوطني بناءا على أمر من القاضي المختص وبعد إطلاع وكيل الجمهورية التابعين لها[1].

3-الاختصاص المحلي لجهات الحكم

يُحدد الاختصاص المحلي في قضايا الجنح وفقًا للمادة 329 من قانون الإجراءات الجزائية، بناءً على:

مكان ارتكاب الجريمة، محل إقامة أحد المتهمين أو شركائهم ومكان توقيف المتهمين ويُراعى أن الاختصاص يظل قائمًا حتى إن تم القبض على المتهم لأسباب أخرى، وفي مكان مختلف.

[1] جدي نسيمة، مرجع سابق، ص84.

في حالة كون المحكوم عليه موقوفا ينعقد الاختصاص لمحكمة مكان الحبس، ويرجع الاختصاص للمحكمة التي ارتكبت في نطاق دائرتها المخالفة أو المحكمة الموجودة في بلد إقامة مرتكب المخالفة بالنظر في تلك المخالفة.

ونوعيا بالنسبة للأحداث فإن قسم الأحداث المختص إقليميا هو المحكمة التي ارتكبت الجريمة بدائرة اختصاصها أو بها محل إقامة الحدث أو ووالديه أو وصيه، أو محكمة المكان الذي عثر فيه على الحدث أو المكان الذي أودع به الحدث سواء بصفة مؤقتة أو نهائية طبقا لأحكام المادة 451 من قانون الإجراءات الجزائية في فقرتها الثالثة.

وعن معايير تحديد مكان الاختصاص تختلف حسب نوع الجريمة الجريمة المستمرة: المحكمة التي وقع فيها الفعل، الجريمة المتتابعة المحكمة التي وقع فيها اخر فعل، الجريمة ذات النتيجة المحكمة التي تحققت فيها النتيجة الجرمية.

وفي جريمة القرصنة قد تتحقق النتيجة في أكثر من مكان نتيجة انتشار الفيروس او البيانات الضارة الكترونيا، لذا يمكن متابعة المتهم امام أكثر من محكمة، مع إعطاء الأولوية للمحكمة التي تحققت فيها النتيجة وباشرت الإجراءات أولا.

أما عن محل إقامة المتهم فالعبرة بالمحل الذي كان يقيم فيه المتهم وقت اتخاذ إجراءات المتابعة بغض النظر عن التغيرات التي تحدث به ومثال التعاون الدولي البناء في مجال الاختصاص ما أقدمت عليه دول الإتحاد الأوروبي من اعتبارها دولة واحدة وإقليم واحد لحل مشكلة المحكمة المختصة بنظر الدعاوى الجنائية الناتجة عن كافة الجرائم المعلوماتية[1].

ثانيا: تمديد الاختصاص

بعد صدور المرسوم التنفيذي رقم 348/06 المؤرخ 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وجهات التحقيق، وتم استحداث ما يعرف بالأقطاب الجزائية المتخصصة لمحاكم (قسنطينة، ورقلة، وهران، سيدي أمحمد) المتخصصة للفصل في نوع خاص من الجرائم المحددة على سبيل الحصر منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي حددت المواد من 2 إلى 5 مجال تمديد الاختصاص فيها على النحو التالي:

-محكمة سيدي محمد: يمتد فيها الاختصاص المحلي إلى محاكم المجالس القضائية للجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة المدية، المسيلة، بومرداس، تيبازة وعين الدفلى.

[1] جدي نسيمة، مرجع سابق، ص85.

– محكمة قسنطينة: يمتد فيها الاختصاص المحلي إلى محاكم مجالس قسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس والمسيلة.

– محكمة وهران: يمتد فيها الاختصاص المحلي الى محاكم المجالس القضائية لوهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تيموشنت، غيليزان[1]. وجاء هذا المرسوم تبعا لتعديل قانون العقوبات بموجب القانون 14/04[2] المؤرخ 10نوفمبر2004 الذي نص في المادة 37 فقرة 2 و40 فقرة 2 و329 فقرة أخيرة على جواز تمديد الاختصاص المحلي لوكيل الجمهورية أو قاضي التحقيق أو المحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات [3].

المطلب الثاني: وسائل وأساليب التحقيق الجنائي في جريمة القرصنة الالكترونية:

ان التحقيق في الجرائم الالكترونية يمتاز بخصوصية تجعله يفترق عن التحقيق في الجرائم التقليدية، نظرا لتميز هذه الجرائم عن غيرها من الجرائم التقليدية الأخرى خاصة فيما يتعلق بطبيعة مسرح الجريمة، الامر الذي يقتضي ضرورة تطوير وسائل وأساليب التحقيق الجنائي بصورة تجعله يتلاءم مع هذا التميز، بحيث تمكن سلطة التحقيق من كشف غموض هذه الجرائم وتحديد شخص المتهم واثبات التهمة عليه.

وسنقوم بتقسيم هذا المطلب الى فرعين الوسائل المستخدمة في التحري وجمع الأدلة، الوسائل المادية والاجرائية في **(الفرع الأول)**، وأساليب التحقيق الجنائي التقليدية والحديثة في **(الفرع الثاني)**:

الفرع الأول: الوسائل المستخدمة في التحري وجمع الأدلة

عند القيام بالتحقيق في جريمة ما، فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني، وحيث أن للجرائم المعلوماتية طابعها الخاص المميز لها، فإن التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة وبالتالي حل لغزها والوصول إلى الجاني، وفي سبيل ذلك يعتمد المحقق على مجموعة من الوسائل المختلفة.

[1] جدي نسيمة، مرجع سابق، ص86، 87.

[2] القانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، المتضمن ق ع، ج.ر، عدد 71، الصادرة في 14 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156، المؤرخ في 08 جوان 1966.

[3] بوحزمة نصيرة، مرجع سابق، ص 88.

أولا: الوسائل المادية

وهي الادوات الفنية التي غالبا ما تستخدم في بنيه نظم المعلومات والتي يمكن باستخدامها تنفيذ اجراءات واساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصيه مرتكبها ومن اهمها:

1- عناوين ((IP، والبريد الإلكتروني، وبرامج المحادثة.

2- البروكسي ((proxy

حيث يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبك، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة .**(casheMermory)**

3- برامج التتبع

حيث تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان **(IP)**الذي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الأنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الأنترنت ومعلومات أخرى، ومن الأمثلة على هذه البرامج برنامج .**(Hack Tracer)**

4- نظام كشف الاختراق (Instrusion Détection System)

ويرمز له اختصارا بالأحرف(**IDS)**وهذه الفئة من البرنامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الإلكترونية أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسبة الإلكترونية أو الشبكة، ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الإلكترونية أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشاف النظام وجود احد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة، والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها[1].

[1] عثماني عز الدين، **إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية**، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد04، جانفي 2018، ص 54.

5-أدوات تدقيق ومراجعة العمليات الحاسوبية

وهي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجرى على ملفات ونظام تشغيل حاسوب معين وتسجيلها في ملفات خاصة يطلق عليها(**Logs**)والكثير من هذه الأدوات تأتي مضمنة في أنظمة التشغيل بعد اعدادها للعمل[1]

6-أدوات فحص ومراقبة الشبكات

هذه الأدوات تستخدم في فحص بروتوكول ما وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أدوات **(ARP)**وظيفتها تحديد مكان الحاسبة الإلكترونية فيزيائيا على الشبكة[2].

7-أدوات الضبط

تحتاج جهات التحقيق وجمع الاستدلالات الى ضبط الجريمة واثبات وقوعها والمحافظة على الأدلة حتى نسبها الى الجاني، لتقديمها الى النيابة العامة لكسب اعترافه، وأدوات الضبط تعتبر من الوسائل المادية التي تساعد في ضبط جريمة القرصنة منها على سبيل المثال برامج الحماية وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وبرامج التصنت على الشبكة، والتقارير التي تنتجها نظم امن البيانات، ومراجعة قاعدة البيانات.

8-الوسائل المساعدة للتحقيق

من هذه الوسائل المستخدمة في استرجاع المعلومات من الأقراص التالفة وبرامج كسر كلمات المرور، وبرامج الضغط وفك الضغط وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسبة، وبرامج نسخ البيانات، وأيضا من الأدوات المهمة والتي تساعد في عملية التحقيق برامج منع الكتابة على القرص الصلب وذلك لعد ارتكاب الجريمة، مما ساعد في المحافظة على مسرح الجريمة[3].

ثانيا: الوسائل الإجرائية

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة والغير محددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها.

[1] بوحزمة نصيرة، مرجع سابق، ص 144.

[2] عثماني عز الدين، مرجع سابق، ص 55.

[3] بوحزمة نصيرة، مرجع سابق، ص145.

1- اقتفاء الأثر

يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله، او عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق[1].

2- الاطلاع على عمليات النظام ألمعلوماتي وأسلوب حمايته

ينبغي على المحقق الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما ينبغي عليه الاطلاع على عملية النظام والمستفيدين والملفات والإجراءات وتضيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى توزيع الصلاحيات للمستفيدين، وإجراءات امن العاملين[2].

3- الاستعانة بالذكاء الاصطناعي

من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الإلكترونية، وفق برامج صممت خصيصا لهذا الغرض.

4- مراقبة الاتصالات الإلكترونية

لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الاتصالات الإلكترونية، على عكس بعض التشريعات التي عرفتها مثل التشريع الأمريكي والكندي[3].

الفرع الثاني: أساليب التحقيق

هناك بعض إجراءات التحقيق التي تعد منبع للأدلة وهي الانتقال والمعاينة، نذب الخبراء، سماع الشهود والتفتيش وليس لها أي ترتيب يجب اتباعه بل يبدأ المحقق بما يراه ملائما لظروف كل جريمة، إضافة الى بعض الإجراءات المستحدثة لجمع الأدلة والتحقيق في الجريمة الإلكترونية، سنتطرق الى الأساليب التقليدية أولا ثم الأساليب الحديثة ثانيا.

أولا: الأساليب التقليدية

1- الخبرة

تكتسي عملية ندب الخبير خلال التحقيق في جرائم المعلوماتية اهمية بالغة، وذلك للطبيعة الفنية والتقنية الدقيقة التي تتميز به ادوات ارتكاب الجريمة المعلوماتية وكذلك لتنوع الأجهزة في هذا المجال وسرعة تطورها، وندب الخبير من سلطات المحقق وليس هناك في القانون ما يلزم المحقق بذلك، ويحدد المحقق

[1] عثماني عزدين، مرجع سابق، ص55.

[2] بوحزمة نصيرة، مرجع سابق، ص148.

[3] عثماني عز الدين، مرجع سابق، ص55.

للخبير المهمة التي كلف بها وميعاد تسليمه لتقريره، كما يجب عليه ان يؤدي اليمين القانونية بهذا الخصوص.

والمستندات المتحصل عليها من خلال عملية التفتيش لا يحتاج المحقق فيها للمساعدة من قبل الخبراء وهذه المستندات تتمثل في: سجلات ادارة الكومبيوتر، وثائق البرامج، السجلات، البيانات المطبوعة، ويتم التخطيط على هذه المستندات ويمكن تحديد ما إذا كانت كاملة، اصلية، او صورا من خلال استجواب القائمين على حفظها.

اما الأدلة الأخرى فيمن فحصها أكثر تعقيدا مثل:

الأشرطة الممغنطة الأسطوانات، البرامج وتتطلب استعانة المحقق بأحد الخبراء حتى يتمكن من الإلمام بمحتوياتها.

واهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:

– تركيب الحاسب الآلي وصناعته ونوعه ونوع نظام تشغيله وأهم الأنظمة الفرعية التي يستخدمها بالإضافة الى الأجهزة الطرفية الملحقة به وكلمات المرور او السر ونظام التشفير.

– طبيعة بيئة الحاسب او الشبكة من حيث تنظيم ومدى تركيز او توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة قرصنتها.

– الموضع المحتمل لأدلة الاثبات والشكل او الهيئة التي تكون عليها[1].

2-الانتقال ومعاينة مسرح الجريمة المعلوماتية

يقصد بالانتقال ذهاب مأموري الضبط القضائي أو المحقق الجنائي إلى المكان الذي ارتكبت فيه الجريمة، حيث توجد آثارها وأدلتها.

أما المعاينة يقصد بها فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء تحقيق لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من مزق أو ثقوب والمعاينة بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو إلى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة غير أن المحقق قد ينتقل لغرض آخر غير المعاينة كالتفتيش مثلا، وفي الجريمة المعلوماتية يقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت ، وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكومبيوتر و الشبكة العالمية.

[1] معتوق عبد اللطيف، مرجع سابق، ص114.

والمعاينة جوازيه للمحقق، شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أولم يطلبوها. ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية، ومرد ذلك الاعتبارين:

❖ الجرائم التي تقع على نظم المعلومات والشبكات فلما يترتب على ارتكابها آثار مادية.

❖ أن عدد كبيرا من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها مما يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

– تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته ويراعي تسجيل وقت وتاريخ ومكان التقاط كل صورة.

– العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقة الولوج إلى النظام أو الموقع أو الدخول معه في حوار.

– ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن أجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.

– عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

– التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة وغير السليمة أو المحطمة وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

– التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات[1].

3–ضبط الادلة في الجريمة المعلوماتية

إلى الغرض من القيام بعملية التفتيش هو ضبط الأشياء التي يحتمل أنها استعملت في ارتكاب الجريمة، و هو من أعمال الضبطية القضائية حسب نص المادة 12 من قانون الإجراءات الجزائية الجزائري،

[1] رابحي عزيزة، مرجع سابق، ص 275.

و على ضابط الشرطة القضائية ان يحرر محضرا بالأشياء المضبوطة و يرسله إلى وكيل جمهورية، و إذا كانت الجريمة متلبس بها 5ان ضابط الشرطة القضائية ملزم بالمحافظة على أثار الجريمة التي يخشى أن تختفي، و يقوم بوضعها في كيس و يختم عليه بختمه، كما يقوم بعرض الأشياء المضبوطة على الأشخاص المشتبه فيهم للتعرف عليها، مثلما نصت على ذلك المواد 42، 45 و المادة 47 مكرر من قانون الإجراءات الجزائية الجزائري.

وقد يكون الدليل المادي عبارة عن مستند أو محرر مكتوب أو مطبوع أو منسوخ أو نصور أو مسجل بحيث يكون مناسبا لإثبات الواقعة.

وكانت عملية ضبط الأدلة في الجريمة المعلوماتية تثير إشكالات فيما يخص البيانات والمعلومات المجردة من الطابع المادي لها كالدعامة أو الوسيط الحامل لها، وسبق أن تطرقنا لوجهات نظر الفقهاء بهذا الخصوص عن حديثنا عن عملية تفتيش المنظومة المعلوماتية.

فبعض الفقهاء رأوا عدم صلاحية البيانات والمعلومات لأن تكون أدلة مادية يمكن ضبطها مجردة من دعامتها المادية، إلا أن اتجاه آخر رأى أن البيانات والمعلومات رغم كونها مجردة من الدعامة المادية فانه لا يوجد ما يمنع من صلاحيتها لان تكون محلا للضبط.

وللتوفيق بين وجهتي النظر السابقتين ظهر اتجاه ثالث رأى بعدم جدوى تطويع النصوص التقليدية وتطبيقها على البيانات والمعلومات المخزنة اليا واقترح تدخل المشرع نطاق الأشياء الممكن ضبطها نع ضرورة إعداد ضباط الشرطة القضائية وتكوينهم في كيفية للتعامل مع أدلة من هذا النوع[1].

4-سماع الشهود

لشهادة كدليل في الدعوى الجزائية لها أهميتها البالغة، إذ تكمن من كشف العمل غير المشروع الذي يجتهد المجرم المعلومات في إخفائه، فسماع الشهود من الأمور المألوفة في الجرائم التقليدية، إذ يمكن لرجال الضبطية القضائية سماع أقوال الأشخاص الحاضرين وقت ارتكاب الجريمة، حيث أن المشتبه فيه أو من تواجد في مكان ارتكاب الجريمة يكون مدفوعا إلى الإدلاء بأقواله أمام ضابط الشرطة القضائية لما لهذا الأخير من سلطه تخول له احتجاز الأشخاص الذين يرى فيهم ضرورة التحقيق معهم.

وقد أجاز المشرع الجزائري لضابط الشرطة القضائية منع اي شخص من اباحة مكان الجريمة ريثما من تحرياته حسب نص المادة 50 من قانون الإجراءات الجزائية الجزائري.

[1] معتوق عبد اللطيف، مرجع سابق، ص112.

ويختلف مفهوم الشاهد في الجريمة المعلوماتية عنه في الجرائم التقليدية، للاعتبارات التقنية المميزة للجريمة المعلوماتية، الخبرة والتخصص في تقنيه الحاسب الآلي بحيث تكون لديه معلومات أساسية عن الدخول الى الحاسب المراد البحث فيه عن أدلة للجريمة، ولهذا يطلق عليه مصطلح الشاهد المعلوماتي[1].

5-التفتيش

التفتيش من إجراءات التحقيق التي تنطوي على مساس بحرية الأشخاص وحرمة ممتلكاتهم ومساكنهم الهدف منها البحث عن الأدلة متى وجدت قرائن على حيازة الخاضع لهذا الإجراء.

وأول فكرة تتبادر للذهن المجرم بعد ارتكاب الجريمة هو طمس معالمها وإزالة كل أثر قد يكشف عن شخصيته، وقد يتطلب ذلك تفكيرا ووقتا، والتفتيش هو الوسيلة لإثبات الأدلة المادية.

ويقصد بالتفتيش بمدلوله القانوني بالنسبة لهذه الجرائم إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للمعطيات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة مرتكبة تشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم[2].

و قد اجاز القانون الجزائري لضابط الشرطة القضائية تفتيش مساكن المشتبه فيهم بشروط تحت طائلة البطلان، نصت عليها المادة 44 من قانون الإجراءات الجزائية الجزائري، تتمثل في الحصول على اذن من وكيل الجمهورية او قاضي التحقيق مع استظهار هذا الاذن قبل الشروع في عملية التفتيش ولا يختلف الأمر بالنسبة لتفتيش في احد الجرائم التي نصت عليها المادة 37 من نفس القانون و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و قد اعفى المشرع الضابط القائم بعملية التفتيش من ضرورة حضوره مع صاحب المسكن او ممثل له و هذا اذا تعلق الامر بجريمة المساس بأنظمة المعالجة الآلية للمعطيات حسب ما ورد في نص المادة 45 من قانون الاجراءات الجزائري.

اما عن ميقات التفتيش فقد اعطى المشرع الجزائري، وفق المادة 47 من نفس القانون، كامل الصلاحية لضابط الشرطة القضائية في اجراء التفتيش والمعاينة والحجز في كل محل سكني او غير سكني وفي كل ساعة من ساعات الليل او النهار وذلك بناءا على اذن مسبق من وكيل الجمهورية، وذلك عندما يتعلق الأمر بجريمة المساس بأنظمة المعالجة الآلية للمعطيات.

[1] معتوق عبد اللطيف، مرجع سابق، ص115.

[2] جدي نسيمة، مرجع سابق، ص 93، 94.

والتفتيش في مجال الجريمة المعلوماتية يخضع لمعيار مدى قابلية مكونات الحاسب الآلي المادية **(hard wear)** ومكوناته غير المادية او المنطقية **(soft wear)**، بالإضافة الى شبكات الاتصالات التي يكون مرتبطا بها في غالب الأحيان الى التفتيش[1].

ويتم تفتيش المكونات المادية للكمبيوتر بحثا عن كل ما يتصل بالجريمة ويفيد وقوعها للكشف عنها وعن مرتكبيها، وهنا جواز تفتيش هذه المكونات يتوقف على طبيعة المكان الموجودة فيها، ما إذا كان مسكن المتهم أو الغير وفي أي ساعة وبصفة عامة تخضع إجراءات التفتيش هنا لذات الضمانات المنصوص عليها في قانون الإجراءات الجزائية التي سنأتي على ذكرها.

أما عن تفتيش المكونات المعنوية فهو مسألة تثير عدة إشكالات تتعلق بمحل التفتيش الذي يقع على معنويات وليس ماديات، وكأصل يهدف التفتيش للحصول على دليل مادي والمشرع الجزائري أجاز التفتيش عن أي شيء ولم يحدد الطبيعة المادية كشرط، وعليه يطبق التفتيش على هذا النوع من المكونات المعنوية من برامج ومعطيات مخزنة لعدم وجود قيد على ذلك، إضافة لوسائط الحفظ والتخزين والوحدات المركزية وكل ما يتعلق بالحاسب الآلي.

ولتفتيش البيانات المخزنة آليا يتطلب ذلك عون مؤهل للتعامل بالبرامج وحفظ الملفات وفك الشيفرات وكلمات المرور للتمكن من الحصول على الأدلة وحفضها.

وبهذا المفهوم فالتفتيش فيما يتعلق بهذه الجرائم ليس له مسرح جريمة محدد إذ يمكن التفتيش على ذات الشبكة من غير الحاسوب المستعمل في ارتكاب الجريمة، إذ يمكن للجاني أن يستعمل حاسوب من أي مقهى أنترنيت بنظام معين وعليه يمكن البحث عن آثار استخدام نظام معين من أي حاسوب آخر متصل بذات الشبكة[2].

وتتمثل شروط اجراء عملية التفتيش فيما يلي:

من أجل مكافحة الجريمة الإلكترونية، أُجيز للعديد من الجهات المختصة التفتيش عن هذه الجرائم، والوصول إلى الدليل الإلكتروني بوسائل تقنية محددة. وقد أقرّ التشريع الجزائري مجموعة من القواعد التي تُبيّن مشروعية هذا التفتيش، خاصة إذا كان الغرض منه الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، أو التحقيق فيها.

[1] معتوق عبد اللطيف، مرجع سابق، ص 110،

[2] جدي نسيمة، مرجع سابق، ص 95.

ومن بين الشروط التي نصّ عليها القانون (المادة 03 والمادة 05) ما يلي: أن تكون هناك معلومات مؤكدة تفيد بوجود تهديدات تمسّ الأمن العام، أو الدفاع الوطني، أو تمثل خطرًا على مؤسسات الدولة أو الاقتصاد الوطني، أو تتعلق بجرائم خطيرة. وفي هذه الحالات، يُسمح للسلطات القضائية المختصة بالدخول إلى الأنظمة المعلوماتية، وضبط البيانات المخزّنة بداخلها، أو نسخها، أو نقلها وفقًا لما تقتضيه الضرورة القانونية.

و المادة 44 من ق.إ.ج.ج تضمنت مجموعة من هذه الضمانات اذ لا يمكن القيام بعملية تفتيش مساكن الأشخاص الذين يظهر انهم ساهموا في جناية او جنحة متلبس بها او التحقيق في الجرائم الإلكترونية او تفتيش مساكن اشخاص يتبين انهم يحوزون أوراق او أشياء لها علاقة بالأفعال الجرمية المرتكبة إلا بإذن مكتوب صادر من وكيل الجمهورية او من قاضي التحقيق، مع التأكيد على ضرورة اظهار ذلك الإذن قبل الدخول و الشروع في التفتيش، كما اكدت فقرات تلك المادة على ان يتضمن الإذن وصفا للجرم المرتكب و كذا عنوان الأماكن التي سيتم زيارتها و التفتيش فيها، و كل ذلك تحت طائلة البطلان[1].

ثانيا: الإجراءات الحديثة

لقد عزز المشرع الجزائري اختصاصات الضبطية القضائية، وذلك بموجب التعديل الأخير لقانون الإجراءات الجزائية تحت رقم 06-22[2]، بوضع أساليب وآليات جديدة للتحري والتحقيق في بعض الجرائم الواردة على سبيل الحصر، نظرا لما تحويه من خطورة على المجتمع وسنتطرق إليهم كما يلي: التسرب، اعتراض المراسلات والتقاط الصور، ثم المراقبة والتتبع[3]:

1-التسرب

على ضوء التغيرات والتطورات التي طالت الجريمة حيث تولدت لدينا الجريمة المستحدثة المسماة الجريمة المعلوماتية أو ما سماها المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تتضمن في طياتها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يسعى المشرع لوضع سياسة جزائية فعالة للحد من انتشار هذا النوع من الجرائم ومن بين آليات مواجهتها ميدانيا أسلوب التسرب.

---

[1] شنتير خضرة، مرجع سابق، ص76، 77.

[2] القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 **المتضمن قانون الإجراءات الجزائية**، المعدل والمتمم للأمر 66-155، المنشور بالج.ر رقم 84.

[3] شرف الدين وردة، **مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري**، مجلة المفكر، جامعة محمد خيضر، بسكرة، العدد15، جوان 2017، ص5.

اعتمد المشرع الجزائري أسلوب التسرب في ميدان التحقيق بموجب القانون 22/06 المعدل لقانون الإجراءات الجزائية حيث خصص له الفصل الخامس من الباب الثاني تحت عنوان "في التسرب" فأصبح لوكيل الجمهورية ولقاضي التحقيق بعد إخطار وكيل الجمهورية صلاحية منح الإذن بإجراء عملية التسرب لأجل مراقبة الأشخاص لإيهامهم من قبل المتسرب بأنه فاعل معهم أو شريك، وذلك بموجب المواد من 65 مكرر 11 إلى المادة 65 مكرر 18 قانون 06-22[1] ونتناول أيضا من خلال هذه المواد مفهوم عملية التسرب وشروطها وإجراءاتها.[2]

1.1تعريف التسرب

للتسرب عدة مرادفات كالتوغل او الاختراق وهي تقنية يسمح بموجبها الدخول لوسط مغلق كجماعة إجرامية او شبكة تتاجر في مواد ممنوعة، مما يفيد اقحام عنصر اجنبي عن الجماعة المراد اختراقها، وهذا بالذات ما يطلق عليه الزرع، ليكون عينا عليها يرقب اعمالها ويرصد تصرفاتها، أي زرع احد الضباط او أعوان الضبطية القضائية ممن تتوفر فيهم بعض المواصفات الخاصة وسط مجموعة إجرامية، بقصد مراقبتها من الداخل، معرفة الإمكانيات المادية والبشرية والتنظيمية للمجموعة من أساليب عمل ووسائل اتصال وتنقل وغيرها، حتى تتمكن المصالح الأمنية من مكافحة اجرامهم وتقديمهم للعدالة واثبات التهم عليهم[3].

يعرفه البعض بأنه تقنية من تقنيات التحري والتحقيق الخاصة التي تسمح لضباط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية، ولتقديم المتسرب لنفسه على أنه فاعل أو شريك.

كذلك يعرف بأنه" أكثر وسائل التحري تعقيدا وخطورة، لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات وتصرفات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة، ولكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط، ويوهمهم بأنه فاعل وشريك لهم وذلك حتى يطلع على أسرارهم من الداخل، ويجمع ما يستطيع من أدلة إثبات، ويبلغ السلطات بذلك فتتمكن من ضبط المجرمين ووضع حد للجريمة".

[1] انظر القانون رقم 06-22، السابق الذكر.

[2] رابحي عزيزة، مرجع سابق، ص295، 296.

[3] بوحزمة نصيرة، مرجع سابق، ص293، 294.

وتعرفه المادة 65 مكرر12 قانون 06-22: بأنه" قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيمانهم أنه الفاعل أو شريك لهم أو خاف"[1].

والجرائم الإلكترونية والتي من بينها جريمة القرصنة الإلكترونية ورد ذكرها في المادة 65 مكرر 05 قانون 06-22[2] من ق إ ج حددت الجرائم المستحدثة التي يجوز فيها اللجوء إلى هذا الإجراء، ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية كاشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال، او كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم، ويعتبر التسرب آلية جديدة في البحث والتحري عن الجرائم البالغة الخطورة على أمن الضبطية القضائية، بحيث تتطلب جرأة وكفاءة ودقة في العمل يجب التحضير لها وتنظيمها بدقة تامة، تستهدف أوساطا معينة مدروسة بشكل مقنن، حيث يتم الوقوف أمام أدق التفاصيل والخصوصيات قبل مباشرة التسرب، لأن هاته العملية تتطلب المشاركة المباشرة في نشاط الجماعة الإجرامية، فيدخل ضابط الشرطة القضائية او العون المكلف في اتصال مع الأشخاص المشتبه فيهم، ويربط معهم علاقات محدودة من أجل المحافظة على السر المهني إلى غاية تحقيق الهدف النهائي من العملية، ويتم اللجوء لمثل هذا النوع من التدابير في مرحلة التحقيق عندما تقتضي الضرورة ذلك، وبعد عدم نجاعة الأساليب العادية وحتى الغير عادية في الحقيقة مما يستوجب معه اللجوء لهذا الأسلوب من التحقيق للكشف حقيقة الجريمة ومرتكبيها[3].

2.1شروط صحة التسرب :

وتتمثل هذه الشروط فيما يلي:

1.2.1الشروط الموضوعية

يشترط للقيام بعملية التسرب مراعاة مجموعة من الشروط الموضوعية من قبل السلطة المختصة بإجراء التسرب، خاصة وقت ومكان اجراء عملية التسرب، ونوع الجريمة.

[1] شرف الدين وردة، مرجع سابق، ص9.

[2] انظر القانون رقم 06-22، السابق الذكر.

[3] دحو نجاة، أولاد علي فاطمة، مرجع سابق، ص58، 59.

- السلطة المختصة بإجراء التسرب

يتم اللجوء الى التسرب إذا اقتضت ضرورات التحري او التحقيق ذلك، والجهة المختصة بإصدار او منح الاذن بالتسرب هو اما وكيل الجمهورية او قاضي التحقيق. ففي مرحلة التحري فان وكيل الجمهورية هو من يقوم بمتابعة والرقابة على تلك العملية أي هو من يأذن به وهو من يتولى متابعة سيره من خلال ماله من مكانة في إدارة نشاط ضباط واعوان الشرطة القضائية.

وبالتالي فان القانون خول له ان يأمر ويراقب لا ات يتسرب، ومن ثم فان لدينا من يراقب وهو وكيل الجمهورية ومن يقوم بدور المسؤول المباشر وهو ضابط الشرطة القضائية، ولا يمكن لوكيل الجمهورية القيام بالعملية بنفسه باعتباره من أعضاء النيابة العامة.

اما في مرحلة التحقيق، فان قاضي التحقيق، بعد اخطار وكيل الجمهورية هو الذي يأذن بالتسرب وهو من يقوم بمراقبته، حيث يقوم بمنح اذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، اذ يصعب تصور قاضي التحقيق متنكر في زي مجرم بحثا عن مرتكب الجريمة، فالبحث عن المجرم من مهام الشرطة القضائية، وضابط الشرطة القضائية هو من يتولى مهمة التنسيق في عملية التسرب[1].

-وقت ومكان اجراء عملية التسرب

باعتبار التسرب اجراء من إجراءات التحقيق، يجعل من المتسرب غير مقيد بحيز زمني يتحرك فيه، فضرورة التحقيق تبرر عملياته طول ساعات الليل والنهار، وله ان يدخل كل الأماكن التي يمكن ان يكشف فيها الحقيقة دون قيد او شرط، لأنه لا يتحرك بصفة ضابط الشرطة القضائية بل هوية مستعارة.

-نوع الجريمة

يجب ان يتم اجراء التسرب بمناسبة جرائم محددة على سبيل الحصر وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الالية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة تشريع الخاص بالصرف وجرائم الفساد، وهذه الجرائم بعضها من نوع الجنايات والبعض الاخر من نوع الجنح، وهذه الجرائم خطيرة واثارها وخيمة على المجتمع، فهي جرائم سريعة الانتشار وعابرة للحدود الوطنية، كما انها تسخر عددا كبيرا من المجرمين، وجرائمها قائمة على التخطيط واستخدام كل الوسائل لمحو اثار الجريمة وطمس معالمها، كما انها تدر أموالا طائلة على الضالعين فيها.

[1] بوحزمة نصيرة، مرجع سابق، ص395، 396.

2.2.1الشروط الشكلية

نظرا لما تتطلبه عملية التسرب من سرية وحيطة وحذر نتيجة خطورة العملية على حيازة المتسرب حرص المشرع على سير العملية واستوجب شروط شكلية وهي[1]:

-صدور اجراء التسرب بإذن قضائي

يجب ان يتم الاذن بعملية التسرب من طرف وكيل الجمهورية او من طرف قاضي التحقيق، بعد اخطار وكيل الجمهورية.

يجب ان يكون الاذن المسلم مكتوبا ومسببا وذلك تحت طائلة البطلان، مع ذكر الجريمة التي تبرر اللجوء الى هذا الاجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته[2].

-مدة تنفيذ عملية التسرب

يجب ان يحدد في الاذن مدة عملية التسرب، ويمكن تجديد هذه المدة إذا اقتضت ضرورات التحري والتحقيق ذلك مع اصدار اذن آخر وفق الشروط الزمنية نفسها التي صدر فيها الاذن الأول[3].

ثانيا: اعتراض المراسلات وتسجيل الأصوات والتقاط صور

جعل المشرع الجزائري من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور اهم الأساليب المستحدثة للكشف عن الجرائم الالكترونية، وهي إجراءات تباشر بشكل خفي، وذلك تماشيا مع التقدم العلمي والتكنولوجي المعاصر، لا سيما في مجال الاتصال والهندسة الالكترونية، مما افرز أساليب علمي عالية الكفاءة والفعالية أحدثت ثورة في مجال التحريات الجنائية. وقد نص المشرع في قانون الإجراءات الجزائية في المادة 56 دون تحديد مفهومه واجراءاته، غير ان المشرع استدرك الامر بموجب القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية حيث استحدث فصلا كاملا من المواد65 مكرر5 الى المادة 65 مكرر 10[4]، حيث نصت المادة 65 مكرر5 من قانون الإجراءات الجزائية على: اذا اقتضت ضرورات التحري في الجريمة المتلبس بها او في التحقيق الابتدائي في جرائم المخدرات او في الجرائم المنظمة العابر للحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الالية للمعطيات او جرائم تبييض الأموال او الإرهاب او الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص ان يأذن بما يأتي:

---

[1] بوحزمة نصيرة، مرجع سابق، ص 397.

[2] شرف الدين وردة، مرجع سابق، ص10.

[3] بوحزمة نصيرة، مرجع سابق، ص398.

[4] انظر القانون رقم 06-22، السابق الذكر.

1-اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

2-وضع الترتيبات التقنية، دون موافقة المعنيين، من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية من طرف شخص او عدة اشخاص يتواجدون في مكان خاص.

3-يسمح الاذن المسلم بغرض وضع الترتيبات التقنية بالدخول الى المحلات السكنية او غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم او رضا الأشخاص اللذين لهم حق على تلك الأماكن.

4-تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص.

في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناءا على اذن من قاضي التحقيق وتحت مراقبته المباشرة[1].

5-كما نجد ان المشرع الجزائري حدد المقصود بالمراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، كل تراسل او ارسال او استقبال علامات او إشارات او كتابات او صور او أصوات او معلومات مختلفة عن طريق الاسلاك او البصريات او اللاسلكي الكهربائي او أجهزة أخرى كهربائية مغناطسية.

اما فيما يخص تسجيل الأصوات فان المشرع الجزائري لم يعطي تعريفا صريحا لها، بل عرفها ضمنيا في نص المادة 65 مكرر من ق.ا.ج.ج على انها: وضع واستعمال الوسائل والترتيبات التقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث التسجيل الكلام المتفوه به بصفة خاصة او سرية من طرف شخص او عدة اشخاص يتواجدون في أماكن خاصة.

وطبقا لنص المادة 65 مكرر5 ق.ا.ج.ج فانه لا يمكن لضباط الشرطة القضائية اللجوء العمليات المذكورة سابقا الا بعد ان يحصل على اذن مكتوب ومسبب من طرف وكيل الجمهورية او قاضي التحقيق في حالة فتح تحقيق قضائي.

وعلى وكيل الجمهورية او قاضي التحقيق قبل منح هذا الاذن تقديره فائدة اجراء الاعتراض وجديته وملائمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا.

ولقد حدد المشرع الجزائري الجرائم التي يجوز فيها مباشرة اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وهذه الجرائم محددة على سبيل الحصر في المادة 65 مكرر5 منها الجرائم الماسة بأنظمة

[1] رابح سعاد، **ضوابط مكافحة الجريمة المعلوماتية**، مجلة القانون العام الجزائري والمقارن، جامعة جيلالي اليابس، سيدي بلعباس، المجلد 7، العدد01، جوان 2021، ص 272، 273.

المعالجة الالية للمعطيات، نظرا لخصوصيتها ولعدم كفاية الإجراءات التقليدية لجمع الدليل التقني واستكمال مقتضيات التحقيق.

يحرر ضابط الشرطة القضائية المأذون له او المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي او السمعي البصري ويذكر بالمحضر تاريخ وساعة بداية هذه العملية والانتهاء منها وهو ما نصت عليه المادة 65 مكرر 9 ق.ا.ج.ج، كما حمى المشرع الجزائري الاعتداء على الاتصالات والمراسلات بأية تقنية كانت ووسع من مجال حماية الاتصالات والمراسلات[1].

ثالثا: المراقبة والتتبع

يمكن لضباط الشرطة القضائية بعد تعديل القانون 22/06 للمادة 16 مكرر من قانون الإجراءات الجزائية تمديد الاختصاص بموافقة وكيل الجمهورية بكامل التراب الوطني لتنفيذ عمليات مراقبة الأشخاص اللذين يوجد ضدهم مبرر مقبول أو أكثر يحتمل على الاشتباه فيهم بارتكابهم هذه الجرائم، أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو أشياء ستستعمل في ارتكابها[2].

[1] بوحزمة نصيرة، مرجع سابق، ص390، 391.

[2] جدي نسيمة، مرجع سابق، ص 100.

المبحث الثاني: العقوبات والجهود المشتركة لمكافحة جريمة القرصنة الالكترونية

في ظل التطور المتسارع الذي يشهده العالم في مجال تكنولوجيا المعلومات والاتصالات، أصبحت الفضاءات الرقمية جزءاً لا يتجزأ من حياة الأفراد والمؤسسات على حد سواء. غير أن هذا التوسع الهائل رافقه بروز العديد من التحديات، من أبرزها جريمة القرصنة الإلكترونية، التي باتت تهدد أمن المعلومات، خصوصية الأفراد، واستقرار الأنظمة الاقتصادية والاجتماعية للدول، ولمواجهة هذا الخطر المتنامي، تكاثفت الجهود على الصعيدين الوطني والدولي، من أجل وضع أطر قانونية تقنية وتعاونية فعالة للحد من هذه الجريمة، والقبض على مرتكبيها، والتقليل من آثارها. فقد سعت الدول إلى سن تشريعات حديثة، وتحديث بنياتها الأمنية، فيما برز التعاون الدولي كأداة أساسية لمجابهة الطبيعة العابرة للحدود لهذه الجرائم. وقد قسمنا هذا المبحث الى مطلبين: **(المطلب الأول)** العقوبات، و**(المطلب الثاني)** المتمثل في الجهود الوطنية الدولية.

المطلب الأول: العقوبات

تتمتع الجريمة المعلوماتية بطبيعة مغايرة ومختلفة عن الجريمة التقليدية، لذا كان على المشرع الجزائري التصدي لها مثل باقي دول العالم، وذلك على مختلف درجات القانون انطلاقا من القانون 24-06 المعدل لقانون 04-15 المتضمن النصوص القانونية التي تعاقب على ارتكاب الجرائم الماسة بالأنظمة المعلوماتية. وتم تقسيم هذا المطلب الى فرعين: **(الفرع الأول)** العقوبة الأصلية، **(الفرع الثاني)** العقوبة التكميلية.

الفرع الأول: العقوبات الاصلية

نص المشرع الجزائري في القانون رقم 04-15[1] على العقوبات التي تستهدف المساس بالأنظمة المعلوماتية وجاء القانون رقم 24-06 [2] المتضمن تعديل قانون العقوبات، اذ بموجبه عدل في العقوبات

أولا: الشخص الطبيعي

تدرجت العقوبات المطبقة على الشخص الطبيعي وفقا لطبيعة الجريمة وخطورتها حيث يتبين لنا من خلال استقراء النص هذا التدرج:

1- عقوبة الدخول أو البقاء غير المصرح بهما:

تنص المادة 394 مكرر من القانون رقم 04-15 في فقرتيه 02 و03 على تشديد العقوبة، إذا تم تخريب نظام المعالجة واشتغال المنظومة حيث تصبح العقوبة من 6 أشهر الى سنتين والغرامة من 50.000 دج الى 150.000 دج بعد ان كانت العقوبة المقررة للشخص الطبيعي في جريمة الدخول والبقاء في صورتها البسيطة من 03 أشهر الى سنة وغرامة من 50.000 دج الى 100.000دج.

بعد تعديل 2024 فان العقوبة المقررة لهذه الأفعال بموجب المادة 394 مكرر من قانون العقوبات هي الحبس من 6 أشهر إلى سنتين والغرامة من 60.000 دج إلى 200.000 دج.

وتجدر الإشارة أن المشرع الجزائري اعتبر أنها العقوبة الأنسب لهذه الأفعال وما لها من خطورة كبيرة على سرية المعلومات المعالجة آليا، الأمر الذي جعل الدخول اليها وانتهاك سريتها أمر يعرض أصحابها للأضرار فادحة، خاصة إذا تعلقت بشركات أو إدارات تعتمد في تسير شؤونها على نظم المعالجة الآلية.

[1] انظر القانون رقم 04-15، السابق الذكر.

[2] انظر القانون رقم 24-06، السابق الذكر.

2- عقوبة جريمة إدخال او إزالة معطيات:

نصت المادة 394 مكرر 1 من القانون 04-15 على الحبس من 06 أشهر الى 03 سنوات، وبغرامة من 500.000دج الى 2.000.000دج كل شخص طبيعي قام بجريمة الاعتداء على سلامة المعطيات ونظام المعالجة بطريق الغش.

بعد التعديل الذي جاء به القانون رقم 24-06 فان المشرع الجزائري قرر لها في مادة 394 مكرر 1 عقوبة الحبس من سنة الى 3 سنوات، والغرامة المالية من 500.000 دج الى 2.000.000 دج.

3- عقوبة التعامل في معطيات غير مشروعة:

نصت المادة 394 مكرر 2 من قانون العقوبات الجزائري على جريمة التعامل الغير مشروع في معطيات، حيث فرض لها عقوبة الحبس من 02 شهرين إلى 03 سنوات، وبغرامة من 1.000.000دج إلى 5.000.000دج فهذه العقوبة مقررة للشخص الطبيعي الذي يقترف، وبالإضافة إلى ذلك نصت المادة 394 مكرر 3 من القانون رقم 04-15 على تشديد العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات التي تخضع إلى القانون العام، دون إخلال بتطبيق عقوبات أشد وظرف التشديد هنا يتمثل في مركز المجني عليه المتعلق في الهيئة العمومي.

اما بعد التعديل الذي جاء به القانون 24-06 هي الحبس من سنة الى 5 سنوات والغرامة من 1.000.000 دج 5.000.000 دج وذلك بموجب المادة 394 مكرر 2 في الفقرة (1).

ثانيا: الشخص المعنوي

تبنى قانون العقوبات الجزائري مبدأ المسؤولية الجزائية للأشخاص المعنوية بموجب القانون 04-15 في نص المادة 18 مكرر ليعزز ذلك بالقانون رقم 23 لسنة 2006 بنص المادة 51 مكرر وفي مضمون هذا النص استثنى المشرع الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة، ومن خلال استقراء المادة م 18 كرر فالعقوبات التي تطبق على الشخص المعنوي في الجنايات والجنح كالتالي:

- الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

ومما تجدر الإشارة إليه في هذا المقام أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب، بل تقع على كل الجرائم التي يرتكبها الشخص المعنوي، بينما ما يتعلق بالجرائم ضد الأنظمة المعلوماتية المحددة في المواد من 394 م كرر وما بعدها فإن الغرامة المطابقة على هذا

الأخير هي 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وذلك تطبيقا للمادة 394 مكرر 4 من قانون العقوبات الجزائري.

حيث أن المشرع الجزائري شدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية وهي الطائفة التي تنتمي إليها جل جرائم الدراسة، إذ نصت المادة 394 م كرر 4 بمضاعفة قيمة الغرامة 5 أضعاف ما قررته للشخص الطبيعي ونصت على الآتي: " ... بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي."

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة فتضاعف الغرامة في التشريع الجزائري مرتين، إذ تضاعف إلى خمس (5) مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي، وثم يضاعف ذلك إلى ضعفين لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة إلى عشر (10) أضعاف عما هو مقرر على الشخص العادي[1].

الفرع الثاني: العقوبات التكميلية

نص المشرع على عقوبات تكميلية للشخص الطبيعي والمعنوي في المادة 394 مكرر 6 من قانون العقوبات الجزائري "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على اغلاق المحل او مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها"

1-المصادرة: وهي مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية.

2- اغلاق المواقع: وهي اغلاق المواقع التي تكون محلا لجريمة من الجرائم الماسة بأنظمة المعلوماتية.

3- اغلاق المحل: يكون في حالة ما إذا كان صاحب المحل مشاركا في الجريمة او إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها، او بمنع مرتكبيها من ارتياد محله لارتكاب مثل هذه الجرائم وهي اغلاق المحل او مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها[2].

[1] رابحي عزيزة، مرجع سابق، ص248.

[2] معتوق عبد اللطيف، مرجع سابق، ص127.

بالنسبة لمدة الغلق لم تحددها المادة 394 مكرر 6 من قانون العقوبات وعليه يمكن ان تكون مؤبدة او مؤقتة كما نصت على ذلك المادة 26 من قانون العقوبات: "يجوز ان يأمر بغلق المؤسسة نهائيا او مؤقتا في الحالات المنصوص عليها في القانون[1]."

المطلب الثاني: الجهود الوطنية والدولية في مكافحة جريمة القرصنة الإلكترونية

ان ما تتميز به الجرائم المعلوماتية من حداثة الأسلوب وسرعة التنفيذ وسهولة الاخفاء والقدرة على محو اثارها وتعدد صورها واشكالها، ليس هذا فحسب بل اتصفت بالعالمية وبانها عابرة للحدود حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا امام مرتكبي الجرائم المعلوماتية، على المستوى وإزاء ذلك كان لابد من تكاتف الدول من اجل مكافحة هذا النوع المستحدث من الجرائم وعليه سنقسم هذا المطلب الى فرعين: **(الفرع الأول)** الجهود الوطنية الأخرى و **(الفرع الثاني)** الجهود الدولية.

الفرع الأول: الجهود الوطنية الاخرى

امام تزايد معدلات الجريمة المعلوماتية، حيث اخدت منحنى خطير خاصة بعد ما كشف عنه الدول من إحصائيات نتيجة الاستخدام الواسع للتقنيات الرقمية بمختلف أنواعها، الامر الذي الزم تدخلا فعالا من اجل وضع نصوص قانونية وانشاء مراكز ووحدات لغرض مواجهة جريمة القرصنة المعلوماتية، وسنتطرق الى الضوابط التشريعية ومراكز وطنية متخصصة.

أولا: الضوابط التشريعية

تنوعت الضوابط التشريعية المتبعة من اجل مواجهة الجريمة المعلوماتية، وذلك على مختلف درجات القانون، انطلاقا من احكام الدستور، والتي ضمنت حرية الابتكار وحقوق المؤلف وفي إطار ذلك وضع المشرع سياجا واضحا، اعتمد على اطر قانونية جاءت على مراحل متفرقة في نصوص متناثرة، بنسب مختلفة، ولعل اهم النصوص القانونية الضابطة لهذه المسالة ما يلي:

1- تقرير حماية جزائية لمعطيات الحاسب الآلي في قانون الملكية الفنية والأدبية

وذلك من خلال القانون رقم 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث اعترف المشرع بوصف المصنف الفكري لمعطيات الحاسب الآلي، إذ نجد أنه وسع من قائمة المؤلفات المحمية، حيث أدمج تطبيق الإعلام الآلي ضمن المصنفات المحمية في المادة الرابعة منه، عندما نص على برامج الحاسوب الآلي، واعتبر أن أي اعتداء على الحق المالي والأدبي لمؤلف البرامج

[1] جدي نسيمة، مرجع سابق، ص127.

والبيانات يشكل فعلا من أفعال التقليد المنصوص عليها في المادة 151 من الأمر 03-05 والتي تقرر العقوبات الجزائية المكرسة في المواد 153-156-154 والمادة 158 من الأمر نفسه [1].

2- مكافحة الجريمة المعلوماتية من خلال القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم الخاصة المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

تضمنت المادة الأولى من هذا القانون الهدف منه وهو الوقاية من الجريمة المعلوماتية، ليحدد في المادة الثانية عديد المفاهيم المرتبطة بتكنولوجيا الإعلام والاتصال، ويصبو هذا القانون إلى التمكين من مكافحة الجريمة المعلوماتية عن طريق مجموعة من التدابير متمثلة في تحديد الحالات التي يجوز فيها لسلطات الأمن مراقبة المراسلات الإلكترونية وهي أربع حالات: - الأفعال التي تحمل وصف جرائم الإرهاب والتخريب، والجرائم ضد أمن الدولة.- عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة والدفاع الوطني أو النظام العام لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية، دون اللجوء إلى المراقبة الإلكترونية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما تضمن قانون 09-04 [2] إجراءات جديدة تدعم تلك المنصوص عليها في قانون الإجراءات الجزائية ولاسيما المتعلقة بالجرائم المعلوماتية والتي يمكن تلخيصها فيما يلي:

- جواز التفتيش ولو عن بعد للمنظومة المعلوماتية أو جزء منها من طرف الجهات القضائية المختصة وضباط الشرطة القضائية.
- إمكانية تمديد آجال التفتيش بإذن من السلطة القضائية المختصة.
- إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في المنظومة المعلوماتية الموجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل طبقا للمادة الخامسة من القانون 09-04[3].

3- مكافحة الجريمة المعلوماتية في قانون التأمينات الاجتماعية

إضافة لما سبق قرر المشرع مواجهة الجريمة المعلوماتية كذلك من خلال قانون 08-01 المعدل للقانون 83-11 المتعلق بالتأمينات الاجتماعية، حيث أشارت المادة 6 مكرر 1 منه إلى البطاقة الإلكترونية

[1] رابح سعاد، مرجع سابق، ص 270.

[2] القانون رقم 09-04، السابق الذكر.

[3] رابح سعاد، مرجع سابق، ص 274.

المسلمة للمؤمن له، بينما أشارت المواد من 93 مكرر 2 إلى مكرر 6 إلى العقوبات المطبقة على كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية للمؤمن له اجتماعيا في المفتاح الإلكتروني، كما جرم كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له، كما جرم المشرع كل من ينسخ أو يضع أو يحوز أو يوزع بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال البطاقة الإلكترونية وغيرها[1].

ثانيا: المراكز والوحدات الوطنية المتخصصة

يتمثل في المراكز والوحدات التي أنشأت لغرض مواجهة الجريمة الإلكترونية، ومدى استعدادها لأدائها من ذلك والمتمثلة أساسا في:

1- المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني

هو مؤسسة عمومية ذات طابع اداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بالمهام التالية:

-اجراء الخبرات والفحوص العلمية في إطار التحريات الاولية والتحقيقات القضائية وهذا بغرض اقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.

-ضمان المساعدة العلمية اثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.

-المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل اشكال الإجرام.

-تصميم وانجاز بنوك المعطيات.

-المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.

-المبادرة واجراء بحوث متعلقة بالإجرام باللجوء الى التكنولوجيات الدقيقة.

ولتأدية مهامه على أكمل وجه فان المعهد الوطني للأدلة الجنائية وعلم الاجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمه:

-مصلحة الاعلام الآلي : على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة الإلكترونية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية[2].

[1] رابح سعاد، مرجع سابق، ص 274، 275.

[2] بارة سمير، **الامن السبراني في الجزائر**، المجلة الجزائرية للأمن الانساني، جامعة قاصدي مرباح، ورقلة، العدد الرابع، جويلية 2017، ص271.

2-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني

استجابة لمطلب الأمن المعلوماتي و محاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، و التي كانت عبارة عن فصيلة شكلت النواة الاولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني و التي انشأت سنة 2011، ليتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015[1].

الفرع الثاني: الجهود الدولية

ان جريمة القرصنة جريمة عابرة للحدود وإزاء ذلك كان لابد من تكاتف الدول من اجل مكافحة هذا النوع المستحدث من الجرائم، وبناءا عليه سيتم التفصيل في هذا الفرع من خلال التطرق الى الاتفاقيات المبرمة للتصدي لهذه الجريمة والى التعاون الدولي.

اولا: الاتفاقيات المبرمة لمكافحة جريمة القرصنة الإلكترونية

وتتمثل هذه الاتفاقيات في: اتفاقية بودابست والاتفاقية العربية وسنتطرق إليهم كالآتي:

1-اتفاقية بودابست لمكافحة جرائم المعلوماتية والأنترنت (بودابست 2001)

لعب المجلس الأوروبي دورا مهما في مكافحة الجرائم المعلوماتية، وصدر عنه العديد من التوصيات لحماية تدفق المعلومات، ففي سنة 1981 وقع المجلس الأوروبي اتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية، وفي أفريل من سنة 2000 تقدمت اللجنة الأوروبية لمشكلات الحاسب الآلي **(CDPC)** بمشروع اتفاقية جرائم المعلوماتية والتي تم المصادقة عليها في بودابست بالمجر سنة 2001.

وتتكون الاتفاقية من مقدمة وأربعة فصول، حيث تم استعراض أهداف الاتفاقية ومرجعياتها السابقة وبعض التدابير التشريعية الإقليمية والدولية المتعلقة بجرائم المعلوماتية، كما ثمنت المقدمة التعاون الدولي في هذا المجال، وأكدت مقدمة الاتفاقية على أهمية ما تم انجازه من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوروبي ومجموعة الدول الصناعية (مجموعة الثمانية)[2].

1.1الأحكام الموضوعية للاتفاقية

-الجرائم ضد سرية وسلامة وإذاعة البيانات والنظم المعلوماتية.

-إساءة استخدام أجهزة الحاسوب.

---

[1] بارة سمير، مرجع سابق، ص272، 273.

[2] اتفاقية بودابست بشأن الجرائم الالكترونية، رقم المعاهدة 185 ETS. NO، بودابست، 2001.

-الجرائم المعلوماتية (الجرائم المتصلة بالحاسب).

-الجرائم المتصلة بالمحتوى.

-الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة.

2.1 الاحكام الإجرائية لاتفاقية بودابست

نصت المواد من 14 إلى 21 من الاتفاقية على الأحكام الإجرائية لجرائم الحاسوب، وقد تضمنت هذه المواد إلزام كل طرف في هذه الاتفاقية بتهيئة تشريعية داخلية لتقرير السلطات الإجراءات اللازمة في مجال التحقيق بالجرائم.

كما ألزمت هذه الاتفاقية الدول الأطراف عند سن تشريعاتها الداخلية المتعلقة بجرائم الحاسوب والأنترنت، وأن تراعي الاتفاقيات الدولية لحقوق الإنسان، مثل الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية لعام 1950، والميثاق الدولي حول الحقوق المدنية والسياسية لعام1966 (المادة 15 من الاتفاقية).

وتجدر الإشارة أن الدول الأعضاء في الاتفاقية بحاجة لمواصلة سياسية جنائية مشتركة تهدف إلى حماية المجتمع من جرائم القضاء المعلوماتي كهدف أساسي ضمن أشياء أخرى وذلك بتبني تشريعات مناسبة وتنمية التعاون الدولي.

أما فيما يتعلق بتفتيش وضبط البيانات المعلوماتية المخزنة في الحاسوب، فقد أشارت المادة 19 من الاتفاقية على ضرورة أن يكون هناك نصوص تشريعية داخلية لدى تتضمن الإجراءات المتبعة في جميع الأدلة الجنائية وهي:

-تفتيش نظام الحاسوب أو جزء منه والبيانات المخزنة فيه.

-تفتيش معالج تخزين البيانات في الحاسوب الذي يحتوي على بيانات معينة، ويدخل ضمن مفهوم معالج تخزين البيانات حسب المذكرة التفسيرية للاتفاقية الأقراص الليزرية والأقراص المرنة[1].

ثانيا: الاتفاقية العربية

وافقت على الاتفاقية مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21-12-2010.

وتسري هذه الاتفاقية بعد مضي ثالثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها من سبع دول عربية بموجب الفترة الثالثة من الأحكام الختامية للاتفاقية.

وتهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنيات المعلومات، وذلك من أجل المحافظة على أمن الدول العربية ومصالحها وسالمة مجتمعاتها وأفرادها من كل أشكال الإجرام الإلكتروني.

[1] اتفاقية بودابست، المذكورة سابقا

وتجدر الإشارة أن الاتفاقية العربية تتكون من ثالثة وأربعين مادة حيث ذكرت المادة الثانية تحديد مفهوم بعض المصطلحات مثل تقنية المعلومات، مزود الخدمة البيانـــات البرنامـــج المعلوماتي، الشبكة المعلوماتية.

1-الاحكام الموضوعية للاتفاقية العربية لمكافحة جرائم تقنيات المعلومات

وتجدر الإشارة ان الاحكام الموضوعية للاتفاقية تضمنت عدة أنواع من الجرائم المتصلة بالتطور التكنولوجي وهي:

-جريمة الدخول غير المشروع

وتشمل هذه الجريمة فعل الدخول والبقاء غير المشروع وهو كل اتصال مع كل أو جزء من تقنية المعلومات أو الاستمرار به، أو الحصول على معلومات حكومية سرية، وتشدد العقوبة إذا نتج عن الدخول أو البقاء أو الاتصال محو أو تعطيل أو تدمير البيانات المخزنة داخل الحاسب والأجهزة الإلكترونية وشبكات الاتصال.

-جريمة الاعتراض غير المشروع

الاعتراض غير القانوني والمتعمد بدون وجه حتى بواسطة وسائل تكنولوجية وقطع بث أو استقبال بيانات تقنية المعلومات.

-جريمة الاعتداء على سلامة البيانات

وتشمل الأفعال الإجرامية الآتية، تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات متعمدا، ويجب أن تسبب هذه الأفعال بضرر جسيم للمعلومات والبيانات المخزنة داخل الأنظمة الإلكترونية أو أي وسيلة الاتصال[1].

2-الأحكام الإجرائية للاتفاقية العربية لمكافحة جرائم تقنيات المعلومات

تضمنت المواد من 66 إلى 61 من الاتفاقية العربية الأحكام الإجرامية، حيث ألزمت الاتفاقية كل دولة طرف أن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصالحيات والإجراءات الواردة في مجال التحقيق في الجرائم المذكورة أعاله، وكذلك إجراءات التفتيش المعلومات المخزنة في الحاسب الآلي وفق قانونها الداخلي، وتضمنت الإجراءات المتبعة في حالة ارتكاب الجرائم خارج الإقليم الوطني ولكنها تمس بالأمن الداخلي للدولة، أو تمس بسيادة الدولة وكذلك نصت الاتفاقية على أشكال التعاون الأمني والقضائي في مجال تمديد الاختصاص القضائي للبحث والتحري والقبض على المجرمين[2].

[1] عمر يوسف عبد الله، مرجع سابق، ص 258، 259.

[2] نفس المرجع، ص262.

ثانيا: التعاون الدولي

ان التعاون الدولي هو سبيل التعاون الفعال لمكافحة الجرائم المعلوماتية، من ثم أنشئ عدد من المنظمات والكيانات الدولية والعربية وابرمت العديد من الاتفاقيات الدولية التي تسهم في كافة الإجراءات لمكافحة الجرائم المعلوماتية، وسنوضحه فيما يلي:

1-التعاون الأمني على المستوى الدولي

في مواجهة الجريمة المعلوماتية عموما، غالبا ما تقف السلطات القضائية وقوات الشرطة عاجزة عن التحكم في هذا الإجرام الجديد وذلك لعوامل عديدة يأتي في مقدمتها الحدود الطبيعية بين الدول، بيد أنه تقف حاجزا في وجه المكلفين بمكافحة الإجرام المعلوماتي والتي تتوقف صلاحيتها عند حدود دولتهم، وفي حالة اتصال شبكة معلومات الكمبيوتر بين دولتين أو أكثر، نكون بحاجة إلى التعاون لتخطي هذا الإشكال دولة – لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل

في كافة ميادين الحياة. فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوعٌ من الجرائم المعلوماتية، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة، ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي ، على المستوى الإجرائي الجنائي بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها.

والإشكال المحتم بالنسبة لهذه الجرائم هو أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشافها ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المتصلة بالحاسب الآلي وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة بين الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى آخر أنه متى ما فر المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزا[1].

[1] رابحي عزيزة، مرجع سابق، ص283.

1.1جهود منظمة الأمم المتحدة في مجال مكافحة الجرائم الالكترونية

لعبت المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة دورا مهما في الحفاظ على الأمن والاستقرار، وخاصة في مجال مواجهة الجريمة الالكترونية عبر إقرار العديد من الاتفاقيات وعقد المؤتمرات، أهمها مؤتمر منع الجريمة ومعاملة المجرمين، كما أنشأت وكالات متخصصة لهذا الغرض كالمنظمة العالمية للملكية الفكرية (WIPO).

وتجدر الإشارة أن الأمم المتحدة تبذل جهودا في سبيل تعزيز العمل المشترك بين أعضاء المنظمة من اجل التعاون في مواجهة الجرائم المتصلة بالتطور التكنولوجي والانترنت التي تهدد الأمن ألمعلوماتي على المستوى الدولي.

وتسعى الأمم المتحدة من خلال هيئاتها والوكالات التابعة لها لوضع الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة، وكانت عدد من المنظمات الدولية تعمل باستمرار لمواكبة التطورات في شان امن الفضاء الالكتروني، ووضع السياسات العامة والتدابير العامة والتدابير الأمنية و المبادئ التوجيهية وطرق إدارة المخاطر والحماية و التدريب، وتشمل هذه السياسات المعلومات وأجهزة الكمبيوتر و حماية نظم اتصالات السلكية و اللاسلكية و مجمل المعلومات المنقولة أو المخزنة في الأجهزة الالكترونية، و يهدف الأمن ألمعلوماتي لضمان تحقيق سالمة المؤسسات و الإفراد في مواجهة المخاطر الأمنية و كل ما يتعلق بشبكة الانترنت[1].

2.1جهود المنظمة الدولية للشرطة الجنائية" الإنتربول

نشأت "اللجنة الدولية للشرطة الجنائية" في 20-4-1923م، وكان اختصاصها التنسيق بين أجهزة الشرطة في الدول الأوروبية في مجال مكافحة الجريمة. إلا أن عملها توقف بسبب نشوب الحرب العالمية الثانية، وطوال السنوات العشر اللاحقة، حتى تاريخ 14-7-1956م أُعيد تنظيم اللجنة من جديد، ووُضع لها نظام جديد ودستور أساسي للعمل في فيينا، وسُمّيت "المنظمة الدولية للشرطة الجنائية"، وتم اعتماد لفظ "إنتربول" **(Interpol)**رمزاً لها في جميع اللغات، وتضم هذه المنظمة 190 دولة، ومقرها الحالي في مدينة ليون الفرنسية. وللمنظمة أربع لغات رسمية هي: (العربية – الإنجليزية – الفرنسية – الإسبانية). وتتكون المنظمة وفقاً لنص المادة (5) من دستورها من خمسة أجهزة، وهي: الجمعية العامة – اللجنة التنفيذية – الأمانة العامة – جهاز المستشارين – المكاتب المركزية الوطنية[2]، ومن مهامها فيما يخص الجريمة

[1] عمر يوسف عبد الله، مرجع سابق، ص 268.

[2] طاهر محمود أبو القاسم، مرجع سابق، ص 260.

الالكترونية تعقب مجرمي المعلوماتية عامة وشبكة الأنترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الالي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا على ما قد تحويه من ادلة وبراهين على ارتكاب الجريمة الالكترونية[1] من اختصاصاته:

–تشجيع التعاون المتبادل بين سلطات الشرطة في الدول الأطراف على نحوٍ فعال يحقق نتائج إيجابية في مكافحة الجريمة ذات الطابع الدولي، وهي كذلك تختص بمكافحة الإجرام المنظم العابر للحدود بجميع صوره، بما في ذلك الجرائم المعلوماتية.

–إقامة وتنمية النظم التي من شأنها أن تسهم على نحو فعال ومؤثر في منع ومكافحة جرائم القانون العام، ويتضح من المادة (الثامنة) من ميثاق المنظمة الدولية للشرطة الجنائية أن المنظمة تعمل على تأكيد التعاون الدولي بين الدول الأعضاء، نتيجة ما حدث بالجماعة الدولية من تطورات في المجالات كافة، وخاصة في مجال المواصلات التي كان لها أثرها في سهولة انتقال المجرمين بين الدول، بعد ارتكابهم لجرائمهم في البلدان المختلفة؛ الأمر الذي يتطلب التعاون بين أجهزة الشرطة كافة، لمكافحة مثل هذه الأعمال.

فتدخل الإنتربول يعود لطبيعة الجريمة التي قد يسهم في ارتكابها عنصر أجنبي كونها عابرة للحدود، فقد يرتكب شخص جريمة على أرض دولة ثم يهرب إلى دولة أخرى، أو تكون الجريمة مرتكبة في عدة دول في مراحل أو كل دولة لها جزء من أركان الجريمة، وهذا التعاون بين الدول الأعضاء يجب أن يكون في إطار الإعلان العالمي لحقوق الإنسان وبعيدًا عن الأمور السياسية والدينية والعنصرية، للعمل على قيام نظام أكثر أمانًا وسلامًا، وهذا ما أكده رئيس الإنتربول (كوبون هوى) في المؤتمر الدولي لمكافحة الجرائم الماسة بالملكية الفكرية والمنعقد في (بانما) عام 2012م حيث تم عرض نماذج عن العمليات الدولية التي نُفذت في عام 2012م بدعم من المنظمة، في كل من أفريقيا وأوروبا والشرق الأوسط وأمريكا، وأسفرت عن ضبط العديد من القضايا المرتبطة بسلع مقلدة ومغشوشة وغير مشروعة وتدخلات في المواقع التجارية وتبادل بيانات غير مشروعة، بلغت قيمتها نحو 155 مليون يورو. وقد تم ضبط أكثر من 1700 من المتهمين، وذلك لخلق والحفاظ على بيئة آمنة للأفراد والأسر والمجتمعات والمؤسسات والدول.[2]

وأما عن علاقة الجزائر بالمنظمة الدولية للشرطة الجنائية فالجزائر انخرطت مباشرة بعد الاستقلال أي في سنة 1963 وشاركت في عدة ملتقيات وكانت عنصرا نشيطا بها، وقد أقام المشرع الجزائري علاقة

[1] شنتير خضرة، مرجع سابق، ص 210.

[2] طاهر محمود أبو القاسم، مرجع سابق، ص 261.

قانونية بين أعمال المنظمة وما يتطلبه تحويل المتهمين عبر نقاط الحدود والسفارات المعتمدة لدى الدولة فجاء في قانون الإجراءات الجزائية مفهوم إجراءات التسليم وآثاره وحركة العبور سواء طبقا لاتفاقية أو بطريقة دبلوماسية وهذا بعد انجاز الطلبات الواردة في شكل استمارات من الانتربول أو بضمانات دولية[1].

2-التعاون القضائي الدولي في مجال جرائم القرصنة

تعّرف المساعدة القضائية الدولية بأنها"" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم" ، وتتخذ المساعدة القضائية في المجال الجنائي صور عدة كما أنه قد تكون هده المساعدة رسمية أو غير رسمية لقد نص المشرع الجزائري في القانون /04 09 على مبدأ المساعدة القضائية في المادة 16 منه معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، وتتخذ المساعدة القضائية الدولية عدة صور أهمها:

1.2تبادل المعلومات

يُعد تبادل المعلومات والخبرات من أبرز العناصر الفعَّالة في مجال الوقاية من الجريمة، حيث يُسهم تشارك البيانات وسرعة الوصول إليها في تسهيل مهام الأجهزة الوطنية لاتخاذ الإجراءات المناسبة لمواجهة الأنشطة الإجرامية.

ولهذا السبب يُولي المجتمع الدولي أولوية قصوى لتبادل المعلومات باعتباره آلية حاسمة لمكافحة الجريمة بشكل عام، والجريمة الإلكترونية على وجه الخصوص. فالمعلومات الدقيقة والموثوقة تدعم أجهزة إنفاذ القانون في مختلف المجالات مثل تتبع أنشطة المنظمات الإجرامية، ومراقبة تدفقات الأموال غير المشروعة، وفي هذا الإطار أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين بضرورة تطوير التبادل المنهجي للمعلومات كعنصر أساسي في الاستراتيجيات الدولية للوقاية من الجريمة ومكافحتها، داعيًا إلى إنشاء قاعدة معلوماتية تابعة للأمم المتحدة لاطلاع الدول على الاتجاهات العالمية في مجال الجريمة.

ويتم تحقيق تبادل المعلومات عبر المنظمات والاتفاقيات الدولية ويتضمن ذلك مشاركة البيانات والوثائق والأدلة التي تطلبها سلطة قضائية أجنبية أثناء نظرها في قضية إجرامية، كما يشمل التبادل معلومات عن

[1] رابحي عزيزة، مرجع سابق، ص 309.

الاتهامات الموجهة لمواطني دولة ما خارج حدودها والإجراءات القانونية المتخذة ضدهم، بالإضافة إلى السوابق القضائية للمجرمين[1].

2.2نقل الإجراءات

يُقصد بنقل الإجراءات قيام إحدى الدول – بناءً على اتفاقية أو معاهدة – باتخاذ إجراءات جنائية في جريمة ارتُكبت في إقليم دولة أخرى ولمصلحة تلك الدولة، وذلك عند توافر شروط محددة. من أبرز هذه الشروط ان يكون التجريم المزدوج ويُقصد به أن يكون الفعل المنسوب إلى المُتهم مُجرَّمًا في قانون كل من الدولة الطالبة (التي تطلب نقل الإجراءات) والدولة المطلوب إليها النقل، كذلك شرعية الإجراءات أي أن تكون الإجراءات المطلوب اتخاذها مُقررة في قانون الدولة المطلوب إليها النقل لنفس الجريمة وأهمية الإجراءات تكمن في أن تكون الإجراءات المطلوبة ذات دور حاسم في الكشف عن الحقيقة وتحقيق العدالة ويُشترط أيضًا ألا تتعارض هذه الإجراءات مع النظام العام أو السيادة القانونية للدولة المطلوب إليها النقل[2].

3.2 الإنابة القضائية الدولية

قصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية كسماع الشهود، و اجراء التفتيش والمعاينة، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها.

وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول فيما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى و يتم ارسال طلب الانابة القضائية عبر القنوات الدبلوماسية. و بتطبيق الانابة الدولية القضائية و التعاون القضائي لمكافحة الجرائم المعلوماتية، تلاحظ انه قد يتعارض مع طبيعة هذه الجرائم التي تتميز بالسرعة في ارتكابها و ايضا في قدرة الجاني على محو او التلاعب في ادلة الاثبات بسرعة فائقة[3].

والإنابة القضائية تجد أساسها في القوانين الوطنية وفي الاتفاقيات الدولية وفي مبدأ المعاملة بالمثل الاعتراف بالأحكام الأجنبية حسب القاعدة الكلاسيكية، أن كل دولة لا تعترف إلا بأحكام قانونها الجنائي ولا تعتد إلا بالأحكام الجنائية الصادرة عن محاكمها الوطنية، ولهاته القاعدة ما يبررها فه ي من ناحية

[1] بوحزمة نصيرة، مرجع سابق، ص 429.

[2] مرجع نفسه، ص 431.

[3] طاهر محمود أبو القاسم، مرجع سابق، ص 270، 271.

تعبير عن سيادة الدولة، ومن ناحية أخرى فإن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام، وهذا ما يحول دون إمكانية تطبيق قانون أجنبي.

لكن مع استفحال ظاهرة الإجرام الدولي، وضرورة تعاون الدول فيما بينها لمكافحة الجرائم عبر الوطنية وحتى لا يفلت الجناة من العقاب لمجرد أنهم أقاموا في دولة غير تلك التي صدر ضدهم فيها حكم جنائي بالإدانة صار ممكنا الاعتراف بحجية الأحكام الأجنبية استنادا على معاهدات تبرم بين الدول[1] .

4.2تسليم المجرمين

استقر الفقه القانوني على أن تسليم المجرمين يُعد أحد أشكال التعاون الدولي في مكافحة الجريمة، لا سيما مع تطور وسائل الاتصال والمعلومات الذي أزال الحدود بين الدول أمام مرتكبي الجرائم. ومع امتداد الأنشطة الإجرامية عبر الأقاليم، أصبح من الضروري إيجاد آلية قانونية تُمكن من تسليم المجرمين، خصوصًا في الجرائم التي ترتكب باستخدام التكنولوجيا. ويُشترط لتسليم المجرم أن يكون الفعل مجرّمًا في كلا الدولتين، وأن يصدر طلب رسمي بذلك. كما لا يجوز لأي دولة تجاوز حدودها القضائية لملاحقة مجرمين في دول أخرى دون تنسيق وتعاون قانوني.

ينبني إجراء تسليم المجرمين أساسًا على وجود المتهم في إقليم الدولة، والتي لها الحق في محاكمته إذا كان قانونها يجيز ذلك. أما إذا طُلب تسليمه لدولة أخرى، فيجب أن تتحقق مصلحة مشتركة للطرفين، وأن يتوافق الطلب مع القوانين الداخلية. ولتحقيق هذا التوازن، عمدت أغلب التشريعات إلى وضع قواعد خاصة لتسليم مرتكبي الجرائم المعلوماتية، كونها تمثل نوعًا متطورًا من الإجرام العابر للحدود. ولهذا، أولى المشرّع اهتمامًا كبيرًا بهذا الإجراء كأحد مظاهر التعاون القضائي الدولي[2].

[1] رابحي عزيزة، مرجع سابق، ص 312.

[2] سعيداني نعيم، مرجع سابق، ص 91، 92.

ملخص الفصل الثاني

نستخلص ان جريمة القرصنة المعلوماتية من أخطر اشكال الجريمة الالكترونية بحيث تستهدف الأنظمة المعلوماتية وتواجه هذه الجريمة تحديات كبيرة بسبب طابعها العابر للحدود واعتمادها على تقنيات متطورة يصعب التحقيق فيها وفي مثل هذه الجرائم ويجب ان يكون المحقق ذو خبرة وكفاءة عالية في البحث والتحري، مع استعانته بأساليب حديثة كالتسرب وتسجيل الأصوات واللجوء كذلك الى أساليب قديمة كالتفتيش والمعاينة، وهي تعتمد على وسائل مادية وإجرائية للكشف عنها.

وتعمل الجزائر على تطوير تشريعات خاصة بمكافحة الجرائم المعلوماتية، وتكوين وحدات متخصصة في التحقيق الالكتروني داخل الأجهزة الأمنية وتحديث النصوص القانونية لتعزيز الحماية، اما على الصعيد الدولي فان التعاون بين الدول يعد عنصرا أساسيا في مواجهة هذه الجرائم، من خلال الاتفاقيات الدولية مثل اتفاقية بودابست، والاتفاقيات العربية مثل الاتفاقية العربية، والمساعدة القضائية المتبادلة، وتنسيق الجهود بين الشرطة الدولية " الانتربول".

يمثل التنسيق بين الجهود الدولية والوطنية السبيل الأمثل لمكافحة القرصنة الالكترونية حيث لا يمكن لأي دولة ان تواجه بمفردها التهديدات التي تتجاوز حدودها الرقمية.

الخاتمة

الخاتمة:

من خلال تحليلنا لمختلف صور جريمة القرصنة الالكترونية على حدى يتبين ان النصوص التشريعية التي نص عليها المشرع الجزائري تعتبر ضرورية واساسية لمكافحة القرصنة الالكترونية لكنها ليست كافية وحدها لا بد من دعمها بآليات تنفيذ فعالة، وتعاون دولي وتحديث القوانين بشكل مستمر لمواجهة التحديات التقنية الجديدة، ومن اهم النتائج التي خلصنا اليها بعد هذه الدراسة هي:

أن لجريمة القرصنة الإلكترونية خصائص مميزة، تنقسم إلى خصائص تتعلق بالجريمة نفسها وأخرى بالمجرم المعلوماتي، وتختلف بذلك عن الجرائم التقليدية. فمن بين أبرز خصائصها أنها عابرة للحدود الجغرافية، يصعب اكتشافها، سريعة التنفيذ، ولا تتطلب جهدًا أو عنفًا كما هو الحال في الجرائم العادية، أما فيما يخص الجاني، فنجد أن المجرم المعلوماتي غالبًا ما يكون متخصصًا في هذا المجال، يتسم بالذكاء، وغير عنيف في الغالب. ولهذا السبب، تسعى التشريعات في مختلف الدول إلى مجابهة هذه الأنواع من الجرائم المعلوماتية والحد من انتشارها، ومن بينها جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، والتي تُعقّد من مهام السلطات المختصة في الكشف عنها وجمع الأدلة اللازمة.

وعلى المستوى الوطني، نجد أن المشرع الجزائري قد كافح هذه الجرائم من خلال قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، إضافة الى انشاء مراكز ووحدات للحد من هذه الجريمة كالمعهد الوطني لمكافحة الاجرام المعلوماتي. اما على المستوى الدولي فلجأت لتعاون الدولي العديد الى الانعقاد في اتفاقيات مثل بودابيست والاتفاقية العربية ومراكز الشرطة العالمية "الانتربول" وفي التعاون القضائي كتسليم المجرمين والانابة القضائية.

زيادة على ذلك تتمثل الاقتراحات في:

-إنشاء سلطات متخصصة في البحث والتحري عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

-الإكثار من البرامج التوعوية حول خطورة هذه الجرائم على حياة الفرد والمجتمع بالتنسيق مع المؤسسات التعليمية.

-تشديد العقوبة لمرتكبي هذه الجرائم نظرا لما تخلفه من أضرار.

-توفير الحماية الجنائية اللازمة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

-شرح وتفسير النصوص القانونية المتعلقة بهده الجرائم.

-إنشاء لجان وهيئات متعددة لمكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: الاتفاقيات

1.اتفاقية بودابست بشأن الجرائم الالكترونية، رقم185 ETS . NO، بودابست،2001.

ثانيا: النصوص القانونية

1.الامر رقم 66-156، المؤرخ في 18 صفر1386، الموافق 08 يونيو 1966، المتضمن قانون العقوبات، المنشور بالجريدة الرسمية، عدد 49 المؤرخة في 11 يونيو 1966.

2.القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المتضمن تعديل قانون العقوبات، الصادر في الجريدة الرسمية رقم:71، والذي أضيفت بموجبه المواد من 394مكرر الى 394 مكرر7.

3.القانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، المتضمن قانون العقوبات، ج. ر عدد 71، الصادرة في 14 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 جوان 1966.

4.القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم للأمر 66-155، المنشور بالج. ر، رقم 84.

5.القانون رقم 09-04، مؤرخ في 5 اوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام ومكافحتها، ج. ر العدد 47، الصادر بتاريخ 16 اوت 2009.

6.القانون رقم 24- 06، المؤرخ في 19 شوال 1445، الموافق ل 28 ابريل 2024، المعدل و المتمم للأمر66-156، المتضمن قانون العقوبات، الج. ر.، العدد 30، الصادرة في 30 ابريل 2024.

ثالثا: الكتب

1.بشرى حسين الحمداني، القرصنة الالكترونية أسلحة الحرب الحديثة، الطبعة الأولى، دار أسامة للنشر والتوزيع، الأردن-عمان، 2014.

2.طاهر محمود أبو القاسم، الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية مواجهتها، المنظمة العربية للتنمية الإدارية، القاهرة، 2019.

3.فيصل محمد عبد الغفار، الحرب الإلكترونية، الجندارية للنشر والتوزيع، الاردن-عمان، 2015

4.نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010.

رابعا: الرسائل العلمية

- **اطروحة الدكتوراه**

1. خضرة شنتير، الاليات القانونية لمكافحة الجريمة الالكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة احمد دراية، ادرار، 2021.

2. عمر يوسف عبد الله، الإطار القانوني والمؤسساتي لمكافحة التقليد والقرصنة الالكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة وهران2، 2021-2022.

3. عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بالقايد، تلمسان، 2017-2018.

4. نصيرة بوحزمة، التحقيق الجنائي في الجرائم الالكترونية (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس،2022.

- **رسائل الماجيستير**

1. عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، رسالة ماجيستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012.

2. سيمة جدي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير، كلية الحقوق، جامعة وهران، وهران، 2014.

3. نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري، رسالة ماجستير، كلية الحقوق، جامعة منتوري، قسنطينة، 2013.

4. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.

5. يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

- **مذكرات الماستر**

1. سيهام بن عنطر، التحقيق الجنائي في الجرلئم الالكترونية، مذكرة ماستر، كلية

2. سمير بودواب، فؤاد لبديوي، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 20 اوت 1955، سكيكدة، 2024.

3.شهرزاد رحراح، رشيدة بوكر، جريمة القرصنة في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة بن باديس، مستغانم، 2022، ص 15.

4.نجاة دحو، فاطمة أولاد علي، جريمة القرصنة الإلكترونية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2021-2022.

خامسا: المقالات والمجلات

1.أحلام بن شريف، الصالح بوغرارة، القرصنة الالكترونية أنواعها أشكالها وطرق التصدي لها، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، جامعة تيارت، المجلد05، العدد01، جوان 2012

2.اكرام مزوري، القرصنة الرقمية كعائق تقني لنظام التقاضي، مجلة البصائر للدراسات القانونية والاقتصادية، المركز الجامعي مغنية، الجزائر، العدد الخاص، 2021.

3.الطاهر ياكر، مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الهدى للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، المجلد4، العدد4، 2022.

4.حسين ربيعي، المجرم المعلوماتي شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 40، جوان 2015.

5.زهرة عجري، القرصنة في العهد العثماني في البحر الأبيض المتوسط في القرن 16م، مجلة عصور جديدة، جامعة وهران احمد بن بلة، المجلد14، العدد2، اكتوبر 2024.

6.سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، جامعة جيلالي اليابس، سيدي بلعباس، المجلد 7، العدد01، جوان 2021.

7.سمير بارة، الامن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، جامعة قاصدي مرباح، ورقلة، العدد الرابع، جويلية 2017.

8.عبد القادر فلاح، نادية ايت عبد المالك، التحقيق الجنائي للجرائم الإلكترونية واثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، المجلد04، العدد02، جانفي 2020.

9.عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد04، جانفي 2018.

10.وردة شرف الدين، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة المفكر، جامعة محمد خيضر، بسكرة، العدد15، جوان 2017.

سادسا: المعاجم والقواميس

1. عبد الهادي ثابت، اللسان العربي الصغير قاموس عربي، دار الهداية، الجزائر، 2001.

قائمة المحتويات

قائمة المحتويات.

ملخص:

مكافحة جريمة القرصنة الإلكترونية في التشريع الجزائري:

القرصنة الإلكترونية جريمة تتمثل في الدخول أو البقاء غير المشروع داخل نظام معلوماتي بهدف الإضرار أو تدمير البيانات. من خصائصها السرية، البعد الجغرافي، وصعوبة تتبع الفاعلين. الجاني عادة ذكي وذو خبرة تقنية عالية، تشمل دوافع القرصنة الكسب المالي، التخريب والانتقام، وتأخذ صورًا متعددة مثل الدخول أو البقاء غير المصرح به أو إدخال أو إزالة معطيات. تعتمد التحقيقات على أساليب تقليدية وحديثة مثل الخبرة الفنية والتفتيش، التسرب واعتراض المراسلات. وتشمل وسائل التحقيق القانونية مراقبة الشبكات، وفحص الأجهزة بإذن قضائي. يعاقب القانون على هذه الأفعال بالسجن والغرامات، وتتم مكافحتها وطنيًا بتشريعات داخلية وتكوين فرق ومراكز متخصصة، ودوليًا عبر التعاون الأمني وتبادل المعلومات بموجب اتفاقيات مثل اتفاقية بودابست والاتفاقية العربية لمكافحة

الكلمات المفتاحية: القرصنة، الالكترونية، الجريمة، المكافحة، التشريع الجزائري.

Abstract

Combating Cybercrime in Algerian Legislation

Cybercrime, specifically hacking, is the illegal access or unauthorized presence in an information system with the intent to damage or destroy data. Its characteristics include secrecy, geographic distance, and difficulty tracing the perpetrators. Hackers are usually intelligent and highly skilled technically,the motives behind hacking include financial gain, sabotage, and revenge. It takes various forms such as unauthorized access, remaining in systems without permission, or inserting and deleting data,Investigations rely on both traditional and modern methods like technical expertise, inspections, data leaks, and intercepting communications. Legal investigative tools include network monitoring and device examinations under judicial authorization, Laws punish these crimes with imprisonment and fines. Nationally, combating hacking involves cybersecurity legislation and specialized teams, while internationally, it requires security cooperation and information exchange under agreements like the Budapest Convention and the Arab Convention against Cybercrime.

Keywords: Hacking, Cybercrime, Electronic Crime, Combating, Algerian Legislation.