وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق

التخصص: قانون الإعلام آلي والانترنت

الموسومة بعنوان:

آليات مكافحة الجرائم الالكترونية في التشريع الجزائري

من إعداد الطالبتين:
– عزة خولة
– ربيع شيماء

تحت إشراف الدكتور:
– نجار أمين

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة	الصفة
عشاش حمزة	أستاذ محاضر – ب –	رئيسا
نجار أمين	أستاذ محاضر – أ –	مشرفا
سي حمدي عبد المؤمن	أستاذ محاضر – أ –	مناقشا

السنة الجامعية: 2023-2024

بسم الله الرحمن الرحيم
١٤٣٨

شكر وعرفان

الحمد لله الذي بنعمته تتم الصالحات.

كل الشكر والتقدير والامتنان إلى أستاذنا "نجار آمين"، نسأل الله تعالى أن يجزيه كل الخير ويديم عليه الصحة والعافية على كل الجهود والتوجيهات التي قدمها لنا حتى زالت العقبات والصعاب

تشكراتنا إلى كل من علمنا حرفا منذ نعومة أظافرنا "أساتذتنا الفضلاء" لهم منا كل الاحترام والتقدير.

وكل الشكر إلى الأساتذة المحترمين الذين تفضلوا بمناقشة عملنا المتواضع.

إهداء

إلى من جعل الجنة تحت أقدامها وسهلت لي الشدائد بدعائها إلى الإنسانة العظيمة التي لا طالما تمنت أن تقر عينها لرؤيتي في يوم كهذا أمي العزيزة.

إلى من كلل العرق جبينه ومن علمني أن النجاح لا يأتي إلا بالصبر والإصرار إلى النور الذي أنار دربي والسراج الذي لا ينطفئ نوره بقلبي من استمديت منه قوتي واعتزازي بذاتي والدي العزيز.

إلى ضلعي الثابت إلى من شددت عضدي بهم فكانوا لي ينابيع أرتوي منها إلى خيرة أيامي وصفوتها إلى قرة عيني أختي الوحيدة وخالاتي أطال الله بعمرهم.

لكل من كان عونا وسندا في هذا الطريق لصديقاتي ورفيقات دربي.

لمن اعتبرتها أختي الثانية فكانت خير رفيقة سندس الغالية.

أهديكم هذا الإنجاز وثمرة نجاحي الذي لطالما تمنيتها ها أنا اليوم أتممت وأكملت أول ثمراته بفضله سبحانه وتعالى فالحمد لله على ما وهبني.

خولة

إهداء

الحمد لله حبا وشكرا وامتنانا على البدء والختام.

(وآخر دعواهم أن الحمد لله رب العالمين).

بكل فخر أهدي هذا النجاح إلى:

إلى النور الذي أنار دربي والسراج الذي ينطفئ نوره أبدا والذي بذل جهد السنين من أجل أن أعتلي سلالم النجاح الذي أحمل اسمه بكل فخر: "أبي الغالي".

إلى من جعل الجنة تحت أقدامها إلى معنى الحياة وسر الوجود إلى من كان دعائها سر نجاحي إلى من رافقتني في كل مشاوير الحياة ولا تزال تفعل إلى الآن إلى قرة عيني "أمي العزيزة".

إلى ضلعي الثابت وأماني أيامي إلى من شددت عضدي بهم فكانوا لي ينابيع أرتوي منها إلى خيرة أيامي وصفوتها: "إخواني الغاليين ونساء إخواني".

إلى كل من كان عونا وسندا في هذا الطريق للأصدقاء الأوفياء.

لأصحاب الشدائد والأزمات إلى من أفاضني بمشاعره ونصائحه المخلصة إلى عائلتي المخلصة (أخوالي وخالاتي، أعمامي وعماتي)

وأخيرا من قال لها "نالها".

شيماء

مقدمة

ظهرت الجريمة مع ظهور المجتمع البشري، حيث تميز كل عصر بنظام قانوني يحدد الأفعال المجرمة ويحدد العقوبات المناسبة، إذ تمثل الجريمة كل نشاط يتعارض مع النظام والقانون والأعراف الاجتماعية. ومع التطور التكنولوجي وبالرغم من الإيجابيات الكثيرة لهذا التقدم الحاصل في العالم وما قدمه من اختراعات تخدم الإنسان في مختلف المجالات حيث أصبح من الصعب الاستغناء عن هذه الخدمات اللامحدودة التي أصبحت من ضروريات العصر الحالي إلا أن هذا التقدم حمل معه العديد من السلبيات فقد انتشرت في الآونة الأخيرة ظاهرة ما يعرف بالجريمة الإلكترونية بشكل كبير وذلك بسبب انتشار أجهزة الحاسب لآلي والهواتف الذكية المتصلة بشبكة الانترنت كما أن هذه الجريمة المستحدثة تختلف كثيرا عن الجريمة التقليدية في طبيعتها ومضمونها ونطاقها وكذا وسائلها، فقد أصبحت هذه الجرائم تشكل هاجسا لكثير من الدول باعتبارها من الجرائم المنظمة والعابرة للحدود الوطنية الأمر الذي دفع بالكثير منها لمحاولة التعامل مع هذه الظاهرة والحد منها وذلك عن طريق سن قوانين وتشريعات وطنية تجرم الأعمال الغير مشروعة التي تتم عن طريق شبكة الانترنت، وقد حاول المشرع الجزائري على وجه الخصوص التصدي لهذه الجرائم من خلال سن قانون 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بالإضافة إلى آليات تشريعية ومؤسساتية لمكافحة الجريمة الإلكترونية.

أهداف الدراسة:

- الجريمة الإلكترونية موضوع حديث ذو قيمة علمية في كافة مجالات الحياة العامة والخاصة يستدعي دراسته والبحث فيه.
- التعرف على الجريمة الإلكترونية.
- التعرف على الإجراءات والآليات المستجدة من قبل المشرع الجزائري للحد من هذه الجريمة.

أهمية الدراسة: يعد موضوع الجريمة الإلكترونية موضوع مهم جدا في عصرنا الحالي وذلك راجع للأسباب التالية:

- تساهم في فهم طبيعة هذه الجرائم وكيفية اكتشافها ومكافحتها.
- تمكننا من تطوير تقنيات وأدوات لحماية المعلومات الشخصية والبيانات الحساسة.
- تكمن أهمية دراسة هذا الموضوع في تقديم فكرة عامة للقارئ عن موضوع البحث العلمي وكذا تحديد الفوائد التي تعود على القارئ كفرد من أفراد المجتمع.

أسباب اختيار الموضوع:

الأسباب الذاتية: من أهم الأسباب الشخصية التي دفعتنا لاختبار هذا الموضوع ما يلي:

- الشغف وحب الاستطلاع على الجرائم وأنواعها.
- اهتمامنا بمعرفة كيفية التعامل مع هذه الجريمة من الناحية الإجرائية والقانونية.
- الجريمة الإلكترونية لها جانب من الغموض خصوصا من ناحية إطار مكافحتها.

الأسباب الموضوعية:

- الجريمة الإلكترونية موضوع حديث يمس الواقع الذي نعيش فيه.
- نظرا لتزايد استخدام التكنولوجيا في حياتنا يعني زيادة فرص ارتكاب الجريمة الإلكترونية.
- فهم هذه الجرائم وكيفية اكتشافها ومكافحتها مما يساعد في حماية أنفسنا ومجتمعنا من التهديدات الرقمية.

الدراسات السابقة:

- "آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري" مذكرة ماستر تخصص قانون الإعلام الآلي والانترنت، عقباش بريزة ومبارك حنان، جامعة محمد البشير الإبراهيمي 2022،2021.
- الغرض من هذه الدراسة التعرف على الآليات القانونية والمؤسساتية للوقاية من الجريمة الإلكترونية في التشريع الجزائري.
- اقتصرت إشكالية هذه الدراسة على كيف تصدى المشرع الجزائري لهذا النوع من الجرائم.

من ناحية الاستفادة التعرف على الجريمة الإلكترونية وآليات مكافحتها.

من ناحية الاختلاف أن موضوع دراستنا تضمن الآليات القانونية والمؤسساتية والتعاون الدولي لمواجهة الجريمة الإلكترونية إلا أنه في الدراسة السابقة لم يتطرقوا للتعاون الدولي القضائي للحد من هذه الجريمة.

الإشكالية:

- **ما مدى فعالية آليات الحد من الجريمة الإلكترونية و انتشارها؟**

صعوبات البحث: من الصعوبات التي وجهناها من خلال دراستنا لهذا الموضوع:

- صعوبة الحصول على المراجع.
- تناثر القوانين ذات الصلة.
- صعوبة الحصول على المعلومات في السلطة الأمنية.

منهج الدراسة: اعتمدنا في دراستنا لهذا الموضوع على المنهج الوصفي التحليلي من خلال التعريف بالجريمة الإلكترونية والمجرم الإلكتروني، وتحليل بعض النصوص القانونية العقابية التي سنها المشرع الجزائري للحد من هذه الجريمة.

للبحث عن هذه الدراسة اخترنا خطة اعتمدنا فيها على تقسيم البحث إلى ثلاث فصول:

الفصل التمهيدي بعنوان الإطار المفاهيمي للجريمة الإلكترونية تضمن مبحثين حيث شمل المبحث الأول ماهية الجريمة الإلكترونية.

والمبحث الثاني أركان وخصائص الجريمة الإلكترونية.

أما الفصل الأول تضمن الآليات التشريعية للوقاية من الجريمة الإلكترونية إذ تناولنا في المبحث الأول الآليات القانونية والمبحث الثاني تصنيفات الجريمة الإلكترونية والآليات الموضوعية لمكافحتها.

والفصل الثاني تحت عنوان الآليات المؤسساتية والتعاون الدولي لمواجهة الجريمة الإلكترونية، حيث شمل المبحث الأول الهياكل الخاصة لمواجهتها والمبحث الثاني التعاون الدولي القضائي لمواجهة هذه الجريمة..

الفصل التمهيدي:

الإطار المفاهيمي للجريمة الالكترونية.

تمهيد:

لقد أصبحت الجرائم المعلوماتية من أخطر الجرائم في عصرنا الحالي، وبعد أن تتعدى حدود الكمبيوتر وتؤثر على حياتنا عبر الانترنيت[1]، كما أن الجرائم الالكترونية لها خطورة كبيرة على الحق في الخصوصية والأمان الشخصي وتؤثر على سيادة الدول وتزيد فقدان الثقة في التقنية، كما تهدد إيداع العقل البشري، فمن المهم فهم طبيعة هذه الجرائم ومخاطرها والخسائر التي تسببها، بالإضافة إلى انه يجب التعرف على ملامح المرتكبين ودوافعهم لذلك، فان إدراك هذه الأمور ضروري التعامل بأمان مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والاجتماعية والثقافية وكذا الأمنية[2]، ومن ثم قسمنا هذا الفصل إلى مبحثين، فقد تناولنا في المبحث الأول (ماهية الجريمة الالكترونية)، وخصصنا المبحث الثاني للحديث عن (أركان وخصائص الجريمة الالكترونية).

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2007، ص1.

[2] https://www.droiteentreprise.com.

مطماطي راوية، الجريمة الإلكترونية في التشريع الجزائرين2024/05/3، 22:55.

المبحث الأول: ماهية الجريمة الالكترونية:

لقد شهدت أنماط الجريمة تطورا كبيرا في العصر الحديث، فلم يعد الاعتداء يستهدف أشخاص والممتلكات فحسب بل أصبح هناك اهتمام أكبر بالاعتداء على المعلومات، يعرف هذا النوع من الجرائم على الساحة الدولية بجرائم "ذوي الياقات البيضاء" أن المجرمون العصريون يشتغلون التكنولوجيا لارتكاب جرائمهم دون اللجوء إلى العنف الجسدي أو إراقة الدماء أو حتى الانتقال من أماكنهم، بل ترتكب هذه الجرائم في أمن وهدوء دون إثارة الشبهات مما جعل البعض يصفها بالجرائم الناعمة (SOFT CRIME)، فبمجرد لمس لوحة المفاتيح يحدث دمارا وخرابا في اقتصاديات كبرى كالشركات، وهذا النوع من الجرائم ليس مقصورا على منطقة ودولة معينة لكنها تعتبر مشكلة عالمية[1] انطلاقا من هذا لنا أن نتطرق إلى المطلبين الآتيين:

المطلب الأول: تعريف الجريمة الالكترونية:

إن عصر انتشار تكنولوجيا المعلومات قد تكون فيه أكثر عرضة للوقوع كضحايا للجرائم الالكترونية فانتشار هذه التكنولوجيا قد يسهل علينا الاتصال حول العالم من أجل قريب المسافات بين الدول والحضارات كما يمكن استخدام هذه التكنولوجيا في التسبب لأضرار وسلبيات لأشخاص أو مؤسسات بغرض تحقيق أهداف سياسية أو مادية أو شخصية.[2]

لم يتوصل الباحثون والدارسون والتشريعات إلى تعريف موحد للجريمة الالكترونية وعناصرها الأساسية وهذا ما يفسر تعدد التسميات التي أطلقت عليها فالبعض أطبق عليها اسم الجريمة الالكترونية والبعض تسمية جرائم الانترنت وجرائم الكمبيوتر وأطلق عليها آخرون في تسميتها بجرائم المعالجة الآلية للبيانات والمعطيات.[3]

هناك العديد من التعريفات المختلفة التي قدمها الفقهاء لهذا النوع من الجرائم، وبالمقارنة مع التعريف العام للجرائم العادية ويمكن تحديد مفهوم الالكترونية بأنها : أي فعل أو امتناع غير مشروع يهدد بالخطر أو ينذر بضرر ،و يستخدم الانترنت أو أي جهاز الكتروني كوسيلة لارتكابه

---

[1] بونعارة ياسمينة، الجريمة الالكترونية، مجلة المعيار، مجلد20، عدد 39، 2015، ص275.

[2] www.it-pillars.com. الجرائم الالكترونية أنواعها وكيفية تنفيذها وطرق مواجهتها. 21-04-2024,12 ;49.

[3] د. شوقي يعيش تمام، الجريمة المعلوماتية، الطبعة الأولى، سلسلة مطبوعات المخبر، الجزائر، 2019، ص18.

سواء على الجهاز نفسه أو على جهاز آخر ويتم تعيين عقوبة قانونية أو تدبير احترازي لهذا النوع من الجرائم وفقا لقانون العقوبات العام.[1]

الفرع الأول: الاتجاه الموسع لتعريف الجريمة الالكترونية:

قد تكون التعاريف السابقة غير شاملة لجوانب ظاهرة الجريمة الالكترونية، بعضها يركز على وسائل ارتكابها، وهذا يؤدي بالضرورة إلى توسيع نطاق فهم الجريمة الالكترونية تشمل العديد من الجرائم ذات الصلة بالمعلوماتية مثل سرقة الأجهزة الحاسوبية والأقراص أو الأسطوانات، ولأن الجريمة الالكترونية تقع على المكونات غير المادية (البرامج والمعطيات) أما المكونات المادية للحاسب لا تختلف في ذلك عن الأموال الأخرى وبالتالي فالجرائم التي تقع عليها هي جرائم تقليدية ونفس الشيء بالنسبة للجرائم التي يكون للحاسب دور ثانوي في المساعدة على ارتكابها.

كما أن الوسيلة المستخدمة في ارتكاب الجريمة ليست جزءا من تعريف الجريمة الالكترونية وأيضا التركيز على الفاعل ومعرفة التقنية ليس معيارا مناسبا لتعريف الجريمة الالكترونية حيث أنها تحددت بدون وجود معرفة تقنية لدى الجاني، إذ يمكن ارتكاب هذه الجريمة دون أن يكون للجاني أي خبرة أو دراية بمجال المعلوماتية فإرسال رسالة تحمل فيروسا لشخص معين لا تتطلب إلا معرفة محدودة أو بسيطة وكذا الاتجار في برامج ترتكب بها جرائم الكمبيوتر فهذا الأمر لا يتطلب المعرفة بتقنية المعلوماتية.[2] على رأسهما الفقيهات (CERDI/MICHEL) قد قاموا بتوسيع مفهوم الجريمة الالكترونية ليشمل استخدام الحاسوب كأداة لارتكاب الجريمة بالإضافة إلى حالات الولوج غير مصرح به لحاسوب المجني عليه أو بياناته، كما أن الجريمة الالكترونية تشمل أيضا الاعتداءات المادية على الحواسب والمعدات المتصلة بها بالإضافة إلى ذلك تشمل استخداما غير مشروع لبطاقات الائتمان وانتهاكا لماكينات الحسابات الآتية. بما يتضمنه من شبكات تمويل

[1] عالية سمير، الجرائم الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2020، ص68 ص69.

[2] د. باطلي غنية، الجريمة الالكترونية، منشورات الدار الجزائرية، الجزائر، 2015، ص 18 ص19.

الحسابات المالية بطريقة الكترونية وتزييف المكونات المادية والمعنوية للحاسوب بل وسرقة الحاسوب في حد ذاته أو مكون من مكوناته[1].

الفرع الثاني: الاتجاه الضيق لتعريف الجريمة الالكترونية:

قام أنصار هذا الاتجاه بحصر مفهوم الجريمة الالكترونية باستخدام معايير مختلفة سواء كانت وفقا لمعيار شخصي يعتمد على المعرفة والخبرة التقنية أو وفقا لمعيار الموضوع والمعايير المتعلقة بالبيئة التي تم فيها ارتكاب الجريمة.[2]

وتوجد العديد من التعريفات للجريمة الالكترونية وفقا لهذا الاتجاه فهي تعتبر أنها: "كل فعل غير قانوني يتطلب المعرفة بتكنولوجيا الكمبيوتر بشكل كبير لازما لارتكابه ومتابعته ويتم تحديد هذا التعريف بواسطة وسيلة ارتكاب الجريمة والتي هي الكمبيوتر معتبرا إياها بأنها فعل غير مشروع كما تعرف بأنها "هي التي تحدث على جهاز الكمبيوتر أو داخل نظامه"، وقد اعتمد هذا التعريف أيضا على معيار وسيلة ارتكاب الجريمة التي تتمثل في الكمبيوتر، وتم تعريفها من قبل الفقيه الألماني تيدمان بأنها: "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب وعرفها الأستاذ جون فورسا بأنها: "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" إذن تشترك هذه التعريفات جميعها التي تخص الجريمة الالكترونية في المعيار المعتمد ألا وهو وسيلة ارتكابها المتمثلة في الكمبيوتر.

بينما آخذ البعض الآخر من أنصار هذا الاتجاه بمعيار النتيجة، وذلك من خلال تعريف الأستاذ الفرنسي ماس للجريمة الالكترونية بأنها: "تلك الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح" بين هذا التعريف أن الغاية من الجريمة المعلوماتية مادية وهي تحقيق الربح وبذلك يكون قد ركز على معيار النتيجة، وعرفها الفقيه روزملات على أنها نشاط غير مشروع موجه للنسخ أو الوصول إلى المعلومات بطريقة غير مشروعة وكذا معيار وسيلة

[1] بوبعاية ابتسام، التحقيق في الجريمة الالكترونية، مذكرة ماستر، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021-2022، ص9 ص10.

[2] مقلاتي مونة مشري راضية، الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، المجلد 6 العدد 01، 2021، ص493.

ارتكاب هذه الجريمة ألا وهي الحاسوب كما عرفها بأنها: "أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب" وقريبا من ذلك عرفت بأنها: "أي فعل غير مشروع تكون المعرفة بتقنية أساسية لمرتكبه..

تشير الجرائم الإلكترونية إلى جميع الجرائم الجنائية التي يحتمل ارتكابها على أو من خلال نظام كمبيوتر متصل بشكل عام بشبكة الإنترنت، حيث أن الجريمة الإلكترونية هي أي سلوك غير قانوني أو غير أخلاقي أو غير مصرح به يتضمن معالجة أو نقل البيانات تلقائيا. [1]

الفرع الثالث: التعريف القانوني للجريمة الالكترونية:

قام المشرع الجزائري بتعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على أنها: تتضمن المساس بأنظمة المعالجة الآلية للبيانات المحددة في قانون العقوبات، بالإضافة إلى أي جريمة أخرى ترتكب أو يكون من السهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية وبهذا التعريف يجمع المشرع الجزائري بين الحالات التي تكون فيها النظم المعلوماتية وشبكات الاتصال موضوعا للجريمة وبينها كوسيلة أو دعامة للجرائم التقليدية ويلاحظ انه لولا هذه النظم المعلوماتية وشبكات الاتصال لما كان للجرائم هذه الصفة المعلوماتية على هذه الجرائم على عكس المشرع الفرنسي لم يعطي أي تعريف للجريمة الالكترونية.

كما قام المشرع الجزائري بتسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب المادة الثانية من القانون 09-04 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.[2]

---

[1] بوجادي صليحة، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، مجلد 7، العدد 01، 2021، ص 2528، ص2529.

- Sam lyes,la criminalité électronique et son impact sur la sécurité nationale et la sécurité du citoyen , strategia revue des études de défense et de prospective , numéro 16, 2021, page 27

[2] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة أستاذ الباحث للدراسات القانونية والسياسية، مجلد 3، العدد 11، 2018، ص352.

كما عرفت الجريمة الالكترونية من قانونيا أنه: كل نشاط غير ينتج عن إرادة الجاني ويقرر القانون لها عقوبة أو تصرف قانوني.[1]

المطلب الثاني: أطراف الجريمة الالكترونية:

يختلف أطراف الجريمة الالكترونية نوعا ما عن باقي أنواع الجرائم حيث تحتاج إلى طرفين فاعل أو جاني و مجني عليه.[2]

بالإضافة إلى النيابة العامة التي تمثل الحق العام إذ أن تشكيل الجريمة ينحصر في الأطراف الثلاثة باستثناء حالة مشاركة أطراف آخرين مع الجاني حيث يدخلون في هذه الدائرة مع الجاني والمجني عليه.[3]

الفرع الأول: الجاني في الجريمة الالكترونية:

إن ارتباط الجريمة الالكترونية بالحاسوب يساهم في تمييزها عن الجرائم التقليدية وأيضا في تمييز المجرم المعلوماتي عن غيره من المجرمين العاديين[4] ويمكن تقسيمهم إلى:

الهاكرز: هم أشخاص يتمتعون بمعرفة عالية في مجال التقنية المعلوماتية ويستخدمونه لإنشاء وتعديل البرمجيات والأجهزة، وغالبا ما يكون شبابنا مهتمين بالمعلوماتية وقدراتهم الغنية، والباعث الأصلي لدى الهاكرز هو الاستمتاع باللعب والمزاح باستخدام هذه التقنية لإثبات قدراتهم باكتشاف مواطن الضعف في الأنظمة المعلوماتية دون إلحاق الضرر بها.

الكراكز: وهم المخترقون سواء كانوا محترفين أو هواة، وغالبا ما يقوم مجرمو هذا النمط باستخدام قدراتهم الفنية في الاختراق تحقيقا لأهداف غير شرعية كالقيام بأعمال تخريبية والحصول على معلومات سرية، وتتمثل هذه الطائفة في الشباب الذين تجاوز عمرهم الخامسة والعشرون عاما ويتميزون بالتخصص الغالي في مجال الحاسب الآلي والمعرفة التقنية والذكاء.

---

[1] ابن الضب ،فاطنة حبي فتيحة، الآليات المستحدثة للحد من الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر، جامعة غرداية، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012، 2019، ص10.

[2] أشخاص الجريمة المعلوماتية، علي أحمد الزغبي، 2020/04/20، https://almerja.net.reading.23:35

[3] عباد الحلبي خالد، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2011، ص31.

[4] المعلوماتي: تصنيفات متنوعة ومهارات مختلفة، عبد العال، 20/04/23:05,2024,المجرمhttps://accronline.com

ويصنفون كأخطر مرتكبي الجرائم الالكترونية وقراصنة هذا المجتمع من ذوي الحالة الاجتماعية العادية أو المتخصصين في العلوم الالكترونية[1].

الفرع الثاني: المجني عليه في الجريمة الالكترونية:

إن تنوع أصناف المجرمين المعلوماتيين يؤدي إلى تعدد أصناف الضحايا ويمكن أن يكون الضحية فردا عاديا في المجتمع أو مؤسسة اقتصادية كشركات التأمين، ومن الأخطر أن تكون الضحية دولة أو مؤسسات عسكرية من خلال عمليات التجسس، لذلك يجب أن يكون هناك اهتمام خاص بالوقاية من جرائم التكنولوجيا واتخاذ إجراءات لحماية الأفراد والمؤسسات في الجزائر وقد تم اعتماد إجراءات خاصة للوقاية منها أي إجراء مراقبة الاتصالات الالكترونية بإعتبارها إجراءا وقائيا.

في إطار الضبط الإداري وهذا بموجب 04 من القانون 09-04 فإن الضحية في الجريمة الالكترونية وفي الجريمة بصفة عامة قد يكون شخصا طبيعيا أو معنويا إنتهك حق من حقوقه المحمية قانونيا فلحقه جزاء ذلك ضرر معنوي أو مادي.[2]

وقد يصعب تحديد الضحايا في الجرائم الالكترونية بدقة لأن المجرمين غالبا ما يكونون غير معرفين بهدف الجرائم حتى تحدث بالفعل، وعادة ما يكونون غير راغبين في الاعتراف بأن نظامهم المعلوماتي تعرض لانتهاك م، وهذا السلوك السلبي قد يكون مغريا لمرتكبي هذه الجرائم للاستمرار في نشاطهم.[3]

وفي الجرائم الالكترونية يختلف المجني عليه أو الضحية عن المجني عليه في الجرائم التقليدية في اتخاذهم دورا سلبيا أكثر أمام تكتم الكثيرين وخوفهم على سمعتهم وبالتالي يترددون في

---

[1] بن عطية خيرة، الجريمة الالكترونية خصائصها وأهدافها، الجريمة الالكترونية وحجب الدليل الرقمي في الإثبات الجنائي، الطبعة الأولى، المركز المغاربي شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة بريطانيا، 2024، ص74.

-Nassima Azizi,ibtissem khedri , cybercriminalité un fléau planétaire, Revue diaa des etudes juridique, volume 01, numéro 01,2020,page 6

[2] بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة ماستر، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021-2022، ص17.

[3] الشمري غانم مرضي، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الدار العلمية للنشر والتوزيع، عمان-الأردن، 2016، ص32.

الإبلاغ عن الجريمة، وفي حالة كون المجني عليه والضحية مؤسسة اقتصادية تجارية فمن المؤكد أنها لن تكشف عن نفسها في حالة اختراق موقعها الالكتروني لوجود ثغرة أمنية أو سرقة كلمات السر أو فك التشفير وغيرها من أساليب ارتكاب الجريمة ولن يقوم بذلك حتى مقدم الخدمات إلا في حالات معينة التي تعفيه من المسؤولية القانونية.[1]

المبحث الثاني: أركان وخصائص الجريمة الالكترونية:

من خلال هذا المبحث سنحاول التعرض إلى الأركان التي ترتكز عليها الجريمة الالكترونية وكذا استعراض أهم الخصائص التي تتميز بها كل من الجريمة الالكترونية والمجرم الالكتروني.

المطلب الأول: أركان الجريمة الالكترونية:

يشترط لقيام الجريمة المعلوماتية ثلاث أركان المعلوفة للجريمة التقليدية وهذا ما سنبينه من خلال هذا المطلب بتفصيل الأركان الثلاثة لهذه الجريمة والمتمثلة في: الركن الشرعي، الركن المادي، الركن المعنوي.

الفرع الأول: الركن الشرعي:

يعني وجود نص قانوني يجرم هذا الفعل ويدينه ولا يمكن ملاحقة الفاعل بعد إلغاء النص، كما لا يمكن التوسع في تفسيره بل يجب الالتزام به من طرف القاضي عملا بمبدأ رجعية القوانين بنص صريح، فقد تم دمج الجريمة الالكترونية في القوانين العادية عن طريق تكييف النصوص القديمة مع هذه الجرائم الحديثة وهناك من وضع نصوص جديدة للتعامل مع هذه الجرائم.[2]

الفرع الثاني: الركن المادي:

يتكون الركن المادي في الجريمة الالكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية أنه يمكن تحقق الركن المادي دون تحقق نتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها مثل: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل، يتخذ الركن المادي فر هذه الجريمة عدة صور بحسب كل فعل، إيجابي مرتكب

[1] بوديسة بجاد عبد الرؤوف، مرجع سابق، ص17ص18.

[2] عقباش بريزة، مبارك حنان، آليات مواجهة الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021-2022، ص23.

مثل: جريمة الإرهاب الالكتروني الركن المادي فيها هو إطلاق صفحات أو مواقع تدعو وتحرض على الانضمام لمثل هذه الجماعات.[1]

الفرع الثالث: الركن المعنوي:

الحالة النفسية والذهنية للفاعل عند ارتكابه للجريمة فعندما يكون الشخص متعمدا بارتكاب جريمة فإنه يخطط لها ويتخذ قرار متعمدا لارتكابها فهنا تعتبر جريمة مقصودة يتخذ ركنها صورة القصد الجنائي، أما إذا لم تكن نواياه متجهة نحو ارتكاب جريمة فتكون جريمته غير مقصودة ويتخذ ركنها صورة الخطأ وكلاهما القصد والخطأ صور الركن المعنوي.

بما أنه يجب التنويه أن الركن المعنوي يتحدد وقت ارتكاب الجريمة عكس المسؤولية الجنائية التي يتم البحث عنها بعد وقوع الجريمة لتحديد ما إذا كان الفاعل أهلا لتحملها.[2]

المطلب الثاني: خصائص الجريمة الالكترونية:

تتسم الجريمة الالكترونية بجملة من الخصائص لا تتوافر في الجريمة الكلاسيكية وكذلك الأمر بالنسبة لمرتكبيها حيث لهم عدة خصائص تميزهم عن المجرمين العاديين وهذا ما سنبينه في التالي:

الفرع الأول: السمات الخاصة بالجريمة الالكترونية:

تتميز الجريمة الالكترونية بالعديد من الخصائص التي تميزها عن غيرها من الجرائم التقليدية. أهم خصائصها ما يلي:

صعوبة اكتشاف الجريمة الالكترونية: فالجرائم الالكترونية تكون مستترة وخفية لأن الجاني يستخدم مهاراته الفنية لتنقية الجريمة كإرسال فيروسات وسرقة الأموال البيانات الخاصة أو إتلافها، بعد ارتكاب الجريمة الالكترونية يكون من الصعب إيجاد ثار لها ومعرفة الجاني وهذا الأمر يصعب مهمة المحققين في التعامل مع هذه الجرائم حيث يستخدم فيها وسائل فنية غير عادية

[1] طالة لامية، سلام كهينة، الجريمة الالكترونية بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلد 6، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 6، العدد2، 2020، ص9.

[2] بوزنون سعيدة، محاضرة في مقياس النظرية العامة للجريمة والعقوبة، موجهة لطلبة سنة الثانية حقوق، كلية الحقوق، جامعة الإخوة منتوري قسنطينة، 2021-2022، ص35.

تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها وفي كل الأحوال تحتاج مواجهة هذه الجرائم إلى خبرة فنية عالية متخصصة لإثباتها.[1]

- **الجريمة الالكترونية عابرة للحدود (الزمان والمكان):** يعني أن الجرائم الالكترونية تتجاوز الحدود الجغرافية لأي دولة ومع توسع شبكة الاتصالات العالمية أصبح بإمكان أي شخص من أي مكان في العالم القيام بأعمال إجرامية غير أجهزة الكمبيوتر حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر.

مع تطور تقنية المعلومات وتوسع استخدام الانترنت أصبح للمجرمين فرصة أكبر لاستغلال هذه التقنيات في ارتكاب جرائمهم وخرق القانون وبالتالي مسرح الجريمة الالكترونية أصبح عالميا فالمجرم يستطيع ارتكاب جريمته عن بعد دون الحاجة للتواجد المادي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء.[2]

- **جرائم هادئة:** الجرائم الالكترونية لا تحتاج إلى مجهود عضلي كالجرائم التقليدية بل تعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر وهذا ما يسمح بالمجرمين بتنفيذ جرائمهم بشكل متطور ومتسلسل، فالجرائم الالكترونية تعتمد على تعديل والتلاعب بالبيانات المخزنة في ذاكرة الحواسب وبالتالي يمكن للمجرمين تغيير أو حذف المعلومات أو البيانات للتستر على أنشطتهم الالكترونية.[3]

جرائم صعبة الإثبات: من الصعب إثبات الجريمة الالكترونية حيث يصعب تتبعها باكتشافها فهي لا تترك أثرا ماديا كالبصمات التي يمكن استخدامها في التحقيقات التقليدية، كما يتطلب تتبع الجرائم الالكترونية خبرة فنية متخصصة فالمحقق العادي قد يواجه صعوبة في التعامل مع تلك الجرائم بالإضافة إلى ذلك يقوم مرتكبو الجرائم

[1] رحموني محمد، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلد 16، مجلة الحقيقة، المجلد 16، العدد41، 2018، ص441.

[2] مرجع نفسه، ص442

[3] مرجع نفسه، ص 443

الالكترونية بتمويه أنشطتهم وتضليل الأدلة بغاية عدم التعرف عليهم لذلك يتطلب التحقيق في الجرائم الالكترونية فريقا متخصصا وتقنيات متقدمة لمواجهة تلك التحديات.[1]

الفرع الثاني: السمات الخاصة بالمجرم الالكتروني:

يتميز مرتكب الجريمة المعلوماتية بصفات خاصة تميزه عن غيره من مرتكبي الجرائم وذلك من حيث:

- **أنه إنسان اجتماعي:** المجرم الالكتروني لا يظهر نفسه على أنه عدواني بشكل مفرط في المجتمع يل يتوافق ويتكيف بشكل جيد مع البيئة المحيطة به فتزداد خطورته الإجرامية كلما زاد تكيفه الاجتماعي وتمكنه من إخفاء جوانب شخصيته الإجرامية.
- **أنه إنسان محترف وذكي:** المجرم المعلوماتي يستخدم طرقا مختلفة للتلاعب بالبيانات والبرامج الحاسوبية حيث يقوم بزرع الفيروسات واستخدام القنابل المنطقية أو الزمنية لكي يشل حركة النظام المعلوماتي ويجعله غير قادر على القيام بوظائفه الطبيعية.[2]
- **المجرم المعلوماتي مجرم متخصص:** لأنه تبين في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي وجود التخصص في هذا النوع فقط من الجرائم دون أن تكون لديه علاقة بنوع من الجرائم التقليدية مما يبين أن المجرم المعلوماتي هو مجرم متخصص في هذا المجال فقط.
- **المجرم المعلوماتي غير عنيف:** لا يلجأ للعنف بتاتا في تنفيذ جريمته لأنه تبع جريمة عن طريق الحيل لأنه مجرم يتمتع بالمهارة وأحيانا على درجة كبيرة من الثقافة والمستوى العلمي.[3]

[1] رحموني محمد، مرجع سابق، ص441، ص443.

[2] بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص41.

[3] شاين نوال، الجريمة الالكترونية في التشريع الجزائرين، مجلد 6، مجلة سوسيولوجيا، العدد 2، ص69.

الفصل الأول:

الآليات التشريعية للوقاية من الجريمة الالكترونية

تمهيد:

شهد العالم تحولا كبيرا نتيجة التطور التكنولوجي وتوسع استخدام الكمبيوتر والانترنت، فقد أصبحت هذه التكنولوجيا جزءا أساسيا من حياة الناس في جميع أنحاء العالم، وساهمت في تواصل الثقافات وتبادل المعلومات وتعزيز التواصل الاجتماعي، ومن خلال هذه التحول أصبحت المعلومة أكثر قوة وثروة وأصبح للناس الوعي بأهمية الاستفادة منها في تحقيق التقدم والتطور، وانشغالا بمخاطر احتمال استخدام الحاسوب وشبكة المعلومات في ارتكاب الجرائم الجنائية، وهي جرائم حديثة تقف حاجزا أمام تطور المجتمع على كامل الأصعدة.[1]

لذا كل دولة تسعى جاهدة لمحاربة جرائم الانترنت وحماية المعلومات الحساسة من الاختراق والاستغلال غير القانوني، كما تختلف الأساليب التي تستخدمها التشريعات في صياغة النصوص القانونية لمكافحة الجرائم المعلوماتية من دولة لأخرى، وقد أصبحت عملية مكافحة الجريمة المعلوماتية ضرورة حتمية يجب التصدي لها لاحتواء هذا النوع الجديد والخطير من الإجرام، ففي الجزائر قام القانون الجزائري بتعديل قوانين وإصدار قوانين عقابية جديدة أخرى تتصدى لمختلف أنواع الإجرام المعلوماتي الجديد.[2] وهذا ما سنحاول معالجته من خلال هذا الفصل حيث سنتطرق إلى الآليات القانونية والإجرائية لمكافحة الجريمة الإلكترونية (المبحث الأول) وتصنيفات الجريمة السيرانية والآليات الموضوعية لمكافحتها (المبحث الثاني):

[1] بقدار شيماء، آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني، مذكرة ماستر، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2023، ص42.

[2] بن جدو فاطمة الزهراء، كوكي حياة، آليات مكافحة الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر الجامعة الافرقية العقيد أحمد دراية أدرار، كلية العلوم الاجتماعية والإنسانية والإسلامية، قسم العلوم الإنسانية، 2022/2021، ص42.

المبحث الأول: الآليات القانونية والإجرائية لمكافحة الجريمة الالكترونية:

إن التشريعات القانونية هي الأساس في مكافحة الجريمة بغض النظر عن نوعها، فالدول تعمل جاهدة لوضع قوانين خاصة لمكافحة الجرائم الالكترونية، وقد كانت السويد من بين الدول الرائدة في تشريعات جديدة لمكافحة الجرائم الالكترونية.

تليها الولايات المتحدة الأمريكية بقانون خاص بحماية أنظمة الحاسب الآلي سنة 1976، وأتبعته بقوانين أخرى، كما قام المشرع الفرنسي بإصدار قانون خاص بالمعلوماتية والحقوق الشخصية سنة 1978.

وأعقب ذلك بإصدار مرسوم في أواخر سنة 1981 يتعلق بتحديد بعض المخالفات المرتبطة بجرائم المعلومات ثم أصدر في سنة 1988 قانونا لحماية نظم المعالجة الآلية للمعطيات والمعلومات، واتبع ذلك بتعديلات لقانون العقوبات وقوانين أخرى في هذا المجال كما قامت بريطانيا عام 1081 بإصدار قانون لمكافحة التزوير، عرفت من خلاله أداة التزوير ووسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق الالكترونية أو التقليدية أو أي طرق أخرى.

ولأن الجرائم الالكترونية تمس كافة الدول دون استثناء حرص المجلس الأوروبي على التصدي لها من خلال اتفاقية بودا بسبب الموقعة في 2001/11/23 والمتعلقة بالجرائم الكوني وذلك إيمانا من الدول الأعضاء في المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية.

ولنفس السبب حرصت الأمانة العامة لمجلس وزراء الداخلية للعرب على مكافحة هذه الجرائم بوضع إستراتيجية عربية تنبثق من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي اعتمدها مجلس وزراء الداخلية للعرب في القاهرة في دورته الحادية والثلاثين بتاريخ

21/12/2010 والتي كانت الجزائر من بين الموقعين عليها سنة 2014 لأن بداية المشرع الجزائري مع الجرائم الالكترونية كانت سنة 2004 من خلال تعديله و تتميمه لقانون العقوبات.[1]

المطلب الأول: القواعد الإجرائية المقررة وفقا لقانون الإجراءات الجزائية:

لقد أدرك المشرع الجزائري أنه لا يكفي فقط وضع قواعده قانونية موضوعية ذات طبيعة ردعية فقط لمواجهة الإجرام الالكتروني، بل يجب أيضا وجود قواعد إجرائية وقائية وتحفيظية تساعد في تجنب وقوع الجريمة الالكترونية وهو ما استدركه بتضمين القانون رقم 2206 المعدل لقانون الإجراءات الجزائية تدابير جديدة تتعلق بالتحقيق في الجرائم الإلكترونية.[2]

وهذا ما سنتطرق إليه في الفرعين الآتيين:

الفرع الأول: الاختصاص والتسرب:

أولا: التسرب: لغة: مشتق من الفعل تسرب أي اندس ودخل خفية بطريقة أو بأخرى إلى مكان أو جماعة.

كما يعد التسرب أو الاختراق تقنية جديدة قام المشرع بإدراجها في تعديل قانون الإجراءات الجزائية وذلك بناءا على ضرورة التحقيق والتحري في الجرائم المذكورة في المادة 65، ويسمح لوكيل الجمهورية بمباشرة عملية التسرب تحت رقابته ضمن شروط محددة.

ويعتبر التسرب تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط الشرطة القضائية آخر مكلف

[1] شنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة دكتوراه، جامعة أحمد دراية بأدرار، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021/2020، ص41 ص 42.

[2] جمال شريف، عبد العزيز زقرار، آليات مواجهة الجرائم السيبيرانية في الجزائر، مذكرة ماستر، جامعة محمد البشير الابراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2023/2022، ص09.

بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية وذلك بإخفاء الهوية الحقيقية ويقدم المتسرب نفسه على أنه فاعل أو شريك معهم.

والتعريف القانوني للتسرب أخذه المشرع الجزائري في المادة 65 مكرر 12 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 على أنه: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم".[1]

ثانيا: الطبيعة القانونية للتسرب:

تلجأ السلطة القضائية المتمثلة في وكيل الجمهورية أو قاضي التحقيق إلى تقنية التسرب إذا اقتضت ضرورة التحري في الجرائم السنة المذكورة المعروفة بخطورتها وطبيعتها الخاصة يكون هدفها في تحقيق الربح الغير المشروع.

وتكون بتقديم إذن أو رخصة لمباشرة عملية التسرب داخل هذه الجماعة الإجرامية إلى ضابط عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية ضمن الشروط المحددة.

ويعد التسرب آلية مستحدثة في البحث عن الدليل الجنائي في جرائم أقل ما يمكن أن نقول عنها أنها جرائم معقدة وخطيرة ولها امتداد دولي في شكل خلايا إجرامية منظمة، ويصعب الحصول فيها على أدلة كافية لتحريك الدعوى العمومية بشأنها. والاكتفاء بطرق البحث التقليدية ستكفل جهات التحقيق وتجعل من المستحيل عليها أن تحصل على براهين جازمة للكشف عن الوقائع وماديات الجرائم ونسبتها إلى مرتكبيها مما يؤدي إلى إفلات المجرمين من العقاب.

كما يتمتع القاضي الجزائي بسلطة تقديرية في تقدير الوقائع وطرح الأدلة للمناقشة وتقديرها، هذا يساعده على بناء قناعته الشخصية حول الحكم الصادر بشأن الجريمة المعينة، وبما

[1] زوزو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، مجلد 6، العدد 11، 2014، ص117.

أن استخدام الحيل والأساليب الخادعة يمكن أن يثير الشكوك ويكون غامضا في بعض الأحيان، فإن قانون الوقاية يهدف إلى ضمان نزاهة وشفافية العون أو الضابط في أداء واجبها فقد تضمنت المادة 56 من قانون الوقاية والفساد ومكافحته رقم 06-01 ينصها:... وتكون الأدلة المتوصل إليها بهذه الأساليب حجيتها وفقا للتشريع والتنظيم المعمول بهما."[1]

ثالثا: شروط التسرب:

لكي يتم التوفيق بين المصلحة العامة في كشف الحقيقة وحماية الحق في الخصوصية يشترط قانون الإجراءات الجزائية الامتثال لبعض الشروط تتمثل في:

الشروط الشكلية: إن قانون الإجراءات الجزائية يحتوي على شروط شكلية لضمان الحفاظ على حقوق الأفراد والخصوصية وهي كالآتي:[2]

- **الإذن القضائي:** يجب أن يتوفر إذن من وكيل الجمهورية المختص أو قاضي التحقيق لتنفيذ عملية التسرب، بدون هذا الإذن القضائي لا يجوز لضابط الشرطة القضائية القيام بالعملية، ويجب أن يكون الإذن مكتوبا بشكل صريح وواضح إذا تم تنفيذ هذه العملية دون هذا الإذن، فانه يعتبر غير قانوني ومن الممكن أن يؤدي إلى بطلان الإجراء طبقا لنص المادة 65 مكرر 15 من قانون الإجراءات الجزائية.
- المدة المطلوبة لعملية التسرب التي لا تتجاوز أربعة أشهر ويمكن تجديدها حسب المقتضيات والظروف إلى أربعة أشهر أخرى طبقا لنص المادة 65 مكرر 15 ق-إ-ج ويجوز للقاضي الذي رخص بإجرائها أن يأمر بوقفها في أي وقت قبل انقضاء المدة المحددة.

[1] لصلج نوال، غزيوي هندة، التسرب كآلية من آليات البحث عن الدليل الجنائي في التشريعات الجنائية المعاصرة، مجلة البيان للدراسة القانونية والسياسية، مجلد 03، العدد 02، 2018، ص121،ص122.

[2] شنين صالح، التسرب في قانون الإجراءات الجنائية الجزائري حماية النظام العام والحريات أم حماية النظام العام، المجلة الجزائرية للقانون المقارن، مجلد 1، العدد02، 2015، ص123.

- إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية الانتهاء من العملية حفاظا على السرية المطلوبة التي حصرها المشرع بين القاضي الأمر بها (وكيل الجمهورية أو قاضي التحقيق) وضابط الشرطة القضائية المشرف على العملية وكذا العون والمتسرب.
- تحرير محضر يتضمن تقرير عن العناصر الضرورية لمعاينة الجرائم والظروف التي تمت فيها العملية وكذا جميع متطلباتها.
- صفة الضابط المسخر لهذه العملية حيث نصت المادة 65 مكرر 12 ق-إ-ج على من لهم الحق في القيام بعملية التسرب وهم ضباط وكذا أعوان الشرطة القضائية وكذا الأشخاص المسخرين لذلك في المادة 65 مكرر 14 ق.إ.ج.[1]

الشروط الموضوعية: تتمثل في شرطين أساسيين هما التسبب ونوع الجرائم المرتكبة:

- **التسبب:** يعتبر التسبب أمرا مهما جدا لذا يجب على الهيئات القضائية مثل وكيل الجمهورية المختص أو قاضي التحقيق أن يحصلوا على إذن قبل تنفيذ عملية التسرب وإلا فإن ذلك يؤدي إلى بطلان وشرعية الإجراءات، ويجب أن يتم ذكر الجريمة التي تبرر اللجوء إلى عملية التسرب.
- **نوع الجريمة:** اشترط المشرع في اللجوء إلى أسلوب التسرب ارتكاب جرائم معينة محصورة في المادة 65 مكرر 05 من ق.إ.ج وهي: جرائم المخدرات، جرائم الفساد وكذا جرائم المعالجة الآلية للمعطيات، جرائم الإرهاب والتخريب والجرائم الماسة بتشريع الصرف وكذا الجرائم العابرة للحدود الوطنية.[2]

رابعا: آثار التسرب:

عندما تنتهي عملية التسرب تستطيع جهات البحث والتحري من الوقوف على التفاصيل الأساسية لارتكاب الجرائم وتحرير محاضر تشكل أدلة تدعم الدعوى وتكشف الحقيقة في بؤر

[1] لصلج نوال، غزيوي هندة، مرجع سابق، ص 122، ص 123

[2] مرجع نفسه، ص 122،ص123

الإجرام وداخل العصابات، وكذلك تعرض أمام جهات الحكم، التي تحتفظ بحرية تقديرها المحاضر المحررة بطرق احترمت فيها الشروط الشكلية والموضوعية، وأي مخالفة لهذه الشروط تؤدي إلى تهدير ما يترتب عليها، كما تقدم شهادات شهود عيان للقاضي حيث قد خاطروا بأنفسهم للحصول على دليل قوي يدعم الدعوى، وهذا كله لتحقيق الهدف الأساسي من الدعوى العمومية تحديدا والإثبات الجنائي عموما المتمثل في البحث عن الحقيقة والكشف عنها.

ويمكن أن نشير إلى المخاطر التي يستطيع أن يتعرض إليها المتسرب بعد انتهاء عملية التسرب في حياته والتي يمكن أن تمتد إلى أفراد أسرته، وهنا قد وفر المشرع حماية لهؤلاء من خلال العقوبات المنصوص عليها في المادة 65 مكرر 16 من قانون الإجراءات الجنائية التي تنص على معاقبة كل شخص يكشف هوية ضباط الشرطة القضائية بالحبس من سنتين إلى 05 سنوات وبغرامة 50.000 إلى 200.000 دج وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أصولهم تكون العقوبة بالحبس من 05 إلى 10 سنوات وغرامة من 200.000 دج إلى 500.000 دح، وإذا تسبب الكشف في وفاة أحد هؤلاء الأشخاص تكون العقوبة بالحبس من 10 إلى 20 سنة والغرامة من 500.000 دج إلى 1000.000دج.

كما رتب المشرع حماية أخرى تتمثل في عدم تقديم العون المتسرب للإدلاء بشهادته شخصيا حفاظا على حياته، بل يقتصر الأمر على إدلاء ضابط الشرطة القضائية المكلف بتنسيق العملية وحده دون سواه بشهادته تحت مسؤوليته.[1]

الاختصاص:

إن المشرع الجزائري يسعى دائما لمواكبة التطورات الحديثة في مجال الجريمة والقانون يعمل على تحديث التشريعات لمكافحة الجرائم الحديثة ومواجهة التحديات الناشئة في هذا المجال،

[1] زوزو هدى، مرجع سابق، ص123.ص122.

سيما ما تعلق بالجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفي هذا الإتجاه جاء تعديل قانون الإجراءات الجزائية بموجب القانون رقم 04-014 المؤرخ في 10 نوفمبر 2004 ومس التعديل المادة 40 من قانون الإجراءات الجزائية لتصبح كما يلي:

"يتحدد اختصاص قاضي التحقيق محليا 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." كما يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

ومن الملاحظ أن تمديد الاختصاص المحلي لقاضي التحقيق مشمولا كما هو الشأن بالنسبة للنيابة بأحكام المرسوم التنفيذي رقم 06-343 المؤرخ في نص 2006/10/05 وقد حددت المادة الأولى من المرسوم المشار له مجال الاختصاص المحلي الممدد في نطاق الأقطاب القضائية السابق الإشارة إليها والمحدد في المواد 2،3،4،5 من نفس المرسوم في الجرائم المتعلقة بالمتاجرة في المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف وما يهمنا في الموضوع هو ما تعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

الفرع الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

من أهم الآليات التي اعتمدها المشرع الجزائري هي نظام اعتراض المراسلات وتسجيل الأصوات والتقاط الصور حيث بالرجوع لنص المادة 65 مكرر 05 من القانون رقم 06-22، والتي جاء فيها: "إذا اقتضت ضرورات التحري في الجريمة الملتبس بها، أو التحقيق الابتدائي في

[1] ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص114،ص115.

جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بالمعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية أن يأذن بما يلي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط الصور وتثبيت وبث وتسجيل الكلام المتفوه أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص...[1]

أولا: اعتراض المراسلات: عند استعراض نصوص قانون الإجراءات الجزائية يتضح أن المشرع لم يقم بإعطاء تعريف لهذا الإجراء بدلا من ذلك قام بتنظيم هذه العملية في المواد من 65 مكرر 05 إلى غاية المادة 65 مكرر 10 من قانون الإجراءات الجزائية، وترك تعريفها للفقهاء، ومن خلال نص المادة 65 مكرر 05 من نفس القانون يمكن فهم عملية إعتراض المراسلات بأنها: اعتراض أو نسخ أو تسجيل للمراسلات التي تتم عن طريق الوسائل السلكية واللاسلكية وتشمل هذه المراسلات بيانات قابلة للإنتاج والتوزيع والإستقبال والعرض والتخزين .[2]

كما يبقى هذا الإجراء مرهونا على توافر الشروط الآتية:

- الحصول على إذن مكتوب من الجهات القضائية المختصة، سواء كان ذلك من طرف وكيل الجمهورية في مرحلة التحقيق الإبتدائي أو من قاضي التحقيق في مرحلة التحقيق القضائي تحت طائلة بطلان الإجراء القضائي، يعتبر هذا الإذن لمراقبة المراسلات السلكية واللاسلكية بطرق غير معلنة للأطراف المعنية وعلى الرغم من فعاليته في الكشف عن الجرائم الإلكترونية إلا أنه يعتبر إنتهاكا لسرية المراسلات والإتصالات ومساس بحرمة الحياة الخاصة التي كفلها الدستور (20/442 المؤرخ في 30 ديسمبر 2020)، ويشترط أن يتضمن الإذن طبيعة

[1] بلواضح الطيب، الجريمة في الفضاء الإلكتروني، الطبعة الأولى، دار وائل للنشر والتوزيع، الأردن–عمان، 2020، ص178 ص179.

[2] مرجع نفسه، 177.

الجريمة التي تبرر الإجراء مع ضرورة أن تكون من الجرائم التي يجوز منح الإذن فيها، بالإضافة إلى تحديد المراسلات المراد اعتراضها وتسجيلها وتحديد الأماكن المقصودة، سواء كانت أماكن عامة أو خاصة مع تحديد مدة الاعتراض والتي لا تتجاوز 04 أشهر قابلة للتجديد

- التسبب: أي تبيان دواعي اللجوء إلى الاعتراض ومراقبة المراسلات وتبيان مدى جدية تلك الدواعي ودورها إظهار الجريمة والجناة.
- تحديد الجرائم محل الاعتراض والمراقبة والتي يتوجب أن لا تخرج عن ما هو مقرر قانونا مع مراعاة سرية الإجراءات وكتمان السر المهني.[1]

ثانيا: تسجيل الأصوات: ورد في نص المادة 56 مكرر 05 فقرة ثالثة من ق.إ.ج.ج عبارة تسجيل الأصوات ووفقا للنص المذكور أعلاه يقصد المشرع الجزائري بمصطلح الأصوات : الكلام المتفوه به بصفة سرية أو خاصة دون موافقة المعنيين من قبل شخص أو عدة أشخاص في أماكن خاصة أو عامة، كما عرف تسجيل الأصوات على أنه: تسجيل الأحاديث التي يتم عبر الهواتف بعد وضعها تحت المراقبة كما يتم أيضا عن طريق وضع ميكرفونات حساسة تستطيع التقاط أصوات وتسجيلها على أجهزة خاصة وقد يتم أيضا عن طريق التقاط إشارات سلكية أو لا سلكية.

وبالرجوع إلى النص الإجرائي السالف الذكر فالتسجيل الصوتي لا يقتصر فقط على التسجيل (enregtstrement) الكلام المتفوه به فحسب بل يشمل أيضا الالتقاط وتثبت وبث الكلام.

فتسجيل الكلام أو الحديث فهو حفظه على الشريط المخصص لذلك أو أي وسيلة أخرى ثم الاستماع إليه بعد ذلك.

[1] مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، مجلد 06، العدد 01، 2023، ص203 ,ص204.

أما التثبيت والبث فيقصد بالتثبيت وضع الكلام المتفوه به على دعامة إلكترونية أو مغناطيسية كما أن لفظ التثبيت يتعلق بالصورة أكثر من تعلقه بالصوت أما البث فيقصد به النقل من خلال النص الإجرائي المذكور المترجم إلى اللغة الفرنسية، أي نقل الحديث الذي تم الاستماع إليه أو تسجيله من المكان الذي تمت فيه إحدى الأفعال السابقة، أما فيما يخص الطبيعة القانونية لعملية التسجيل الصوتي فقد اختلفت الآراء حول ذلك فاعتبرها البعض أن لها علاقة كبيرة بعملية التفتيش حيث يهدف كلاهما للكشف عن حقيقة الجريمة المرتكبة، وكما أن محل مباشرة التسجيل الصوتي هو ذات المحل الذي ينصب عليه التفتيش لكن أوجه الاختلاف بينهما جوهريا، فالغرض من التفتيش هو ضبط الأدلة المادية المتعلقة بالجريمة أما الأحاديث الصوتية ليس لها مكان مادي يمكن ضبطه.

ويعتقد البعض الآخر أن عملية تسجيل الأصوات تنشأ ضبط الرسائل التي تتضمن حديث كتابي وإن التسجيلات الصوتية تتضمن حديث شفوي إلا أن هناك فرق واضح بين عملية ضبط الرسائل التي تتضمن حديث كتابي وإن التسجيلات الصوتية تتضمن حديث شفوي إلا أن هناك فرق واضح بين عملية ضبط الرسائل وتسجيل الأصوات تكمن في كون ضبط الرسائل تعتبر أدلة مادية إلا أن التسجيلات الصوتية ليست بأدلة مادية ولا يقبل بالضبط بالمعنى القانوني فالطبيعة القانونية للتسجيلات الصوتية تكمن في أنها إجراء من نوع خاص فهي مستقلة عن عملية التفتيش وكذلك عن ضبط الرسائل.[1]

ثالثا: التقاط الصور: يمكن أن نستخلص من المادة 65 من قانون الإجراءات الجزائية أن الترتيبات التقنية التي نصت عليها يمكن أن تستخدم لالتقاط صور لأشخاص في مكان خاص وقد استثنى نص المادة 65 التقاط الصور في الأماكن العمومية للأشخاص على عكس التقاط المكالمات الهاتفية، وقد سمح المشرع الجزائري بهذه التدابير في بعض القوانين الخاصة إذ نص

[1] مدرك نريمان، الآليات القانونية لمكافحة الجريمة الإلكترونية في ظل التشريع الجزائري، مذكرة ماستر، جامعة عبد الحميد بن باديس، مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2023، ص41-43.

على استعمال الترصد الإلكتروني والاختراق في المادة 56 من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته.[1]

هذا الإجراء يعرف بأنه: إخفاء أجهزة تصوير تكون صغيرة الحجم في أماكن سرية لأخذ صور تكشف الحقيقة وتسليمها.

أما بالنسبة لنص المادة 65 مكرر 05 المذكورة أعلاه نجد أن عبارة التقاط الصور جاء في الشكل الآتي:... وضع ترتيبات تعقبية... التقاط صور شخص أو عدة أشخاص يتواجدون في مكان خاص.

وبمفهوم نص المادة 65 مكرر 05 فقرة ثالثة، أن الصور المعنية بهذا النص هي تلك الملتقطة بالمكان الخاص، وبمفهوم المخالفة للنص الإجرائي الوارد أعلاه لا تخضع لأي ضبط من الضوابط المنصوص عليها بالمواد 65 مكرر 5 إلى 65 مكرر 10، كما أن مسألة التقاط الصور في المكان العام فجهاز الأمن يعتمد على أسلوب المراقبة عن طريق استخدام أجهزة التصوير في الطريق العامة بالمدن لمراقبة حركة المارة والسيارات وأماكن التجمعات فضلا عن تصوير المسيرات والمظاهرات ومن حيث الظاهر تكون غاية المراقبة واضحة وهي حفظ النظام العام وحمايته.[2]

المطلب الثاني: القواعد الإجرائية المقررة وفقا لقانون 09-04 المتعلق بالوقاية من تكنولوجيا الإعلام والاتصال ومكافحتها:

إن المشرع الجزائري لم يشيد عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، ومع ذلك قام بوضع قواعد جديدة تتعامل مع جرائم الانترنت كظاهرة حديثة تتطلب تطورا في المجال، وبهذا الصدد جاء القانون رقم 09-04 المؤرخ في 08/05 أوت 2009 المتضمن

[1] زبيحة زيدان، مرجع سابق، ص161.

[2] مدرك نريمان، مرجع سابق، ص 44، ص45.

القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومنها ما نصت عليها المادة 03 مما تتطلبه مستلزمات التحريات أو التحقيقات القضائية وهي وضع ترتيبات تقنية هدفها ما يلي:

- مراقبة الاتصالات الإلكترونية.
- تجميع تلك الاتصالات الإلكترونية.
- تسجيل الاتصالات الإلكترونية في حينها.
- القيام بإجراءات التفتيش للمنظومة المعلوماتية.
- القيام بإجراءات الحجز داخل المنظومة المعلوماتية.[1]

وهذا ما سنتطرق إليه في الفرعين الآتيين:

الفرع الأول: مراقبة الاتصالات الإلكترونية وتفتيش المنظومة المعلوماتية:

أولا: مراقبة الاتصالات الإلكترونية:

إن مراقبة للاتصالات هي عملية استخدام التقنية الإلكترونية من طرف المراقب لجمع البيانات والمعلومات للتحقيق في الجرائم والمشتبه بهم سواء كانوا شخصا أو مكانا أو شيئا، وتعد المراقبة الإلكترونية للاتصالات من أهم مصادر التحري وأسرع الطرق لكشف الجرائم الرقمية، مع أهمية التنويه إلى أن المراقبة الإلكترونية هي وسيلة لمكافحة الإجرام عبر الانترنت على المستوى الدولي.

وكما سبق أن نوهنا أن عملية المراقبة التقليدية قد لا تصلح لكشف الجريمة المعلوماتية وضبط مرتكبها والتحفظ على أدلتها لخصوصية الجرائم المتعلقة بالحاسب الآلي بصورة تستدعي تطوير أساليب المراقبة وذلك بالاستعانة بأجهزة التصنت والمراقبة الهاتفية والتصوير في الضوء والظلام والتصوير التلفزيوني وتحديد الاتجاهات والمواقع وتحليل المعلومات باستخدام الحاسب

[1] زبيحة زيدان، المرجع السابق، ص120.

الآلي والتقنية الإلكترونية وعبر شبكة الانترنت لاستنباط الأدلة، ليتمكن مأموري الضبط القضائي من كشف غموض الجريمة والتعرف إلى مرتكبيها، وفي العالم الافتراضي يجب أن تقتصر عملية المراقبة على من تتوافر فيهم الكفاءة العملية والخبرة الفنية في مجال الجرائم التقنية والقدرة على استرجاع المعلومات ممن تلقوا التدريب الكافي بكيفية التعامل مع برامج وملفات البيانات المخزنة بالحاسب وكذا كلمة السر والمرور اللازمين للدخول للنظام، حيث يجب أن يكون ذا ثقافة عالية تتجاوز المعرفة العامة أو السطحية من مأموري الضبط القضائي ومعاونيه من رجال السلطة العامة والمرشدين السريين وممن يتولون إبلاغه عما وقع بالفعل من جرائم، بشرط يحصل المراقب على إذن رسمي يتضمن رقم الحاسوب وصلاحيته للعمل وخلوه من العوائق التكنولوجية واحتواءه على برمجيات أصلية وليست منسوخة، فضلا على ذكر أرقامها المسلسلة ورقم وتاريخ الترخيص بها وجهة إصدارها لمباشرة مهامه في المراقبة عن الجرائم ومرتكبيها كما يجب توثيق نظام الحاسب الآلي ومعلومات تشغيله. ومراقبة المشتبه فيه الذي أساء استخدام مواقع الانترنت أو البريد الإلكتروني تكون من خلال مراقبة اتصالاته الإلكترونية أي تلك التي تتم عن طريق الانترنت بما في ذلك مراسلات البريد الإلكتروني.[1] و وفقا للقانون 09-04 و وفقا لما ذهبت إليه المادة 02 بند (و) يقصد بالإتصالات الإلكترونية : كل إرسال أو تراسل أو إستقبال صور، أصوات، إشارات، كتابات، علامات عن طريق الوسائط الإلكترونية."

كما تعرف في الفقه المقارن بأنها الاتصالات التي تتم عن طريق جهاز الحاسب الآلي، والتي تتخذ شكل البريد الإلكتروني أو شكل محادثة فورية والتي تتم عن طريق شبكة الانترنت.

وتأخذ الاتصالات الإلكترونية شكل محادثات شفوية أو مراسلات مكتوبة أو صور ملتقطة وهي تمثل بذلك أبرز العناصر الأساسية التي يقوم عليها الحق في حرمة الحياة الخاصة، ولهذا يعد هذا الإجراء من أخطر الإجراءات الحديثة التي تمس الإنسان في حقه في الخصوصية بينما يقصد بالمراقبة: تجميع وتسجيل الاتصالات الإلكترونية ومن ثم الإطلاع عليها والكشف عنها وفي

[1] فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016، ص183ص184.

ذلك أيضا تهديد للحق في حرمة الحياة الخاصة، ففي كثير من الأحيان تحوي هذه الاتصالات الإلكترونية على ما يمس حياة الشخص الخاصة بوصفها مستودع سر لصاحبها كما أن المشرع الجزائري لم يحدد وسائل المراقبة الإلكترونية عدا ما ذكره أنه يتوجب وضع الترتيبات التقنية الخاصة بالمراقبة وبالرجوع إلى الفقه المقارن فقد ذهب البعض إلى تحديد أشكال المراقبة الإلكترونية في: استخدام وسائل فنية من خلال ما يسمى بقلم التسجيل أو ما يسمى بالفخ والمتابعة.

وفي هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أي مع بريده الإلكتروني أو مع من يقوم بالمحادثة الفورية معه.

- استخدام وسائل التصنت على محتوى الرسالة الإلكترونية أو المحادثة الفورية الإلكترونية بوسائل للاعتراض والتصنت.[1]

ثانيا: تفتيش المنظومة المعلوماتية:

إن ضعف الحماية الفنية وكثرة التعدي على الأنظمة المعلوماتية تحتاج تشريعا واضحا وصريحا على المستوى الداخلي أو الدولي، حيث تتضمن الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت في: 2001/11/08 من طرف المجلس الأوروبي مختلف أشكال الإجرام المعلوماتي، وقد عدل المشرع الجزائري قانون العقوبات لنفس السبب بإضافة قسم سابع مكرر عنوانه: "المساس بأنظمة المعالجة الآلية للمعطيات" بموجب القانون رقم 04-15 المؤرخ في 2004/11/10 حيث يهدف المشرع إلى حماية نظام المعالجة الآلية للمعطيات الذي يخضع لتطورات متلاحقة في مجال صناعة الكمبيوتر وملحقاته وبرامجه.[2]

[1] ثابت دنيا زاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، مجلد05، العدد01، 2012، ص207 ص208.

[2] بوحليط يزيد، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل، مجلد 22، العدد 04، 2016، ص85.

يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية حسب نص القانون 09-04 في المادة الخامسة الدخول بهدف التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة معلوماتية.

إذن يلاحظ بأن التفتيش في الوضعيات المشار لها يأخذ منحنيين فهو إما أن يكون عملا من أعمال التحقيق تقوم به السلطات القضائية المختصة وإما يكون من أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطة المختصة وفي كلتا الحالتين فإن المستهدف هنا هو جهاز الكمبيوتر (الحاسوب) بمكوناته المادية والمعنوية فالحاسوب كما هو معروف يتكون من مكونات مادية.

وهي مجموعة وحدات لكل منها وظيفة معينة وهي متصلة ببعضها في شكل نظام متكامل منها وحدات الإدخال ومهمتها استقبال البيانات المعلوماتية والغير المعالجة وأيضا لها إلى داخل جهاز الحاسوب لكي تمرر إلى وحدة الذاكرة للمعالجة أو التخزين ووحدة الذاكرة هي التي تقوم بتخزين البرامج والمعلومات وبما تحتويه من ذاكرة رئيسية وعشوائية وذاكرة القراءة ثم وحدة الحساب والمنطق وتتكون من مجموعة دوائر حسابية ومنطقية وسجلات التنفيذ العمليات وتنقسم إلى وحدة المعالجة المركزية ووحدة الذاكرة ثم وحدة التحكم ووحدة الذاكرة المساعدة ووحدة الإخراج والمحتوية على أجهزة الشاشة والطابعة ومشغلات الأقراص وهي التي تستغل المعلومات المعالجة وتمريرها وإخراجها للمستخدم أما المكونات المعنوية للجهاز الكمبيوتر والتي تسمى أيضا بالكيانات المنطقية وهي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات ومما سبق يمكن القول بأن التفتيش وعندما يستهدف الكيانات المادية للحاسوب لا يشكل أي عائق إذ أنه من السهولة بمكان ضبط الأجهزة وحجزها أو إتلافها وإنما الأشكال يثور عندما ينصب التفتيش على مكونات الكمبيوتر المعنوية أو المنطقية كالبرامج وقواعد البيانات ذلك أن التفتيش عن هذه البيانات يتطلب

الكشف عن الرقم السري (الكود) للمرور إلى الملفات وكذا كلمات السر أو الشفرات أو ترميز البيانات.[1]

الفرع الثاني: حجز المعطيات المعلوماتية والتزامات مقدمي الخدمات:

أولا: حجز المعطيات المعلوماتية:

المعلومات المخزنة إلكترونيا تتكون من معلومات رقمية تقسم إلى أرقام أي وحدات ثنائية تكون في صيغة (1) و(0)، وتحفظ وتسترجع بإستخدام البرمجيات يمكن إنشاء وحفظ أي نوع من المعلومات أو الصور أو الكلمات أو جداول البيانات بإستخدام هذه التعليمات وبالفعل حفظ المعلومات المخزنة يتطلب معرفة تقنية دقيقة و فهم المبادئ القانونية الضرورية .[2]

كما يعتبر الحجز من أهم الوسائل التي تحارب الجرائم المعلوماتية وهذا لإجراء موزع في القوانين الخاصة وكذا قانون الإجراءات الجزائية والحجز المخول لرجال الضبطية القضائية وكذا قضاة التحقيق إلى جانب الإجراءات الأخرى مثل المعاينة والتفتيش.

وقد يحدث في بعض الأحيان إذ يكون من الصعب تقديم الدليل في الشبكة العنكبوتية مثل حال مستخدم الانترنت الذي يرتكب جريمة الشبكة دون أن يترك أثرا بالقرص الصلب في محكمة النقض الفرنسية بالغرفة الجنائية في قرارها المؤرخ في 2005/01/05 أثناء نظرها لمدد التفسير الضيق للنص الجنائي عند النظر في واقعه تصفح المواقع الالكترونية لإباحة الأطفال أن مجرد تصفح هذا الموقع التي تبرز أطفال في مواقع جنسية لا يشكل أركان الجنحة المنصوص عليها من المادة 127-4/23 من قانون العقوبات، وفي وقائع هذه القضية لم يتم تقديم أي تسجيل أو طباعة المواقع المتصفحة وتم الاعتماد فيها على ملفات مؤقتة وجدت على المنظومة المعلومات التي لم تعدها محكمة النقض الفرنسية كدليل إثبات.

[1] زبيحة زيدان، مرجع سابق، ص131-133.

[2] ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية، دار النشر الجامعي الجديد، تلمسان، 2018، ص113.

أمام هذه التحديات أجاز المشرع الفرنسي المحققين أثناء التحقيق في الجرائم الأخلاقية ضد الطفل على شبكة الانترنت الدخول في اتصال مع الجانيين لأجل (المحتوى غير المشروع الذي يستهدف الأطفال) والتصدي بتبادل هذه الصور الإباحية ومنه فيمكن للمحققين الدخول وتبادل الاتصالات الإلكترونية على الخط سواء لتقمص دور القاصر أو المجرم الجنسي للأطفال وهذا الإجراء شبيه بإجراء التسرب القانوني في جرائم المخدرات والجريمة المنظمة.[1]

المادة 06 من القانون 09-04 تنص على حجز المعطيات الآلية سواء كانت أشياء مادية أو بيانات معالجة إلكترونية وبالنسبة لتحديد مكان الحجز فالمشرع من خلال نص المادة 06 السابقة الذكر يتيح حجز جميع المعطيات المخزنة التي تكون مفيدة في الكشف عن الجرائم أو مكان البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

وبالتالي ومن خلال قراءتها للمادة نجد أن الأصل أنه يتم حجز كامل المنظومة والاستثناء هو الحجز الجزئي أي الاكتفاء بالمحتوى المجرم وأضاف المشرع الجزائري في آخر المادة سالفة الذكر أنه يجب في كل الأحوال على السلطات التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية[2].

ثانيا: التزامات مقدمي الخدمات:

قام القانون 09-04 بترتيب التزامات أخرى على مقدمي الخدمات عبر الانترنت ومنها الالتزام بمساعدة الضبط القضائي والالتزام بحفظ المعطيات المتعلقة بحركة السير.

[1] طاهري حسين، الجرائم الإلكترونية، الطبعة الأولى، دار الخلدونية للنشر والتوزيع، الجزائر، 2022، ص461-462.

[2] ناني لحسن، مرجع سابق، ص120 ص121.

01- الالتزام بمساعدة سلطات الضبط القضائي:

يشمل توفير البيانات المحفوظة لدى مزودي خدمات الإعلام والاتصال بما في ذلك مزودي خدمات الإنترنت تحت تصرف هذه السلطات ومع ذلك يجب استبعاد بعض أنواع المعلومات المحددة من نطاق هذا الإلتزام.

أ- وضع المعطيات المحفوظة لدى مقدمي خدمات الإعلام والاتصال وكذلك مقدمي خدمات الانترنت تحت تصرف سلطات الضبط القضائي، بحيث يتعين على مقدمي الخدمات في هذا المجال تقديم المعلومات التي بحوزتهم وداخل أنظمة الكمبيوتر إلى سلطات الضبط القضائي، وذلك في حدود معينة وتتمثل هذه الحدود في معرفة هوية مستخدمي خدماتهم والكشف عن محتوى اتصالاتهم والتي تفيد بالكشف عن الحقيقة حسب نص المادة 1/10 من القانون 09-04 وهذا لا يكون ممكنا إلا من خلال المحافظة من قبل مقدمي الخدمات وخاصة منها مقدمي خدمات الدخول وخدمات متعهد الإيواء على البيانات المتعلقة بمستخدمي خدماتهم، كما يتعين عليهم عدم إفشاء أسرار التحري والتحقيق حسب نص المادة 2/10 من القانون المذكور.

ب- أنواع المعلومات المستبعدة من تطبيق الالتزام بالتعاون مع سلطات الضبط القضائي، وهي معلومات معينة استثناها المشرع وتتعلق بسر المهنة المنصوص عليها في المادة 65 مكرر 05 من قانون الإجراءات الجزائية، والتي من ضمن ما نصت عليه أنه إذا ما اقتضت ضرورات التحري في الجريمة ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. وفي ذلك وغيرها من نص المادة 65 مكرر 5 يجوز لوكيل الجمهورية أن يأذن بما يلي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

- تنفيذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص.[1]

2- الالتزام بحفظ المعطيات المتعلقة بحركة السير:

إن مبدأ إخفاء الهوية بعدا يوفر حماية لحرية التعبير خصوصا أثناء تبادل الحوارات والآراء والمعلومات عبر الانترنت إلا أن تزايد المحتويات غير المشروعة عبر هذه الوسيلة اوجب التحقق من الهوية وحماية البيانات الفردية ومراقبتها، ولذلك ألزم المشرع على مقدم الخدمة عبر الانترنت الاحتفاظ بمجموعة من المعطيات وإلا كان مسؤولا عن الإخلال بذلك، ومن هذه المعطيات ما نصت عليها المادة 11 من القانون رقم 09-04 التي جاء فيها على أن يلتزموا مقدموا الخدمات بحفظ المعطيات التالية:

- المعطيات التي تسمح بالتعرف على مستعمل الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل الاتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليهم.

كما يمكن الاحتفاظ بالبيانات الشخصية للمستخدم، والهدف من حفظها هو إجراء التحري أو التحقيق القضائي، ولذلك فإن المدة المتعلقة بالحفظ عادة ما تكون مدة مناسبة لمدة التحري أو التحقيق القضائي ومدة التحري عادة لا تدوم طويلا، ولذلك قدر المشرع مدة الاحتفاظ بهذه البيانات المتعلقة بإثبات الهوية سنة واحدة تبدأ من تاريخ التسجيل يكون بعد هذه المدة لمقدمي الخدمات عبر الانترنت محو تلك البيانات.

[1] بعجي محمد، إلتزامات مقدمي الخدمة عبر الإنترنت، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد 04، العدد 01، 2019، ص 32، ص33

ولكي يتحقق مقدم الخدمات من معطيات مورد المضمون يمكن له أن يلجأ إلى إحدى الطرق وهي إما طريقة الحل القانوني أو إلى طريقة الحل التقني.[1]

أ- طريقة الحل القانوني:

يجب على مقدم الخدمة عبر الانترنت التحقق من صحة المعلومات المتعلقة بهوية المستخدم (الاسم، اللقب، تاريخ الميلاد، الهاتف...) كما يتحقق من مورد المضمون غير المشروع وحتى يعفي مقدم الخدمة من المسؤولية يجب عليه التأكد والتحقق من ذلك جيدا حتى وإن لم يلزم القانون مقدم الخدمة بذلك.

ب- طريقة الحل التقني:

يمكن الحصول على البيانات الشخصية وذلك بفضل التقنيات الحديثة كتقنية الكعكات cookies التي تسمح بإعادة رسم المستخدم وتحديد هويته وبالتالي الحصول على المعلومات التي يبحث عنها.[2]

[1] بعجي محمد ، المرجع السابق، ص33، ص 34

[2] مرجع نفسه، ص 34

المبحث الثاني: تصنيفات الجريمة الإلكترونية والآليات الموضوعية لمكافحتها:

إن الجريمة الإلكترونية تختلف في تصنيفاتها بسبب تسمياتها المختلفة فيمكن تصنيفها بناءا على أسلوب الجريمة أو دوافع ارتكابها أو تعدد محل الاعتداء والحق المعتدي عليه، أما المشرع الجزائري فقد قسمها إلى جرائم مرتكبة بواسطة النظام المعلوماتي والتي نص عليها المشرع بموجب قانون العقوبات.[1] كما قام المشرع بوضع نصوص وآليات قانونية لمكافحة الجريمة المعلوماتية من خلال تعديل قانون العقوبات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 المتمم لأمر 66-156 وخص لهذا النوع قسما كاملا تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ضمن ثمان مواد من المادة 394 مكرر إلى 394 مكرر 7، حيث نصت على جملة من القواعد الموضوعية جرمت من خلالها الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء.[2]

وهذا ما سنفصله في المطلبين التاليين:

المطلب الأول: تصنيفات الجريمة الإلكترونية:

يمكن تصور الجريمة الإلكترونية من زاويتين مختلفتين ففي الزاوية الأولى يمن أن يكون الهدف المباشر للجريمة النظام المعلوماتي نفسه، أما من الزاوية الثانية فقد يكون النظام المعلوماتي هو وسيلة تنفيذ الجريمة وبالتالي تقسم الجريمة الإلكترونية إلى قسمين وهذا ما سنتناوله في الفرعين التاليين:[3]

[1] نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر جامعة أحمد دراية، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2017، ص24.

[2] جمال شريف، زقرار عبد العزيز، مرجع سابق، ص49.

[3] مسعود شهيرة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2021، ص26

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي:

في هذه الجرائم لا يكون النظام المعلوماتي موضوعا أو محلا للجريمة الإلكترونية ولكن الجريمة تقع في هذه الحالة بواسطة النظام المعلوماتي أي أنه يستخدم كأداة لارتكاب الجرائم الإلكترونية وسنذكر البعض من صورها.[1]

أولا: الدخول والبقاء عبر المصرح بعدما إلى النظام المعلوماتي:

1- الصورة البسيطة: يتمثل النشاط الإجرامي في هذه الصورة في الأفعال التالية:

أ- فعل الدخول: يتحقق فعل الدخول بمجرد الوصول لمعلومات المخزنة داخل النظام دون علم ورضا صاحبه، لذلك الدخول يكون مقتصرا على الأشخاص المعنيين أو مقابل نفقات.

ب- البقاء: يعني التواجد داخل النظام المعلوماتي بدون إذن أو تجاوز المدة المسموحة له بالبقاء فيه كما يشمل طباعة المعلومات عندما يسمح الشخص بالرؤية فقط.

2- الصورة المشددة: شخص المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام اشتغال المنظومة.[2]

ثانيا: الاعتداء على حرمة الحياة الخاصة للأفراد:

جرائم انتهاك حرمة الحياة الخاصة للأفراد تعتبر من الجرائم القديمة ولكنها تطورت بفضل التقدم التكنولوجي هذا التقدم ساهم في سرعة وسهولة الاعتداء على حرمة حياتهم الخاصة ومن هنا كانت الحاجة إلى وجود حماية قانونية صارمة تساهم في الحد من هذه الجرائم وهذا ما نصت عليه المادة 303 مكرر 2: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من

[1] مسعود شهيرة، مرجع سابق، ص26.

[2] خضري حمزة ، عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، المجلد 6، العدد02، 2020، ص174.

500.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه."[1]

ثالثا: الاحتيال الإلكتروني:

يشمل ذلك أي سلوك أو تصرف يؤدي إلى إرهاق أو إلحاق أعباء إضافية على الآخرين نتيجة استخدام ممارسات غير أخلاقية للحصول على ميزة غير عادلة أو غير قانونية.[2]

رابعا: التجسس الإلكتروني:

يقصد بهذا السلوك استخدام تقنيات وبرامج معينة للحصول على معلومات غير معلنة على العلن، يمكن أن يتم التجسس عن طريق، الوصول غير المصرح به إلى الملفات الرئيسية في الحواسيب والأجهزة الذكية من خلال ذلك يتم زرع برامج التجسس وتسجيل البيانات ثم رفعها إلى أجهزة الشخص القائم بأعمال الإبتزاز وحفظها في ملفات خاصة ليتم استخدامها في الوقت المناسب.[3]

[1] حوالف حليمة، مهاجي فاطمة الزهراء، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، المجلد 3، العدد16، 2021، ص150.

[2] خنيفر شفيقة، الإجرام الإلكتروني كفاءات ضائعة في عالم التقنية، المؤتمر العلمي الافتراضي الأول، جامعة محمد الشريف مساعديه سوق أهراس، ص09.

[3] https://cyberone.com ، أحمد بطو، الابتزاز الالكتروني، 2024-4-28، على الساعة 13:00.

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي:

تقوم الجريمة الإلكترونية إذا كانت المكونات المعنوية للنظام المعلوماتي ممثلة بالمعلومات بكل صورها هي محل الاعتداء حيث يمكن سرقتها أو تزويرها أو حتى تدميرها وغير ذلك من الأفعال غير مشروعة والتي سنتناول أبرزها في النقاط التالية:[1]

أولا: سرقة المعلومات:

المعلومات لها قيمة اقتصادية كبيرة وتعتبر محركا للتقدم في جميع المجالات لذلك فإن الأفراد والمؤسسات والدول تسعى جاهدة للحصول على المعلومات واستخدامها في تطوير أعمالهم وابتكاراتهم، وبالمقابل كانت هناك طائفة متواجدة دائما للقيام بالاستقلال غير المشروع لهذه المعلومات وبكل الأساليب المتاحة أمامها وسرقة المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكة العالمية للمعلومات (الانترنتà هي إحدى أكثر الأساليب انتشارا في مجال الاعتداء على المعلومات ويطلق البعض على هذه الجريمة: "جريمة قرصنة المعلومات"، وتجري عملية السرقة من خلال وصول الأفراد غير المرخص لهم إلى المعلومات والبيانات وبرامج الحاسوب.

والمقصود بالقرصنة المعلوماتية نسخ البرامج بطرق غير قانونية والحصول على معلومات ون إذن أو الحصول دون وجه حق على معلومات مخزنة في ذاكرة الحاسوب بطريقة مباشرة أو غير مباشرة.[2]

ثانيا: إتلاف المعلومات:

جريمة إتلاف المعلومات تعتبر اعتداءا غير مشروعا على حق الملكية وعلى الرغم من أن النصوص القانونية، قد لا تشر بشكل صريح إلى جرائم إتلاف المعلومات إلا أنها تعتبر مشابهة

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 2، دار الثقافة للنشر والتوزيع، عمان، 2010، ص97.
[2] مرجع نفسه، ص99.

في العديد من الأنظمة القانونية فقد تدخل المشرع في العديد من الدول ليشمل بالحماية الجنائية كل صور الاعتداء كما فعل المشرع الأمريكي في العديد من الولايات أو بالنص على كل جريمة على حدى كما فعل المشرع الفرنسي.[1]

المعلومات التي جمعها ومعالجتها وتحليلها هي المحور الرئيسي في جريمة إتلاف المعلومات حيث يتعمد الجاني إتلاف هذه المعلومات أو تغييرها بطرق غير قانونية للحصول على نتائج معينة من خلال استخدامها.[2]

ثالثا: تزوير المعلومات:

الجاني في جريمة إتلاف المعلومات يستطيع الدخول إلى قاعدة البيانات وتعديل البيانات سواء بحذف البيانات الموجودة أو بإضافة بيانات غير موجودة من قبل، وهو أيضا التغيير المتعمد للمعلومات الواردة في المستند المعلوماتي بغرض التضليل.

وبذلك يمكن القول لكي تكون أمام جريمة تزوير معلوماتي يجب أن يقع التزوير على محرر إلكتروني وأن يكون ذلك التزوير مخالفا للحقيقة الواردة في المحرر وذلك بهدف إثبات حق غير موجود أساسا أو إحداث أثر قانوني ما وإلحاق ضرر بالغير.[3]

المطلب الثاني: الآليات القانونية الموضوعية لمكافحة الجريمة الإلكترونية:

يمكن إجمال القواعد الموضوعية المقررة لمكافحة الجريمة الإلكترونية في تلك الواردة في قانون العقوبات أو بموجب قوانين خاصة على النحو الآتي:

---

[1] رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، مجلة دراسات وأبحاث، المجلد1، العدد1، 2009، ص350.

[2] مرجع نفسه، ص351.

[3] خليفي فتيحة، مهداوي محمد صالح، التزوير المعلوماتي في البيئة الرقمية، مجلة الدراسات القانونية، العدد 2، 2022، ص259.

الفرع الأول: القواعد العقابية المقررة في قانون العقوبات:

أصبحت قضايا الجريمة الإلكترونية محل اهتمام في الجزائر منذ عام 2001 حيث تم إقرار أول نص تشريعي في هذا المجال بصدور القانون رقم 01-09 المؤرخ في 26 جويلية 2001 المعدل والمتمم لقانون العقوبات في المواد من 144 مكرر و144 مكرر 1 و144 مكرر 2 و146 من قانون العقوبات والمتعلق بجريمة القذف والسب والإهانة إزاء رئيس الجمهورية أو فيما يخص دين الإسلام (الرسول وباقي الأنبياء أو ما هو معلوم من الدين) أو ضد الهيئات والمؤسسات العمومية، ومن خصوصيات المادة 144 مكرر أنها أدرجت لأول مرة مصطلح[1] (وسيلة إلكترونية أو معلوماتية) التي تسمح بتجريم الأفعال السالفة الذكر في محيط المعلوماتية والانترنت.

بعدها أحدث قسم في قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 يحدد بشكل واضح الأفعال الماسة بنظم المعالجة الآلية للمعطيات والاعتداء على سير نظام المعالجة الآلية كما يحدد عقوبات الأشخاص المعنوية المرتكبة للجرائم المعلوماتية وكذا عقوبات الشروع والاشتراك في الإجرام الإلكتروني.[2]

أولا: تجريم الاعتداء على نظام المعالجة الآلية:

نصت المادة 394 مكرر من قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من خمسين ألف دينار جزائري إلى مائة ألف دينار جزائري كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف

[1] بن بعلاش خاليدة، عثماني علي، الأحكام الموضوعية والإجرائية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة أبحاث قانونية وسياسية، المجلد6، العدد2، 2021، ص702.

[2] مرجع نفسه، ص703.

العقوبة إذ ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة، وإذ ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين وغرامة من خمسين ألف دينار جزائري إلى مائة وخمسون ألف دينار جزائري."[1]

ثانيا: تجريم الاعتداء على معطيات نظام المعالجة الآلية:

ويكون ذلك بإحدى الاعتداء على معطيات نظام المعالجة الآلية:

ويكون ذلك بإحدى الصورتين:

1- الاعتداء على المعطيات الداخلية للنظام: جاء في المادة 394 مكرر: "يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 دج إلى 2000.000 كل من أدخل بطريقة الغش معطيات في نظام أو أزال أو عدل بطريقة الغش التي يتضمنها."[2]

يمكن أن يتوفر الركن المادي للجريمة بمجرد صدور إحدى هذه الأفعال من الجاني، وأفعال الإدخال والمحور التعديل تعتبر تلاعبا في المعطيات الموجودة في نظام المعالجة الآلية سواء بإضافة معطيات غير صحيحة أو محو أو تعديل معطيات موجودة بالفعل، وبالتالي يتركز النشاط الإجرامي في هذه الجريمة على المعطيات أو المعلومات التي تم معالجتها آليا وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام.[3]

2- الاعتداء على المعطيات الخارجية للنظام: نصت عليه المادة 394 مكرر 2: "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000 دج إلى 5000.000 دج كل من يقوم عمدا وعن طريق الغش بما يلي:

---

[1] المادة 394 مكرر من القانون رقم 04-15 المتعلق بقانون العقوبات المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية، العدد 71، الصادرة ب10 نوفمبر 2010.

[2] المادة 394 مكرر 1، مصدر نفسه.

[3] بن بعلاش خليدة، عثماني علي، مرجع سابق، ص703 , ص704.

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذه القسم.
- حيازة أو إنشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".[1]

3- الاعتداء على سير نظام المعالجة الآلية: قد يكون هناك نقص في النصوص القانونية الصريحة في القوانين الجزائرية بخصوص تجريم الاعتداء على سير نظام المعالجة الآلية للمعطيات لكن يمكن استنتاج ذلك من خلال النصوص القانونية التي تنص على تجريم الاعتداءات على أنظمة المعالجة أو على معطيات هذه الأنظمة سواء كانت معطيات داخلية أو خارجية.

4- عقوبة الشخص المعنوي: معاقبة الشخص المعنوي المرتكب لجرائم المساس بأنظمة المعالجة الآلية للمعطيات بغرامة تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي وفقا للمادة 394 مكرر 4.

5- عقوبة الشروع والاشتراك في الجريمة الإلكترونية: لقد أقرت المادة 394 مكرر 7 من قانون العقوبات بأن: "يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها: "بالتالي يبدوا من خلال هذا النص رغبة المشرع الجزائري في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية.

[1] المادة 394 مكرر2، مصدر سابق.

كما نصت المادة 394 مكرر 5: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها."[1]

الفرع الثاني: القواعد المقررة في القوانين الخاصة:

أولا: القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

نظرا للتطورات الرقمية التي تعرفها الدولة الجزائرية في مجال تطور التقنية والتكنولوجيا، أصبحت تشن تحديات جديدة في مجال الأمن الرقمي حيث قام المشرع الجزائري باعتماد إجراءات جديدة للمواجهة بتكنولوجيا الإعلام والاتصال ومكافحتها، وهو القانون المنظم لفضاء المعلوماتية بشكل عام ويكافح الجرائم المتصلة به كما يتضمن قواعد وإجراءات تسمح بمتابعة الجرائم التقنية ومرتكبيها بشكل قانوني وشرعي.[2]

وقد ذكر المشرع في المادة 2 من القانون 09-04 أنه: "يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية."[3]

ويتألف القانون من 6 فصول تتضمن تعريف للجريمة المعلوماتية، فقد يكون هناك تشابه بين هذا القانون وقانون العقوبات، ويتضمن أيضا بعض الأحكام المتعلقة بمراقبة الاتصالات الإلكترونية وأيضا القواعد الإجرائية لتفتيش المنظومات المعلوماتية إلى جانب ذلك إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومع ذلك يبقى

[1] بن بعلاش خليدة، عثماني علي، مرجع سابق، ص704.

[2] ياكر الطاهر، الجرائم الإلكترونية الأحكام الموضوعية والإجرائية، دار بلقيس للنشر، الجزائر، 2024، ص49، ص50.

[3] المادة 02 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 5 أوت 2009، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 16 أوت 2009.

الفصل الثاني يثير قلقا للحقوقيين بحجة أنه من الضروري أي يكون هناك توازن بين حماية الأمن الإلكتروني وحماية الخصوصية الفردية وأن يتم تطبيق القانون بشكل صحيح ومنصف لضمان حماية الحقوق والحريات الأساسية للأفراد.[1]

ثانيا: القواعد الخاصة المتعلقة بحماية المؤلف والحقوق المجاورة:

إن القفزة الرقمية التي حدثت في العالم أثرت بشكل كبير على حقوق الملكية الفكرية وتحديدا في مجال حق المؤلف وبالتالي صار بإمكاننا نشر وتوزيع المصنفات وعرضها بسرعة وسهولة وبتكاليف أقل، مما أدى إلى مواكبة هذه التطورات لظهور ما يسمى بالملكية الرقمية، حيث تشمل حقوق الملكية الفكرية على شبكة الانترنت والتي مضمونها يشمل جميع المصنفات الإبداعية التي تنتمي إلى بيئة تقنية المعلومات تعد مصنفا رقميا[2].

لهذا سارع المشرع الجزائري على غرار معظم التشريعات الغربية إلى إقرار حماية لبرامج الحاسب الآلي وتطبيق قوانين حماية حقوق المؤلف عليها: حيث أقر صراحة في الأمر 03-05 المؤرخ في 19-07-2003 المتعلق بحقوق المؤلف والحقوق المجاورة بوصف المصنف المحمي لمصنفات الإعلام الآلي،[3] وبموجب المادة الرابعة من نفس الأمر والتي تنص على: "تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يلي:

أ- المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية، والبحوث العلمية والتقنية، والروايات والقصص، والقصائد الشعرية، وبرامج الحاسوب، والمصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي تماثلها."[4]

---

[1] ياكر الطاهر، مرجع نفسه، ص50.

[2] جمال شريف، زقرار عبد العزيز، مرجع سابق، ص39.

[3] براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، المجلد 11، العدد2، 2016، ص147.

[4] أمر رقم 03-05، المتعلق بحقوق المؤلف والحقوق المجاورة، المؤرخ في 19 يوليو 2003، الجريدة الرسمية، العدد44، الصادرة في 23 يوليو 2003.

ولتحقيق حماية جنائية فعالة في هذا المجال ذكر المشرع مجموعة من الأفعال الماسة بالمصنفات وحقوق مؤلفيها وجرمها وبالتالي معاقبة المجرمين الذين يقومون بانتهاك حقوق المؤلف، ومن الجرائم التي جاء بها الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة ما يلي:[1]

نصت المادة 151 من الأمر 05/03 على: يعد مرتكبها لجنحة التقليد كل من يقوم بالأعمال التالية:

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف، استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة، استيراد أو تصدير نسخ مقلدة من مصنف أو أداء، بيع نسخ مقلدة لمصنف أو أداء، تأجير أو وضع رهن التداول نسخ مقلدة لمصنف أو أداء.
- كما نصت المادة 152 من نفس الأمر، ارتكاب جنحة التقليد عن طريق انتهاك الحقوق المحمية بموجب هذا الأمر، فيبلغ المصنف أو الأداء عن طريق أي منظومة معالجة معلوماتية.
- الاشتراك بالعمل أو الوسائل الحائز عليها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة (المادة 154 من نفس الأمر).

إضافة إلى ذلك المواد 153، 156، 157، 158، 159 من الأمر السابق المنضمة العقوبات المقررة لمختلف هذه الاعتداءات، حيث يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادتين 151 و152 أعلاه، بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من خمسمائة ألف دينار (5000.000دج) إلى مليون دينار (1.000.000دج) سواء حصل النشر في الجزائر أو خارجها طبقا للمادة 153 من نفس الأمر، ونص في المادة 154 من نفس الأمر على معاقبة الشريك في ارتكاب جريمة التقليد سواء بأعماله أو بالوسائل التي يجوزها

[1] جمال شريف، زقرار عبد العزيز، مرجع سابق، ص61.

للمساس بحقوق المؤلف بنفس العقوبات المقررة في المادة 153 من الأمر السالف الذكر، كذلك نفس الشيء بالنسبة لكل من يمتنع عن دفع المكافأة المستحقة للمؤلف (المادة 155 من الأمر نفسه).

كما تضاعف في حالة العود العقوبة المنصوص عليها في المادة 153 من هذا الأمر طبقا للمادة 156.[1]

إلى جانب هذه العقوبات أضاف المشرع لهذه الجرائم عقوبات تكميلية، المتمثلة في الفلق المؤقت لمدة لا تتعدى 6 أشهر لمؤسسة يستغلها المقلد أو شريكه والمصادرة في المبالغ التي تساوي مبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي لا صنف أو أداء محمي طبقا للمادة 157 من الأمر 05/03 بالإضافة إلى نشر حكم الإدانة وفقا لأحكام المادة 158 من الأمر نفسه.[2]

ثالثا: القواعد الخاصة المتعلقة بالبريد والمواصلات السلكية واللاسلكية:

واكب المشرع الجزائري التطور الذي شهدنه التشريعات العالمية حيث قام بإصدار قانون رقم 2000-03 المؤرخ في 5 أوت 2000 المتعلق بالقواعد المتعلقة بالبريد والمواصلات السلكية واللاسلكية،[3] والذي عرف المواصلات السلكية واللاسلكية ومنها الأمواج السلكية واللاسلكية، الشبكة الخاصة والشبكة العامة وخدمة الهاتف وخدمة التلكس والخدمات البريدية وأطرافها من مرسل ومرسل إليه وغيرها من المصطلحات التي تم استخدامها في هذا القانون.

بالإضافة إلى أنه تضمن الجرائم الإلكترونية والعقوبات المحددة والتي تتمثل في:

[1] الأمر 03-05، مصدر سابق.

[2] الأمر 03-05، مصدر نفسه.

[3] جمال شريف، زقرار عبد العزيز، مرجع سابق، ص62.

- إنشاء أو استغلال شبكة عمومية للمواصلات السلكية واللاسلكية دون رخصة أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة، وذلك حسب المادة 131 من هذا القانون.
- إنشاء أو العمل على إنشاء شبكة مستقلة دون ترخيص (المادة 132).
- إشهار بغرض بيع تجهيزات أو معدات للمواصلات السلكية واللاسلكية دون الحصول على الاعتماد المسبق (المادة 133 من نفس القانون).[1]

[1] جمال شريف، زقرار عبد العزيز، مرجع سابق، ص63.

خلاصة الفصل الأول:

من خلال ما تطرقنا إليه سابقا يتضح لنا أن المشرع الجزائري أولى اهتماما كبيرا بمكافحة الجرائم الإلكترونية لذا قام بوضع آليات قانونية وإجرائية لمكافحتها والمتمثلة في القواعد الإجرائية المقررة وفقا لقانون الإجراءات الجزائية وتشمل الاختصاص والتسرب وكذا اعتراض المراسلات وتسجيل الأصوات، كما أقر قواعد جديدة تواكب التطورات الحاصلة في جرائم الانترنت للتعامل معها والتصدي لها حيث قام بوضع قواعد إجرائية مقررة وفقا للقانون 09-04 المتعلق بالوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها والمتمثلة في مراقبة الاتصالات وتفتيش المنظومة المعلوماتية بالإضافة إلى حجز المعطيات المعلوماتية والتزامات مقدمي الخدمات. كما قمنا بإبراز تصنيفات الجريمة الإلكترونية.

حيث قسمناها إلى جرائم مرتكبة بواسطة النظام الإلكتروني وجرائم مرتكبة على النظام الإلكتروني إضافة إلى الآليات الموضوعية لمكافحة هذه الجرائم من خلال تطرقنا إلى القواعد العقابية المقررة في قانون العقوبات وكذا القواعد المقررة في القوانين الخاصة.

الفصل الثاني:

الآليات المؤسساتية والتعاون الدولي في مواجهة الجريمة الإلكترونية

تمهيد

الجريمة الإلكترونية هي جريمة حديثة، بسبب ارتباطها بالتكنولوجيا الحديثة وقد أدى ذلك إلى زيادة الغموض المحيط بها، لذا تم إنشاء جهاز خاص للتحقيق في الجريمة الإلكترونية ويتكون من وظائف متخصصة إلكترونيا وقانونيا، وفي الجزائر توجد هيئة ووحدات متخصصة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال بالإضافة إلى وحدات تابعة للأمن والدرك الوطني وكذا هيئات قضائية متخصصة في البحث والتحري عن الجريمة تتمثل في الاختصاص الإقليمي للأقطاب الجزائية المتخصصة كما قمنا بالتطرق إلى تمديد الاختصاص المحلي هذا من جهة، ومن جهة أخرى حاولت الدول أن تبحث عن آليات مشتركة لتنسيق المواقف حول طرق ما يعرف بالتعاون الدولي والمساعدة القضائية الدولية لمواجهة هذا النوع من الجرائم.

المبحث الأول: الهياكل الخاصة لمواجهة الجرائم الإلكترونية:

مع تزايد الجرائم المعلوماتية يوما بعد يوم، ونظرا إلى الطبيعة الخاصة التي ميزت هذه الجرائم، أصبح من الضروري تحديث أجهزة الشرطة القضائية لمواجهة هذا التطور الحاصل في مجال الجريمة الإلكترونية لذلك قامت معظم الدول بإنشاء وحدات خاصة لمكافحة هذا النوع من الجرائم، وقد تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الأنتربول واليوروبول والأفريبول.

أما بالنسبة للجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى الوحدات القضائية وأخرى تابعة لسلك الأمن والدرك الوطني[1] وهذا ما سنبينه من خلال المطلبين الآتيين:

المطلب الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجريمة الإلكترونية:

الهيئات المتخصصة في مكافحة الجريمة المعلوماتية تعتمد على وحدات تضم محققين من نوع خاص يتمتعون بصفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية، وهذه الوحدات تعمل على تنفيذ مهام الوقاية ومكافحة الجرائم الإلكترونية[2]، كما يحدد هوية مرتكبي هذه الجرائم رغما عن تعقيدات الأمر من الناحية التقنية نظرا لطبيعة الجريمة الإلكترونية وأدلتها.

ونادرا ما يتغافل الجاني عن تركها وراءه، واعتمادا على ذلك فإن أمر التحقيق والبحث تقوم به جهات من نوع خاص من حيث التركيبة البشرية المكونة لها، ويتميز أفرادها بالخبرة العملية والكفاءة في مجال النظم المعلوماتية، وهذا ما يمكنهم من التحكم في مجريات التحقيق، من خلال خبرتهم في التعامل مع الوسائل الموضوعة تحت تصرفهم من أجهزة وحواسيب وبرامج تحكم

---

[1] بيكة باكة ، موساوي لمياء، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، المركز الجامعي الشيخ أمود بن مختار إيليزي، معهد الحقوق، قسم الحقوق، 2023/2022، ص30.

[2] وشن لبنى، نباش مراد، دور رجال الضبطية القضائية في مكافحة الجريمة الإلكترونية، مذكرة ماستر، جامعة البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2021، ص44.

خاصة، والتي تسمح لهم بملاحقة المجرمين المعلوماتيين واقتفاء آثرهم الإلكتروني إذ أنه من المستحيل على رجال البحث والتحقيق في الجرائم التقليدية التعامل مع الجرائم المعلوماتية.

وهذا ما أدى إلى ضرورة استحداث وحدات خاصة لأجل مجابهة فئة مجرمي المعلوماتية، لأنهم أخطر فئة من الناحية الإجرامية على أمن وسلامة النظم المعلوماتية، وأيضا بالنظر إلى تفاقم الظاهرة الإجرامية المعلوماتية من يوم لآخر وزيادة مدى خطورتها واتساع رقعة نشاطها لتشمل كل ما هو موصول بالشبكة سواء هيئات عمومية أو خاصة أو أفراد.[1] انطلاقا من هذا لنا أن نتطرق إلى الفرعين الآتيين:

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم الإلكترونية:

قام المشرع الجزائري باستحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والمعلومات ومكافحتها، كما تساعد الهيئة السلطات القضائية في التحقيقات المتعلقة بالجرائم، المعلوماتية وتقوم بتجميع المعلومات وإنجاز الخبرات القضائية.[2]

أولا: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تعرف حسب ما نصت عليه المواد من 01 إلى 04 من القانون 09-04 بأنها: "هيئة إدارية مستقلة بشخصية معنوية واستقلال مالي ويقع مقرها بالجزائر العاصمة".

كما أنشأت الهيئة الوطنية بالجزائر بموجب المادة 13 من القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاتصال والإعلام ومكافحتها، وبالضبط في نص المادة 13، لكنه ترك أمر تشكيل الهيئة وتنظيمها وكيفية سيرها للتنظيم الصادر بموجب المرسوم الرئاسي 261/15.

كما تعتبر الهيئة سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة يترأسها وزير العدل وأساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن،

[1] ربيعي لحسن، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة دكتوراه، جامعة باتنة1، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016/2015، ص145.

[2] سيد علي السيد محمد، الجرائم الإلكترونية (ماهيتها، صورها، إثباتها، مكافحتها)، دار التعليم الجامعي، الإسكندرية، 2020، ص107.

وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء وتضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية النابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين وفقا لقانون الإجراءات الجزائية، تكلف بتجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الإلكترونية قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات والجرائم الأخرى تحت سلطة القاضي المختص.[1]

ثانيا: مهام واختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

مهامها: نصت المادة 14 من نفس القانون على أنه تتولى الهيئة المذكورة في المادة 13 خصوصا مجموعة من المهام نذكر منها:

1- الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تكمن إجراءات الوقاية بتوعية مستعملي تكنولوجيات الإعلام والاتصال وشرح مدى خطورة هذه الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، وعلى رأس هذه الجرائم: جرائم التجسس، على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء...[2]

2- مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

حسب المادة 14 من القانون 09-04 يوجد نوعان من المكافحة تتولاها هذه الهيئة:

- مد يد العون للسلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم.

[1] بوبعاية ابتسام، مرجع سابق، ص32 ص33.

[2] مرجع نفسه، ص33.

- تنشيط وتنظيم عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، تقديم المساعدة لمصالح الأمن والدرك الوطنيين ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة)[1]
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم:
- تقوم الهيئة وطنيا بتنسيق وتحفيز الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات (الهيئات) المشابهة لها على مستوى الدول بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم.[2]

اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

بينت الفقرة 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام التي تتولاها الهيئة على سبيل الحصر والغاية منها هو الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ومن أبرز مهامها:

- اقتراح العناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- تنسيق وتنشيط العمليات الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- مد يد المساعدة لمصالح الشرطة القضائية والسلطة القضائية في إطار مكافحة الجرائم الإلكترونية من خلال تزويدهم بالمعلومات والخبرات القضائية وضمان المراقبة الوقائية للاتصالات الإلكترونية لأجل الكشف عن الجرائم التي تتعلق بعمال الإرهابية والتخريبية التي تمس بأمن الدولة وذلك تحت سلطة القاضي وباستثناء أي هيئات وطنية أخرى.

[1] بوبعاية ابسام ، مرجع سابق، ص33 , ص34.

[2] مرجع نفسه، ص34.

- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.[1]

ثالثا: تشكيل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

لكي تتمتع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بفعالية، يجب أن تتكون من جهاز إداري تنفيذي وذلك لأداء اختصاصاتها على أكمل وجه، يتكون الجهاز الإداري من مجلس توجيه ومديرية عامة وهذا يضمن أداء المهام المنوطة بها وفقا للقانون، يترأس مجلس التوجيه وزير الدفاع الوطني أو ممثلة وتتكون من الوزارات التالية:

- وزارة الدفاع الوطني.
- وزارة العدل.
- الوزارة المكلفة بالمواصلات السلكية واللاسلكية.
- الوزارة المكلفة بالداخلية.

إلا أنه، وما يجب التأكيد عليه أن مثل هذه الهيئات لا تعمل بمعزل عن الأهداف الحكومية الكبرى أو خارج نطاق السياسة العامة للدولة، لأن الغاية من إنشاؤها هو تحقيق سياسة الدولة في المجالات المعنية لذلك، حتى تنجح هذه المهمة تعمد الدولة إلى منح هذه الهيئات نوعا من الاستقلالية كقوة دفع لها حتى تتيح لها الفرصة للعمل بنجاعة.

وتزود الهيئة بأمانة عامة تحت سلطة وزارة الدفاع الوطني، ويتكلف مجلس التوجيه على الخصوص بما يلي:

- التداول حول إستراتيجية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[1] بوبعاية ابتسام، مرجع سابق، ص34، ص35.

- تقييم حالة التهديد دوريا في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال للقدرة على تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بشدة.
- اقتراح النشاطات التي تتصل بالبحث وتقييم الأعمال المباشرة في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- الموافقة على عمل الهيئة.
- دراسة التقرير السنوي لهذه الهيئة.
- تقديم الرأي في كل مسألة تتصل بمهام الهيئة.
- ضبط المعايير القانونية في مجال اختصاصه.
- دراسة مشروع الهيئة.

وقد أكد المشرع على أن سير مجلس التوجيه تحدد بموجب قرار من وزير الدفاع:

وهذا ما يدل على سيطرة وزير الدفاع على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال حتى وبالتالي تبعية هذه الهيئة لوزارة الدفاع فلا يمكن القول باستقلاليتها.[1]

الفرع الثاني: جهازي الأمن والدرك لوطني:

قامت المديرية العامة للأمن الوطني وجهاز الدرك الوطني بإنشاء فرق خاصة لمكافحة الجرائم الإلكترونية وتدريب أفراد متخصصين في هذا المجال على مستوى الداخل والخارج يستخدمون أحدث التقنيات لكشف ومكافحة هذا النوع من الجرائم.[2]

أولا: جهاز الأمن الوطني:

المديرية العامة للأمن الوطني في الجزائر قامت بإنشاء مخابر مركزية بمركز الشرطة بشاطوف– الجزائر العاصمة– ومخيرين بقسنطينة ووهران وتحتوي هذه المخابر على فروع تقنية

[1] بوزبرة سهيلة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، مجلد 17، العدد2، 2022، ص565–567.

[2] زناتي محمد السعيد، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، مجلد 2، العدد01، 2017،ص34 ، ص 35.

خلية الإعلام الآلي، وفرق متخصصة للتحقيق والكشف عن جرائم الانترنت، هناك مخابر أخرى تم تأسيسها في بشار ورقلة وتمنراست، كما يتم توسيع نشاط هذه المخابر لتغطية جميع أنحاء البلاد. ينظم المخبر الجهوي للشرطة العلمية مخبرا خاصا على مستوى قسنطينة يقوم بمهمة التحقيق في الجريمة الإلكترونية تحت اسم "دائرة الأدلة الرقمية والآثار التكنولوجية "ضمت 03 أقسام هي:

- قسم استغلال الرقمية الناتجة عن الحواسب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهاتف النقال.
- قسم تحليل الأصوات ويكون بالاستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية.[1]

ثانيا: جهاز الدرك الوطني:

الدرك الوطني يعتبر جزءا هاما من قوات الأمن في مكافحة الجريمة بشكل عام والجريمة الإلكترونية بشكل خاص. وقد تم تخصيص موارد بشرية ومادية لهذا الغرض وأصبحت مكافحة الجريمة الإلكترونية من أولويات الدولة الجزائرية وقد بدأت الجهود الفعلية لمحاربة الجريمة الإلكترونية بقيادة الدرك الوطني في عام 2004، وهذا ما يعكس التزام الدولة في الحفاظ على الأمن والطمأنينة في الفضاء السيبيراني الوطني، ليتم بعدها إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها والذي يعد اليوم العصب الذي يسير مهام المكافحة واليقظة وفرض احترام القوانين في الوقت الذي يبحر فيه الملايين من المستخدمين عبر صفحات الانترنت سواء من الخواص أو المؤسسات في الفضاء الإلكتروني.

وقد عمل المركز السالف الذكر منذ إنشائه سنة 2008 على تأمين منظومة المعلومات لخدمة الأمن العمومي، بحيث يهدف ضباط وأعوان الشرطة القضائية المؤهلين في الدرك الوطني إلى تطبيق القوانين وجمع الأدلة وتحليل المعطيات وبيانات الجرائم الإلكترونية المرتكبة والبحث عن مرتكبيها، وتحديد هوية أصحابها إن كانوا أشخاصا فرادى أو عبارة عن عصابات كما يعمل المركز على مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها في هذا الخصوص، كما

[1] بوبعاية ابتسام، مرجع سابق، ص38 ،ص 39

يستطيع هذا المركز معالجة أكثر من 100 جريمة إلكترونية سنة 2014 وما يفوق 500 قضية رقمية سنة 2015، وفي الخمسة أشهر الأولى من سنة 2019 تم معالجة 1188 قضية بنجاح من مجموع 1515 قضية مسجلة مع توقيف 1512 متورط، وقد قامت قيادة الدرك الوطني بمجموعة من البرامج التوعوية بالتنسيق مع وزارة التربية الوطنية بتقديم دروس توعية في المدارس باعتبار أن الأطفال هم من أكثر الفئات العمرية تضررا من الجريمة الإلكترونية كخطوة أولية نحو زيادة وعي الطلاب بمخاطر الجريمة الإلكترونية وحمايتهم منها.

ولابد من السعي لمواكبة التطورات والمستجدات الحاصلة في مجال التكنولوجيات، فقد عمل جهاز الدرك الوطني على تكوين الإطارات وأعوان الدرك الوطني بشكل متواصل وذلك من خلال إنشاء مدارس ومعاهد لهذا الغرض، كمدرسة الشرطة القضائية التابعة للدرك الوطني والمعهد الوطني للشرطة القضائية.[1]

المطلب الثاني: الهيئات القضائية المتخصصة في البحث والتحري عن الجريمة الإلكترونية:

تقوم السلطة القضائية بتسوية القضايا المتعلقة بالإجرام المتصلة بتكنولوجيات الإعلام والاتصال خاصة بعد اللجوء الكبير والمتزايد إلى الشبكات الرقمية والنظام القضائي الجزائري ويتجه نحو تثبيت فكرة القضاء المتخصص وذلك ما نص عليه القانون 14/04 المؤرخ في 10 نوفمبر 2010 المعدل والمتمم لقانون الإجراءات الجزائية من إمكانية تمديد دائرة الاختصاص للمحكمة وكذا الوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم، وذلك فيما يتعلق جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

[1] شنتير خضرة، المرجع السابق، ص200 -202.

وقد نصت المادة 40 من قانون الإجراءات الجزائية على: تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد 40، 37، 329.

من هذا القانون ومراعاة أحكام المواد من 40 مكرر 01 إلى 40 مكرر 05 أدناه وتطبيقا لذلك صدر المرسوم التنفيذي رقم 06/ 348 الذي تضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق وقد نصت المادة 10 منه على: تطبيقا لأحكام المواد 37 و40 و329 من الأمر رقم 156/66.. والمتضمن قانون الإجراءات الجزائية ويهدف هذا المرسوم إلى تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دوائر اختصاص محاكم أخرى كما هو محدد في المواد 2 و3 و4 و5 أدناه في الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

وقد سعى المشرع من وراء إنشائه للأقطاب الجزائية إلى سد العجز القائم على فكرة غياب هيئات قضائية متخصصة مؤهلة لمكافحة هذه الجرائم أو التقليل من آثارها وأبعادها الوخيمة على الصعيدين المحلي والدولي لاسيما بعد إثبات عجز القضاء العادي وعدم قدرته على حل هذا النوع الحديث من الجرائم[1] وهذا ما سنبينه في الفرعين الآتيين:

الفرع الأول: الاختصاص الإقليمي للأقطاب الجزائية المتخصصة:

المشرع يضبط الحدود التي يمكن لقضاة النيابة والتحقيق والحكم العمل ضمنها وعادة ما يتم تحديد اختصاص محلي لكل محكمة استنادا على موقع وقوع الجريمة أو المكان الذي يقيم فيه المتهم أو مكان القبض عليه، وهذا ما وصت عليه المادة 01/329 ق.إ.ج.ج كما أن الأصل أن

[1] مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني، المجلد 06، العدد 02، 2022، ص1074.

اختصاص الشرطة القضائية ووكيل الجمهورية المشرف عليهم يكون ضمن الحدود التي يباشرون ضمنها مهامهم في دائرة اختصاصهم وهو ما نصت عليه المادة 16 من ق.إ.ج.ج.[1]

وقد ظهرت فكرة إنشاء محاكم ذات اختصاص موسع كأحد مخرجات برنامج إلى إصلاح العدالة وتطويرها، كما اتجه المشرع من جهة أخرى نحو سياسة تجريمية قصد تطويق أفعال تضر بالمصالح الحيوية للمجتمع، وتتجه نحو اتجاه التزامات الدولة الجزائرية كمكافحة الجريمة المنظمة العابرة للحدود الوطنية والجريمة الإلكترونية وغيرها من الجرائم التي تحتاج كفاءة مهنية عالية، وتقنيات تحري خاصة تحتاج إلى وسائل مادية وبشرية ذات نوعية.

وعلى هذا الأساس جاء القانون رقم 14/04 المؤرخ في 2004/11/10 المتضمن تعديل الأمر رقم 66-155 المتعلق بقانون الإجراءات الجزائية حيث قام بتعديل المواد 37، 40 و329 منه مؤسسا لإمكانية توسيع الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق والمحكمة إلى دائرة اختصاص محاكم أخرى تحدد عن طريق التنظيم، وهذا بمناسبة متابعة جرائم معينة بالتحديد.

وقد جسدت السلطة التنفيذية هذا الاتجاه نحو فكرة التخصيص القضائي بصدور المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 وقد تضمن الجهات القضائية التي سيوسع اختصاصها المحلي، وقد حدد أربعة محاكم على المستوى الوطني وهي محكمة سيدي محمد بالجزائر العاصمة، محكمة قسنطينة، محكمة وهران، محكمة ورقلة.[2]

أولا: محكمة سيدي محمد: مقرها في الجزائر العاصمة، ويمتد إقليميا لتشمل اختصاص محاكم تقع في دائرة اختصاص مجالس قضائية لكل من الجزائر، الشلف، الأغواط، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس وهي عشر مجالس قضائية.[3]

---

[1] عاشور أنيسة، بحيصة خديجة، الأقطاب الجزائية المتخصصة كآلية إجرائية لمكافحة جرائم الفساد، مذكرة ماستر، جامعة غرداية، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2023،ص 26 ،ص 27

[2] بيكرارشوش محمد، الاختصاص الإقليمي في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلد 8، العدد 14 ، 2016، ص 315، ص 316

[3] بيكرارشوش محمد، مرجع سابق، ص 316

ثانيا: محكمة قسنطينة: مقرها في مدينة قسنطينة ويمتد إقليمها إلى اختصاص محاكم التابعة للمجالس القضائية لكل من: قسنطينة، أم البواقي، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة وبرج بوعريريج.[1]

ثالثا: محكمة وهران: مقرها في مدينة وهران ويتوسع اختصاصها الإقليمي إلى نطاق اختصاص المحاكم التابعة للمجالس القضائية لكل من وهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تموشنت، غليزان.[2]

رابعا: محكمة ورقلة: تقع في مدينة ورقلة ويمتد اختصاصها الإقليمي إلى نطاق اختصاص المحاكم التابعة للمجالس القضائية لكل من ورقلة، أدرار، تمنراست، إليزي، تندوف، غرداية.

ويجب الإشارة إلى أنه وبالإضافة إلى ما سبق، فإن المحاكم الجزائرية يمتد اختصاصها المحلي إلى خارج حدود الإقليم الوطني إذا تعلق الأمر بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال الصادر بموجب القانون رقم 09-04 المؤرخ في 05 غشت 2009 في حال ارتكابها خارج الإقليم الوطني.[3]

الفرع الثاني: تمديد الاختصاص المحلي:

من أهم القواعد الإجرائية لمواجهة الجرائم الإلكترونية تمديد الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية:

أولا: تمديد الاختصاص المحلي لوكيل الجمهورية:

يجوز تمديد الاختصاص المحلي لوكلاء الجمهورية حسب ما أقرته المادة 2/37 من ق.إ.ج إلى دائرة اختصاص محاكم أخرى، حينما يتعلق الأمر بجرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال، الإرهاب، جرائم الصرف والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

[1] بيكرارشوش محمد، مرجع سابق، ص 316

[2] مرجع نفسه، ص 316

[3] مرجع نفسه، ص 316، ص 317

وقد تم سحب نظام الملائمة من النيابة العامة في إطار متابعة هذا النوع من الجرائم، إذ يجب على وكيل الجمهورية تحريك الدعوى العمومية بقوة القانون.[1]

ثانيا: تمديد الاختصاص المحلي لقاضي التحقيق:

يجوز تمديد الاختصاص المحلي لقاضي التحقيق حسب ما أقرته المادة 2/40 من ق. إج إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالعرف.[2]

ثالثا: تمديد الاختصاص المحلي لضباط الشرطة القضائية:

يتحدد الأصل المكاني أو الإقليمي لضبط الشرطة القضائية تحت سلطة وكيل الجمهورية الذي يقوم بإدارة أعمالهم في مرحلة جمع الاستدلالات، وبانتداب قاضي التحقيق في حال فتح تحقيق قضائي بالمكان الذي ارتكبت فيه الجريمة أو مكان توقيف المشتبه فيهم أو مكان إقامتهم طبقا للمواد 3/16 من ق.إج: يجوز لهم أيضا في حال الاستعجال أن يقوموا بمباشرة مهمتهم في جميع الأقاليم الوطنية إذ طلب منهم أداء ذلك من القاضي المختص قانونا، ويجب أن يساعدهم ضباط الشرطة القضائية الذي يمارس وظائفه في المجموعة السكنية المعنية.

والمادة 16 مكرر، المادة 40 مكرر 1، المادة 40 مكرر 2، المادة 40 مكرر 3، أي أن اختصاصهم يتسع ليشمل اختصاص إقليمي لمحاكم غير التي يباشرون فيها مهامهم في دائرة اختصاصها.[3]

[1] بونار رويقة، الجريمة المعلوماتية في التشريع الجنائي الجزائري، مذكرة ماستر، جامعة محمد الصديق بن يحي جيجل، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020 /2021 ص 46

[2] مرجع نفسه، ص47

[3] مرجع نفسه، ص 47

المبحث الثاني: التعاون الدولي القضائي في مواجهة الجرائم الإلكترونية:

بما أن الجريمة الإلكترونية تعد جريمة ذات بعد دولي أي أنها عابرة للحدود الوطنية فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي والجنائي، إضافة إلى ذلك فالتحقيقات المتبادلة في الجريمة الإلكترونية وملاحقتها قضائيا تبرز أهمية المساعدة القانونية بين الدول[1]، لذلك تحرص الدول منذ فترة طويلة على عدم إفلات المجرمين من العقاب وذلك من خلال إبرام اتفاقيات ثنائية ومتعددة الأطراف لتعزيز التعاون القضائي في المجال الجنائي بين الدول كما تساهم في تحقيق المصلحة المشتركة وتقديم المجرمين للعدالة، واتخذت كمظاهر لهذا التعاون صورا متنوعة[2]، وأهمها التعاون الأمني على المستوى الدولي والذي سنوضحه في المطلب الأول والمساعدة القضائية الدولية من خلال عرضها في المطلب الثاني.

المطلب الأول: التعاون الأمني على المستوى الدولي.

ويشمل ذلك أربع صور والمتمثلة في ضرورة التعاون الأمني على المستوى الدولي وجهود المنظمة الدولية للشرطة الجنائية (الإنتربول)، بالإضافة لتبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة والقيام ببعض العمليات الأمنية والشرطية المشتركة وهذا ما سنبينه في الفروع التالية.

الفرع الأول: ضرورة التعاون الأمني الدولي:

إن الواقع العملي أثبت أن الدولة بمفردها لا تستطيع مواجهة التحديات الجرمية في هذا العصر المتطور في شتى ميادين الحياة، وبالتالي أصبحت هناك حاجة ماسة لوجود كيان يتولى مكافحة الجريمة الالكترونية، وتتعاون من خلاله أجهزة الشرطة في مختلف الدول خاصة فيما

[1] بوديسة بجاد عبد الرؤوف، مرجع سابق، ص86.

[2] بودربالة إلياس، التعاون الدولي كآلية لمكافحة الفساد، مجلة الحقوق والحريات، المجلد 9، العدد 2، 2021، ص499.

يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة.[1]

الفرع الثاني: جهود المنظمة الدولية للشرطة الجنائية (الانتربول):

تعمل المنظمة على تعزيز التعاون بين أجهزة الشرطة في الدول الأطراف، كما تعمل المكاتب المركزية الوطنية للشرطة الدولية على تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وكذا التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها حول جرائم الأنترنت، وفيما يخص دور المنظمة في ما يتعلق بجرائم الانترنت نأخذ على سبيل المثال ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة من موقعه على شبكة الانترنت وذلك إثر تلقي النيابة اللبنانية برقية الانتربول في ألمانيا بهذا الخصوص.[2]

كما أولت المنظمة اهتماما خاصا بمكافحة الجريمة المنظمة بحيث تم اتخاذ العديد من القرارات الأساسية في الجمعية العامة للأنتربول، ومن أهم هذه القرارات القرار رقم 17/ RES/ AGN/57 الذي تم اتخاذه من خلال دورة الجمعية العامة 57 المنعقدة في بانغوك سنة 1988 بعنوان الجريمة المنظمة. كما أعربت الجمعية العامة للأنتربول في جلستها 67 في القاهرة عام 1988 أن محاربة الجريمة المنظمة أحد أولويات الشرطة الدولية في قيامها بالدور الهام المتمثل بتنسيق تعاون الشرطة الدولية ضد الجريمة المنظمة.

يمكن تفعيل الأدوار التي تمارسها الأنتربول في مواجهة الجرائم المنظمة من خلال العديد من النشاطات التي تقوم بها المنظمة في مجال التعاون الأمني الدولي لمكافحة الجريمة المنظمة، ومنها:

---

[1] محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد2، 2016، ص52.

[2] ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد1، 2022، ص438.

- عقد ندوات ومؤتمرات: فقد عقدت عدة ندوات عالمية كالتي عقدت حول جرائم المخذرات، ومؤتمرات إقليمية وجهوية مثل المؤتمر الآسيوي والإفريقي والأوروبي، كما احتضنت الجزائر عام 1997 الندوة الجهوية الإفريقية لمنظمة الأنتربول.
- التحقق من المجرمين والكشف عن شخصية الجثث المجهولة فإثبات وتحقيق الشخصية يعد مظهرا من مظاهر التعاون الدولي الأمني.[1]

الفرع الثالث: تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة:

الكوارث الضخمة قد تواجه كافة دول العالم وتكون صعبة التنبؤ بها كما يصعب مواجهتها بالإمكانيات القومية للدولة المنكوبة بمفردها، بالإضافة إلى ذلك فإن الوقت يلعب دورا حاسما في التعامل مع الكوارث فالواجب أن يتم تكثيف الجهود والخبرات والإمكانيات للتصدي للتحديات التي تواجهنا في وقت قصير، فالاستجابة السريعة والتنسيق الجيد يساعد في تخفيف الآثار السلبية للكوارث وتعزيز الاستعداد والاستجابة الفعالة وهذا ما يمكن تحقيقه إلا بتضافر الجهود لذلك لابد من التعاون الدولي.[2]

الفرع الرابع: القيام ببعض العمليات الشرطية والأمنية المشتركة:

تعقب المجرم الإلكتروني وجمع الأدلة الرقمية وكذلك عمليات التفتيش العابرة للحدود تعتبر مكونات أساسية وعملية التحقيق الجنائي الحديث، حيث تستخدم الحواسيب والأنظمة المعلوماتية وشبكات الاتصال للبحث عن أدلة وبراهين تساعد في الكشف عن الجريمة المعلوماتية، فالعمليات الشرطية والأمنية تلعب دورا هاما في تطوير مهارات وخبرات القائمين على مكافحة تلك الجرائم من خلال التعاون والتنسيق بين الجهات المعينة مما يؤدي لتعزيز القدرة على مكافحتها ووضع حد لها.[3]

---

[1] غربي أسامة، المنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مكافحة الجريمة المنظمة، مجلة دراسات وأبحاث، المجلد 3، العدد 3، 2011، ص164-165.

[2] غانم مرضي الشمري، مرجع سابق، ص98.

[3] مرجع نفسه، ص98.

المطلب الثاني: المساعدة القضائية الدولية:

المساعدة القضائية الدولية تهدف لتسهيل المحاكمة وكشف الحقيقة في جرائم معينة حيث تعمل السلطات المختصة في الدولة المطلوبة على تنفيذ إجراءات قضائية بناءا على طلب الدولة الطالبة، ووظف مصطلح المتبادلة لتبادل المساعدة القضائية الدولية في إطار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

بالإضافة إلى أن المساعدة القضائية الدولية تلعب دورا هاما في ضمان عدم إفلات مرتكبي الجرائم من العقبات وهي السبيل الفعال للحصول على الدليل الإلكتروني سواء من خلال تبادل المعلومات بين الدول أو نقل الإجراءات أو تفويض جهات أخرى للقيام لأعمالها[2] وهذا ما سنعرضه في الفروع التالية:

الفرع الأول: تبادل المعلومات.

تلعب المعلومة دورا حاسما في مواجهة أي ظاهرة وتحقيق أي إنجاز، والدول تدرك أهمية ذلك وتسعى لاكتساب معلومات أكثر لتعزيز التعاون الدولي ورغم وجود اتفاقيات تلزم الدول بالتعاون إلا أنه قد يكون هناك بعض الإحباطات في التنفيذ، سيما إذا ما تعلق الأمر بالإجرام الذي يتعدى نطاق الدولة الواحدة، ذلك أن المعلومات ذات الصلة في هذا الجانب ترتبط بصورة أو أخرى بأمن الدولة القومي وسيادتها التي لا تريد التفريط بها، وتبالغ الدول عادة في الدفاع عن تلك السيادة.

أقرت العديد من الاتفاقيات هذا النمط من التعاون، وأبرزها ما ورد في الفقرة الثانية من المادة الأولى لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية وكذلك ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة

[1] عصماني ليلى، صهيب سهيل غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، المجلد 9، العدد2، 2020، ص16

[2] مرجع نفسه، ص17.

العابرة للحدود الوطنية، إذ فرضت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي. والأمر نفسه بالنسبة لما قضت به المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية، وفي هذا المجال وضع اتفاق شنغن للإتحاد الأوروبي نظاما متكاملا لتبادل المعلومات.[1]

الفرع الثاني: نقل الإجراءات:

يقوم الدول بالتعاون واتخاذ إجراءات جنائية بناءا على اتفاقيات ومعاهدات لمكافحة الجرائم التي ترتكب في إقليم دولة أخرى ولمصلحة دولة أخرى وذلك عند توافر شروط معينة من أهمها التجريم المزدوج يعني أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها أي أن تكون هذه الإجراءات مقررة في قانون الدولة المطلوب إليها عن نفس الجريمة، كما يجب أن تكون الإجراءات المطلوبة ذات أهمية بالغة حيث تلعب دورا حاسما في الكشف عن الحقيقة.[2]كما أقرت العديد من الاتفاقيات الدولية والإقليمية التي تهدف إلى تعزيز التعاون الدولي في مجال المساعدة القضائية، مثل معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية سنة 2000 في المادة 21 منها، ونفس الشيء نجده في معاهدة المؤتمر الإسلامي لمكافحة الإرهاب الدولي سنة 1999 في المادة 9 منها، وأيضا المادة 16 من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي عام 2003.[3]

[1] شويرب جيلالي، مراد فائزة، الآليات الدولية والوطنية لمكافحة الجريمة السيبيرانية، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 2، 2023، ص165.

[2] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية للنشر والتوزيع، الجزائر، 2018، ص312.

[3] مرجع نفسه، ص313.

الفرع الثالث: الإنابة القضائية:

ويقصد بذلك طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، هذا الطلب يتم تقديمه من قبل الدولة الطالبة إلى الدولة المطلوب إليها للمساعدة في فصل مسألة معروضة على السلطة القضائية في الدولة الطالبة.

يهدف هذا الطلب إلى تسهيل الإجراءات الجنائية بين الدول وضمان إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى مثل سماع الشهود أو إجراء التفتيش وغيرها من الإجراءات.[1]

أولا: تنفيذ الإنابة القضائية:

بخصوص تنفيذ الإنابة القضائية الدولية فإنه إذا استقر القاضي على ضرورة اللجوء إلى الإنابة القضائية، كأن يرى القاضي الجزائري اتخاذ الإجراء القضائي موضوع الإنابة فيمكنه إرسال الطلب إلى الجهة القضائية المختصة في الخارج أو إلى البعثة الدبلوماسية أو القنصلية المتواجدة في الخارج حسب ما أكدت عليه المادة 112 من القانون 08-09 المتعلق بقانون الإجراءات المدنية والإدارية.[2]

أ- عن طريق السلطات القضائية:

الإنابة القضائية عادة ما توجه إلى السلطات في الدولة الأجنبية عن طريق النيابة العامة في البلدين أو أي جهاز قضائي آخر يعهد إليه بتنفيذ الإنابة ويتم إرسالها عن طريق وزارة العدل فوزارة الخارجية ثم وزارة العدل في الخارج أو عن طريق أحد أطراف الخصومة أنفسهم الذي يتقدم

[1] غانم مرضي الشمري، مرجع سابق، ص99، ص100.

[2] زغودي عمر، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، مجلة البحوث القانونية والاقتصادية، المجلد3، العدد2، 2020، ص105.

بطلب للجهات القضائية موضوعه تنفيذ إنابة قضائية في الخارج وهذا ما أقره الفقه والقضاء الفرنسيين وهذه الطريقة في تنفيذ الإنابة القضائية الأكثر اتفاقا مع طبيعة الإنابة.[1]

ب- تنفيذ الإنابة القضائية الدولية بواسطة البعثات الدبلوماسية والقنصلية:

عند تنفيذ الإنابة القضائية يعين تحديد نطاق الهيئة المنابة ولمعرفة هذا النطاق يجب معرفة حدود الهيئة الدبلوماسية أو القنصلية من حيث أن سلطتها في تنفيذ الإنابة القضائية الدولية تشمل رعاياها فقط أم تمتد إلى رعايا دولة أخرى.

وبالإشارة إلى أن اتفاقية فينا للعلاقات القنصلية لعام 1963 اشترطت أن تكون طريقة إرسال الإنابة القضائية وتنفيذها على وفق قوانين وأنظمة الدولة المرسل إليها هذا الطلب والمراد تنفيذه على إقليمها إلا إذا أوجد اتفاق دولي بين الدول المعنية تحدد طريقة خاصة لهذا التنفيذ من قبل الممثل القنصلي على أن عدم وجود اتفاقية بين الدولتين لا يسمح بصورة مطلقة للدول طالبة الإنابة القضائية تنفيذها من قبل مبعوثها الدبلوماسي أو القنصلي في الدولة الأجنبية على وفق قوانين هذه الدولة فإذا قدر القاضي ضرورة اللجوء إلى الإنابة القضائية فعادة ما يلجأ إلى إحدى الطريقتين: اللجوء إلى ممثلي دولته الدبلوماسيين أو قناصلها في الدولة المراد اتخاذ الإجراء فيها، على أن هذا اللجوء إلى هذه الطريقة رهن شرطين أولهما أن يجيز قانون دولة الممثل الدبلوماسي أو القنصلي للقيام بذلك العمل وثانيهما أن تسمح الدولة المعتمدين لديها بمباشرة الإنابة القضائية على إقليمها.[2]

ثانيا: تنفيذ الأحكام الأجنبية:

عندما يتعلق الأمر بإعمال إقليمية القانون الجنائي بصورة مطلقة فإنه بالضرورة يقود إلى القول بإقليمية الأحكام الجنائية وبالتالي القاضي الجنائي لا يطبق سوى قانون دولته، كما أن الحكم الجنائي الأجنبي الصادر من قضاء دولة معينة لا يعترف له إلا داخل إقليم هذه الدولة،

[1] زغودي عمر، مرجع سابق، ص106.

[2] مرجع نفسه، ص106.

ومن ثم لا يجوز قوة الأمر المقضي به ولا يجوز تنفيذه، إلا أن إنشاء صور وأشكال الجريمة عبر الوطن اقتضى ضرورة الاعتراف بحجية الحكم الجنائي الأجنبي الصادر عن محاكم دولة أخرى[1].

كما أن التعاون الدولي في تنفيذ الأحكام الجزائية الأجنبية مهم جدا في مكافحة الجريمة العابرة للحدود ومع ذلك هناك شروط محددة يجب توافرها لتنفيذ الحكم الجزائي الأجنبي في إقليم الدولة وتقرير الحالات التي لا يجوز فيها تنفيذ هذا الحكم.

أما في الجزائر يوجد تجسيد واقعي لتنفيذ الأحكام الجزائية الأجنبية من خلال بعض الاتفاقيات التي أبرمتها الجزائر والمتعلقة بالتعاون القضائي في المجال الجزائي على سبيل المثال اتفاقية الرياض العربية للتعاون القضائي والتي نصت على الشروط التي يجب توافرها من أجل التعاون الدولي بين الدول الأطراف في مجال تنفيذ الأحكام الجزائية في دولة غير الدولة التي أصدرت هذه الأحكام، عندما يكون المحكوم عليهم من مواطني الدولة المطلوب منها التنفيذ وذلك في حالة توافر الشروط، أن يوافق على طلب التنفيذ كل من الطرف المتعاقد الصادر عنه الحكم والمحكوم عليه، أو أن تكون العقوبة المحكوم بها سالبة للحرية لا تقل مدتها أو المدة المتبقية منها أو القابلة للتنفيذ على ستة أشهر أو أن تكون العقوبة من أجل إحدى الجرائم التي لا يجوز فيها التسليم طبقا للمادة 41 من هذه الاتفاقية.[2]

[1] زغودي عمر، مرجع سابق، ص106.

[2] مرجع نفسه، ص107.

خلاصة الفصل الثاني:

وفي نهاية هذا الفصل يتسنى لنا القول أن الجرائم الإلكترونية من المستجدات الإجرامية الحديثة حيث تستهدف الاعتداء على البيانات والمعلومات والبرامج الإلكترونية، لذا قام المشرع بإنشاء هياكل خاصة لردع هذا النوع من الإجرام وذلك بتخصيص هيئات فنية متخصصة في البحث والتحري عن الجريمة وكذا هيئات قضائية، بالإضافة إلى هذه الآليات لابد من تضافر جهود ولية متبادلة أي ضرورة التعاون الأمني القضائي للحد من هذه الجرائم باعتبارها عابرة للحدود ومن أبرز صور هذا التعاون، التعاون الأمني الدولي والمساعدة القضائية.

الخاتمة

الخاتمة

وفي ختام دراستنا نستنتج أنه بالرغم من الإيجابيات التي قدمتها الأنظمة المعلوماتية للبشرية، إلا أنها تترتب عنها مجموعة من السلبيات التي تنتج عن سوء استغلال الأفراد لهذه التكنولوجيا وتقنياتها المعلوماتية حيث ظهرت أنواع حديثة من الجرائم وعلى رأسها الجريمة الإلكترونية، وقد حاولنا طرح موضوع آليات مواجهة الجرائم الإلكترونية من خلال الجهود التي قدمها المشرع الجزائري، جسدنا ذلك في فصل تمهيدي وفصلين أساسيين، حيث تطرقنا في الفصل التمهيدي بتفصيل ماهية الجريمة الإلكترونية وذلك من خلال ذكر تعريفاتها ومرتكبيها في المبحث الأول وكذا خصائصها وأركانها في المبحث الثاني، كما تعرضنا في الفصل الأول تحت عنوان الآليات التشريعية للوقاية من الجريمة الإلكترونية إلى الآليات القانونية الإجرائية في المبحث الأول وتصنيفات الجريمة الإلكترونية والآليات الموضوعية لمكافحتها في المبحث الثاني. كما قمنا بتفصيل الآليات المؤسساتية التي تضمنت الهياكل الخاصة لمواجهة هذا النوع من الجرائم كمبحث أول، قمنا بإبراز دور التعاون الدولي القضائي كمبحث ثاني.

خلصنا بعض النتائج وارتأينا تقديم بعض الاقتراحات لهذا الموضوع تمثلت في:

النتائج:

- تميز المجرم الإلكتروني بالذكاء وامتلاكه لقدرات عقلية وذهنية تمكنه من التلاعب بالبيانات والبرامج الحاسوبية، عكس المجرم التقليدي.
- التحقيق الجنائي يواجه صعوبات وذلك بسبب طبيعة الجريمة الإلكترونية.
- رغبة المشرع الجزائري في القضاء على الجريمة الإلكترونية من خلال قيامه بسن عدة قوانين ومنها القانون 04/09 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- بالرغم من الجهود التي بذلها المشرع لمكافحة هذا النوع من الإجرام إلا أنها غير كافية وذلك بسبب قلة النصوص العقابية.
- قيام المشرع بوضع آليات مؤسساتية للحد من هذه الجريمة الإلكترونية.

- لا تقتصر مكافحة الجريمة الإلكترونية على المستوى الوطني فقط بل تمتد لجميع دول العالم باعتبارها عابرة للحدود الوطنية.

الاقتراحات:

- توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية ومدى خطورتها.
- استحداث نصوص قانونية تتناسب مع مستوى التطور الذي آلت إليه التقنية الإلكترونية.
- استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.
- وجوب إصدار قانون خاص لهذا النوع من الجرائم وتشديد العقوبات على مرتكبيها.
- القيام برسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الانترنت إذ يستلزم التدخل الحكومي والدولي نظرا لخطورتها.

قائمة المرجع

المراجع باللغة العربية

أولا: التشريعات القانونية

1. المادة 02 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 5 أوت 2009، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 16 أوت 2009.
2. المادة 394 مكرر من القانون رقم 04-15 المتعلق بقانون العقوبات المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية، العدد 71، الصادرة ب10 نوفمبر 2010.
3. أمر رقم 03-05، المتعلق بحقوق المؤلف والحقوق المجاورة، المؤرخ في 19 يوليو 2003، الجريدة الرسمية، العدد44، الصادرة في 23 يوليو 2003.

ثانيا: الكتب

1) بلواضح الطيب، الجريمة في الفضاء الإلكتروني، الطبعة الأولى، دار وائل للنشر والتوزيع، الأردن-عمان، 2020

2) بن عطية خيرة، الجريمة الالكترونية خصائصها وأهدافها، الجريمة الالكترونية وحجب الدليل الرقمي في الإثبات الجنائي، الطبعة الأولى، المركز المغاربي شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة بريطانيا، 2024.

3) -بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017.

4) باطلي غنية، الجريمة الالكترونية، منشورات الدار الجزائرية، الجزائر، 2015.

5) زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.

6) سيد علي السيد محمد، الجرائم الإلكترونية (ماهيتها، صورها، إثباتها، مكافحتها)، دار التعليم الجامعي، الإسكندرية، 2020

7) طاهري حسين، الجرائم الإلكترونية، الطبعة الأولى، دار الخلدونية للنشر والتوزيع، الجزائر، 2022.

8) عالية سمير، الجرائم الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2020.

9) عباد الحلبي خالد، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2011.

10) عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2007.

11) عبد القادر المومني نهلا، الجرائم المعلوماتية، الطبعة 2، دار الثقافة للنشر والتوزيع، عمان، 2010.

12) غانم مرضي الشمري، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الدار العلمية للنشر والتوزيع، عمان–الأردن، 2016.

13) فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016.

14) مرضي الشمري غانم، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الدار العلمية للنشر والتوزيع، عمان–الأردن، 2016.

15) مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية للنشر والتوزيع، الجزائر، 2018

16) ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية، دار النشر الجامعي الجديد، تلمسان، 2018.

17) ياكر الطاهر، الجرائم الإلكترونية الأحكام الموضوعية والإجرائية، دار بلقيس للنشر، الجزائر، 2024

18) يعيش تمام شوقي، الجريمة المعلوماتية، الطبعة الأولى، سلسلة مطبوعات المخبر، الجزائر، 2019

ثالثا: الرسائل الجامعية

1) إبن الضب، فاطنة حبي فتيحة، الآليات المستحدثة للحد من الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر، جامعة غرداية، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2018، 2019.

2) بقدار شيماء، آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني، مذكرة ماستر، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2023.

3) بن جدو فاطمة الزهراء، كوكي حياة، آليات مكافحة الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر، الجامعة الإفريقية العقيد أحمد دراية أدرار، كلية العلوم الاجتماعية والإنسانية والإسلامية، قسم العلوم الإنسانية، 2022/2021.

4) بوبعاية ابتسام، التحقيق في الجريمة الالكترونية،مذكرة ماستر، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021-2022.

5) -بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري،مذكرة ماستر، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021-2022.

6) بيكة باكة، موساوي لمياء، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، المركز الجامعي الشيخ أمود بن مختار إيليزي، معهد الحقوق، قسم الحقوق، 2023/2022.

7) بونار رزيقة، الجريمة المعلوماتية في التشريع الجنائي الجزائري، مذكرة ماستر، جامعة محمد الصديق بن يحي جيجل، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021/2020.

8) ربيعي لحسن، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة دكتوراه، جامعة باتنة1، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016/2015.

9) شريف جمال، عبد العزيز زقرار، آليات مواجهة الجرائم السيرانية في الجزائر، مذكرة ماستر، جامعة محمد البشير. الابراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2023.

10) شنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية، مذكرة ماستر، جامعة أحمد دراية بأدرار، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021/2020.

11) عاشور أنيسة، خديجة بحيصة، الأقطاب الجزائية المتخصصة كآلية إجرائية لمكافحة جرائم الفساد، مذكرة ماستر، جامعة غرداية، كلية الحقوق والعلوم السياسية، قسم الحقوق،2023.

12) عقباش بريزة، مبارك حنان، آليات مواجهة الجريمة الالكترونية في التشريع الجزائري،مذكرة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021-2022.

13) مدرك نريمان، الآليات القانونية لمكافحة الجريمة الإلكترونية في ظل التشريع الجزائري، مذكرة ماستر، جامعة عبد الحميد بن باديس، مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2023.

14) مسعود شهيرة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2021.

15) نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر جامعة أحمد دراية، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2017.

16) وشن لبنى، نباش مراد، دور رجال الضبطية القضائية في مكافحة الجريمة الإلكترونية، مذكرة ماستر، جامعة البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2021.

رابعا: المجلات والملتقيات العلمية

1) الزناتي محمد السعيد، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، مجلد 2، العدد01، 2017.

2) أسامة غربي، المنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مكافحة الجريمة المنظمة، مجلة دراسات وأبحاث، مجلد 3، العدد 3، 2011.

3) بعجي محمد، التزامات مقدمي الخدمة عبر الانترنت، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد 04، العدد01، 2019.

4) بوجادي صليحة، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، مجلد 07، العدد 01، 2021.

5) بوحليط يزيد، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل، مجلد 22، العدد 04، 2016.

6) بودربالة إلياس، التعاون الدولي كآلية لمكافحة الفساد، مجلة الحقوق والحريات، مجلد 9، العدد 2، 2021.

7) بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة أستاذ الباحث للدراسات القانونية والسياسية،مجلد 3،العدد 11، 2018.

8) بونعارة ياسمينة، الجريمة الالكترونية، مجلة المعيار، مجلد20، عدد 39، 2015.

9) براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، مجلد 11، العدد2، 2016

10) بن بعلاش خاليدة، علي عثماني، الأحكام الموضوعية والإجرائية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة أبحاث قانونية وسياسية،مجلد6، العدد2، 2021.

11) بوزبرة سهيلة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، مجلد 17، العدد2، 2022.

12) بيكرار شوش محمد، الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلد08، العدد14، 2016.

13) ثابت دنيا زاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، مجلد05، العدد01، 2012.

14) حوالف حليمة، مهاجي فاطمة الزهراء، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، مجلد 3، العدد16، 2021.

15) حليم رامي، جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، مجلة دراسات وأبحاث،مجلد1، العدد1، 2009.

16) خضري حمزة، عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، مجلد 6، العدد02، 2020.

17) خليفي فتيحة، مهداوي محمد صالح، التزوير المعلوماتي في البيئة الرقمية، مجلة الدراسات القانونية،مجلد8،العدد 2، 2022.

18) خنيفر شفيقة، الإجرام الإلكتروني كفاءات ضائعة في عالم التقنية، المؤتمر العلمي الافتراضي الأول، جامعة محمد الشريف مساعديه سوق أهراس.

19) رحموني محمد، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة،مجلد 16، العدد41، 2018.

20) زغودي عمر، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، مجلة البحوث القانونية والاقتصادية،مجلد3، العدد2، 2020

21) زوزو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، مجلد 6، العدد 11، 2014.

22) شاين نوال، الجريمة الالكترونية في التشريع الجزائري، مجلة سوسيولوجيا، مجلد 6، العدد 2، ص69.

23) شنين صالح، التسرب في قانون الإجراءات الجنائية الجزائري حماية النظام العام والحريات أم حماية النظام العام، المجلة الجزائرية للقانون المقارن، مجلد 1،العدد02، 2015.

24) شويرب جيلالي، مراد فائزة، الآليات الدولية والوطنية لمكافحة الجريمة السيرانية، مجلة الدراسات القانونية والسياسية، مجلد 9، العدد 2، 2023.

25) عصماني ليلى، صهيب سهيل غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، مجلد 9، العدد2، 2020.

26) غربي أسامة، المنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مكافحة الجريمة المنظمة، مجلة دراسات وأبحاث، مجلد 3، العدد 3، 2011.

27) لصلج نوال، غزيوي هندة، التسرب كآلية من آليات البحث عن الدليل الجنائي في التشريعات الجنائية المعاصرة، مجلة البيبان للدراسة القانونية والسياسية، مجلد 03، العدد 02، 2018.

28) مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، مجلد 06، العدد 01، 2023.

29) محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، مجلد 14، العدد2، 2016.

30) مقلاتي مونة مشري راضية، الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، مجلد 6،العدد 01، 2021.

31) مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني، مجلد 06، العدد 02، 2022.

32) ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، مجلد 8، العدد1، 2022.

خامسا: محاضرة

1) بوزنون سعيدة، محاضرة في مقياس النظرية العامة للجريمة والعقوبة، موجهة لطلبة سنة الثانية حقوق، كلية الحقوق، جامعة الإخوة منتوري قسنطينة، 2021-2022.

سادسا: المواقع الإلكترونية

-https://accronline.com 20/04/23:05,2024,المجرم المعلوماتي: تصنيفات متنوعة ومهارات مختلفة، عبد العال،

-https://almerja.net.reading أشخاص الجريمة المعلوماتية، علي أحمد الزغبي، 20/04/2020، 23:35.

-https://cyberone.com، 2024-4-28، 13:00 أحمد بطو، الابتزاز الالكتروني،

-https://www.droiteentreprise.co m. مطماطي راوية ،الجريمة الالكترونية في التشريع الجزائري2042/05/03، 22:55

-www.it-pillars.com. 21-04-الجرائم الالكترونية أنواعها وكيفية تنفيذها وطرق مواجهتها 2024,12 ;49.

سابع: مراجع باللغة الأجنبية

- Nassima Azizi, ibtissem khedri, cybercriminalité un fléau planétaire, Revue diaa des études juridique, volume 01, numéro 01,2020, page 6
- Sam lyes,la criminalité électronique et son impact sur la sécurité nationale et la sécurité du citoyen, strategia revue des études de défense et de prospective , numéro 16, 2021, page 27

فهرس المحتويات

العنوان	الصفحة
الإهداء	–
شكر وعرفان	–
مقدمة	أ–د
الفصل التمهيدي: الإطار المفاهيمي للجريمة الالكترونية	
تمهيد	06
المبحث الأول: ماهية الجريمة الالكترونية	07
المطلب الأول: تعريف الجريمة الالكترونية	07
المطلب الثاني: أطراف الجريمة الالكترونية	11
المبحث الثاني: أركان وخصائص الجريمة الالكترونية	13
المطلب الأول: أركان الجريمة الالكترونية	13
المطلب الثاني: خصائص الجريمة الالكترونية	14
الفصل الأول: الآليات التشريعية من الجريمة الالكترونية	
تمهيد	18
المبحث الأول: الآليات القانونية والإجرائية لمكافحة الجريمة الالكترونية	19
المطلب الأول: القواعد الإجرائية المقررة وفقا لقانون الإجراءات الجزائية	20
المطلب الثاني: القواعد الإجرائية المقررة وفقا لقانون 09–04 المتعلق بالوقاية من تكنولوجيا الإعلام والاتصال ومكافحتها	29
المبحث الثاني: تصنيفات الجريمة الإلكترونية والآليات الموضوعية لمكافحتها	39
المطلب الأول: تصنيفات الجريمة الإلكترونية	39
المطلب الثاني: الآليات القانونية الموضوعية لمكافحة الجريمة الإلكترونية	43

خلاصة الفصل الأول	52
الفصل الثاني: الآليات المؤسساتية والتعاون الدولي في مواجهة الجريمة الالكترونية	
تمهيد	54
المبحث الأول: الهياكل الخاصة لمواجهة الجرائم الإلكترونية	55
المطلب الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجريمة الإلكترونية	55
المطلب الثاني: الهيئات القضائية المتخصصة في البحث والتحري عن الجريمة الإلكترونية	62
المبحث الثاني: التعاون الدولي القضائي في مواجهة الجرائم الإلكترونية	67
المطلب الأول: التعاون الأمني على المستوى الدولي.	67
المطلب الثاني: المساعدة القضائية الدولية:	70
خلاصة الفصل الثاني	75
الخاتمة	77
قائمة المراجع	80
فهرس المحتويات	88
الملخص	/

ملخص:

تعتبر الجرائم الالكترونية من الجرائم التي نشأت حديثا وتستهدف بشكل رئيسي البيانات والمعلومات والبرامج بأنواعها المختلفة، ويرتكب هذه الجرائم مجرمون ذو ذكاء عالي ويمتلكون المعرفة التقنية والفنية اللازمة، كما تطرح الجريمة الالكترونية العديد من الإشكاليات على مستوى القانون الإجرامي حيث يصعب على المحققين إجراء التحقيقات وجمع البيانات والأدلة الرقمية بإستخدام الإجراءات التقليدية مثل المعاينة والتفتيش وضبط الأدلة، من هذا المنطق قام المشرع الجزائري بإصدار آليات قانونية إجرائية وآليات موضوعية للحد من هذه الجريمة الالكترونية وكذا وضع آليات مؤسساتية متخصصة في البحث والتحري عن الجريمة الالكترونية، تعتبر هذه الآليات غير كافية لمواجهة هذه الجريمة العابرة للحدود إذ تتطلب توافر جهود دولية تجسدت في التعاون الدولي، وقد اعتمدنا في هذا البحث عن المنهجين التحليلي والوصفي وتوصلنا إلى نتائج مفادها أن المجرم المعلوماتي يختلف عن المجرم التقليدي، إذ يمتلك علما وكفاءة عالية، بالإضافة إلى قدرات عقلية وذهنية تمكنه من الإفلات من العقاب، كما أن آليات المكافحة الحالية غير كافية لمواجهة الجريمة الالكترونية بفاعلية.

الكلمات المفتاحية: الجريمة الالكترونية، المجرم المعلوماتي، الآليات القانونية والاجرائية.

Abstract:

Cyber crimes are considered crimes that have arisen recently and mainly target data, information and programs of various types. These crimes are committed by highly intelligent criminals who possess the necessary technical and artistic knowledge. Cybercrime poses many problems at the level of procedural law, as it is difficult for investigators to conduct investigations and collect digital evidence using traditional procedures such as inspection, inspection, and seizure of evidence. From this standpoint, the Algerian legislator has issued procedural legal mechanisms and substantive mechanisms to reduce this electronic crime, as well as established institutional mechanisms specialized in research and investigation of electronic crime. These mechanisms are considered insufficient to confront this cross-border crime, as it requires the availability of international efforts embodied in cooperation. In this research, we have relied on the analytical and descriptive approaches and we have reached results that indicate that the information criminal differs from the traditional criminal, as he possesses high knowledge and competence, in addition to mental and intellectual abilities that enable him to escape punishment. Also, current control mechanisms are insufficient to confront cybercrime Effectively

Key words: Electronic crime, information criminal, legal and procedural mechanisms.