كلية العلوم السياسية والحقوق

قسم :الحقوق

المكافحة الجنائية للجرائم المتصلة بتقنية المعلومة

مذكرة مكملة لنيل شهادة الماستر في الحقوق

تخصص قانون جنائي وعلوم جنائية

إعداد الطلبة

نبق محمد عصام

عبودي رقية

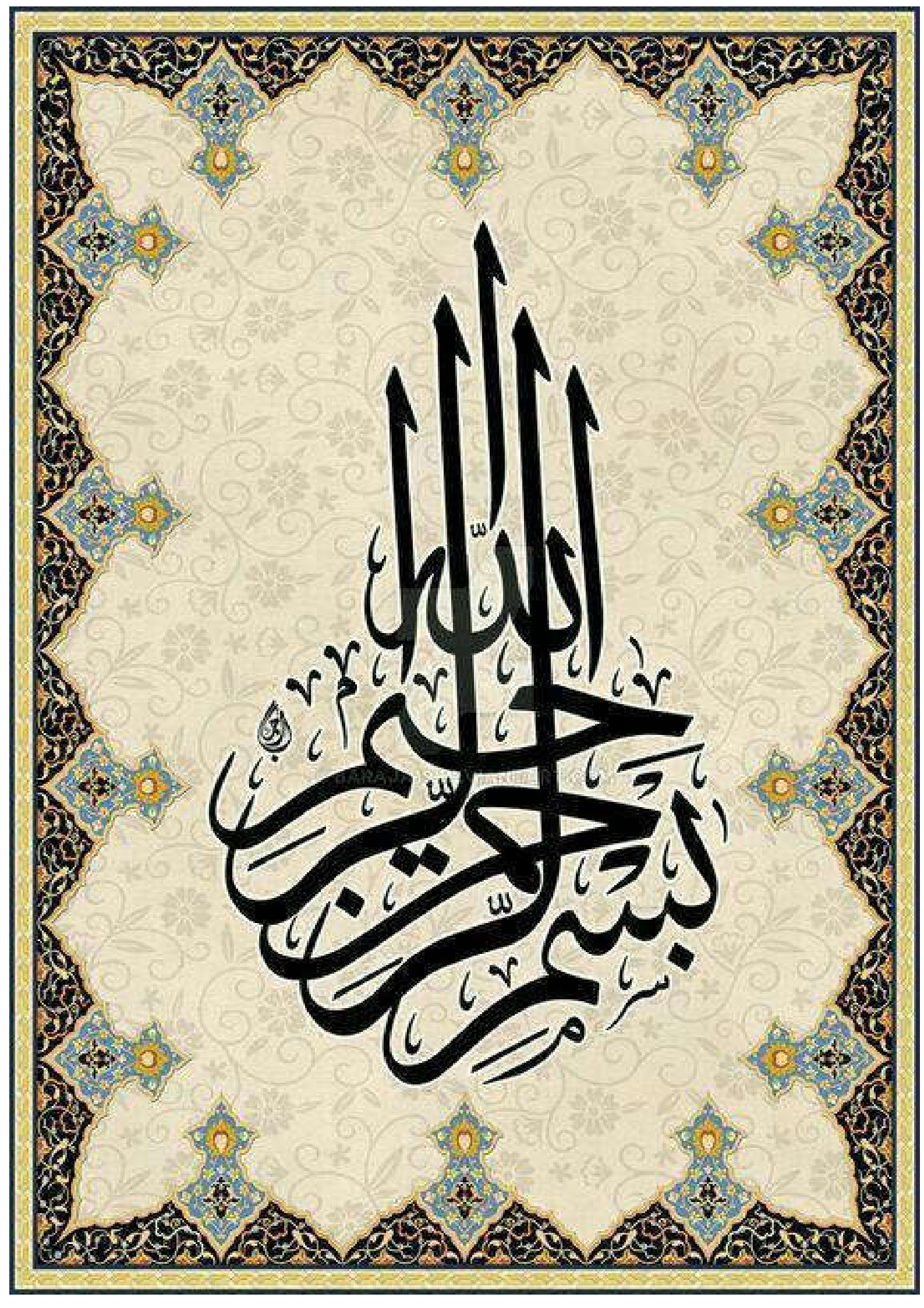
إشراف الدكتور :

د/ غريبي محمد

أعضاء لجنة المناقشة:

د / خضرون عطاء الله	رئيسا
د / غريبي محمد	مشرفا ومقررا
د/ سي ناصر محمد	مناقشا

السنة الجامعية 2026/2025


بسم الله الرحمن الرحيم

شكر وعرفان

قال رسول الله عليه أفضل الصلاة وأزكى السلام:

"من صنع إليكم معروفا فكافئوه فإن لم تجدوا ما تكافئوه فادعوا له حتى تروا أنكم قد كافأتموه"

صدق رسول الله عليه الصلاة والسلام.

لا يسعنا في هذا المقام إلا أن نتوجه بالشكر أولاً وقبل كل شيء إلى المولى عز وجل على توفيقه لنا في إتمام هذا العمل المتواضع.

كما يسرنا أن نتقدم بوافر الشكر والتقدير الى الأستاذ المشرف **خضرون عطاء الله** الذي كان له الفضل من بعد الله عز وجل في إنجاز هذا العمل بتوجيهاته ونصائحه القيمة التي أنارنا بها

كما لا يفوتنا أن نخلص بالشكر إلى أعضاء لجنة المناقشة على ما سوف يقدمونه من توجيهات وتوصيات يكون لها الأثر في تصويب هذه المذكرة.

كما نتوجه بالتحية والشكر إلى كافة اساتذة جامعة عمار ثليجي كلية الحقوق بالأغواط الذي درسونا طيلة مشوارنا الدراسي ونخص بالذكر **د.علاء الدين بن دهقان، د.خديجة حسان، د.عبد الحليم بوقرين . د.ذيب محمد**

وإلى كل من علمنا حرفا وشجع مشوارنا الدراسي

نبق محمد عصام

عبودي رقية

إهداء

بسم الله الرحمن الرحيم

أشكر الله عز وجل على إتمام دراستي وتوفيقي في عملي

أهدي هذا العمل المتواضع.

- إلى والدي الكريمين أسأل الله أن يمد في عمرهما، والى زوجتي وأبنائي أمين، زينب عبد الصمد والكتكوتة الصغيرة منال، أسأل الله أن يحفظهم وينور دربهم بالعلم والمعرفة.
- الى الصديق العزيز مفتش الإدارة **صادقي عبد القادر** الذي بفضله تمكنت من إتمام دراستي بالجامعة.
- الى الزميل و الصديق مشرف التربية **بن الطيرش مخلوف**.
- إلى كل زملائي وزميلاتي بالجامعة دون استثناء.
- إلى كل من يعرفني من قريب ومن بعيد لكم مني كل الشكر.

نبق محمد عصام

إهداء

الحمد لله حبا و شكرا و إمتنانا على البدء و الختام

" و آخر دعواهم أن الحمد لله رب العالمين "

بكل فخر أهدي هذا العمل المتواضع.

الى النور الذي أنار دربي و السراج الذي لا ينطفئ نوره ابدا و الذي بذل جهد السنين من اجل أن اعتلي سلالم النجاح الذي أحمل إسمه بكل فخر " أبي الغالي "

إلى والدتي الحبيبة التي كانت لي الأم الحنون والمعلمة الأولى، والتي غرست في نفسي القيم والمبادئ، والتي كانت لي السند في كل الأوقات، من كانت لي الملاذ الآمن، والتي سعت في تقديم الحب والحنان لي.

إلى إخوتي وأخواتي لدعمهم وتشجيعهم المستمر طوال حياتي. وكان حبهم وثقتهم بي مصدر دافع لمتابعة أحلامي وتحقيق أهدافي و الى قديرو ،اسلام ، زكرياء وأمينة.

الى اخوات لم تلدهم أمي مؤنسات غاليات مخلوفي يمينة و مرادي ربيعة.

إلى أصدقائي الأعزاء الذين كانوا دائمًا بجانبي في كل مراحل حياتي، إلى من شاركوني أفراحي وأحزاني، وإلى من كانوا لي دعمًا في كل الأوقات، إلى من لم يبخلوا عليّ بحبهم واهتمامهم

- إلى كل زملائي وزميلاتي بالجامعة دون استثناء

إلى كل من دعمني من قريب ومن بعيد لكم مني كل الشكر.

عبودي رقية

المقدمة

مقدمـــــة

تعتبر الجريمة ظاهرة اجتماعية نشأت منذ ظهور المجتمع البشري وعرفت العديد من التطورات مع مر العصور، حيث تميز كل عنصر بنظام قانوني خاص يحدد الأفعال المجرمة ويحدد العقوبات المناسبة لها في مختلف المجالات، وقد أدى ظهور الأنماط الجديدة والمستحدثة التي لم يعرفها العالم من قبل إلى توسع وتطور النشاط الإجرامي.

ويعود سبب هذا التوسع إلى عدة عوامل، لعل أبرزها التقدم التكنولوجي الذي شهدته وتشهده الإنسانية مع مطلع القرن العشرين متى عرف العالم قفزة نوعية في مجالي تقنية المعلومات والاتصال وظهور ما يسمى بالعولمة والتطور الهائل في مجال الإعلام والاتصال وانتشارها، إذ أصبحت مختلف القطاعات تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري الدقة والسرعة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين الدول.

إلى جانب ذلك قدمت التكنولوجيا الحديثة للأجهزة الأمنية الكثير من التسهيلات والإمكانات التي تساهم في رفع كفاءتها وقدرتها على التصدي للجريمة، وعليه، فمن يملك المعلومات يملك مفاتيح المستقبل لأنها ثروة لا يستهان بها ومصدر قوة سياسية واقتصادية ومعيار يقاس عليه مدى تطور وتحضر الشعوب.

الأمر الذي أدى إلى ظهور أشكال عديدة للإجرام اصطلح عليها تسمية **الجريمة الإلكترونية** التي كانت من المفرزات السلبية للتطور التكنلوجي والتي أفرزتها تلك التقنية العالية بسبب إساءة استخدام الأنظمة المعلوماتية، حيث تعتبر شكل مستحدث من أشكال الإجرام الذي يستهدف الأفراد والمؤسسات والدول عبر الفضاء الرقمي بتجاوز الحدود التقليدية للجريمة.

وفي ظل هذا التطور السريع والرهيب وتحدي مقترفي هذه الجرائم لأجهزة الأمن والقضاء والتشريعات الدول التي أصبحت غير مواكبة لمواجهة مثل هذه الجرائم، إضافة إلى إبرام إتفاقيات بين الدول لمجابهة هذه الظاهرة وإيجاد حلول تقنية تكوينية لأجهزة الأمن والقضاء وغير ذلك.

والمشرع الجزائري على غرار التشريعات الدولية حاول التصدي لهذه الجريمة من خلال القانون رقم 04/09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، وكذا وضع نصوص قانونية وقائية وردعية تجرم الأفعال الماسة بالأنظمة المعلوماتية.

حيث تكمن أهمية دراستنا لهذا الموضوع في أنها من مواضيع الساعة وأن هذه الجريمة من التحديات الحديثة التي تهدد أمن الأفراد والدول على حد سواء بما تحمله من خطورة تتجاوز الأطر التقليدية للجريمة، خاصة وأن مرتكبيها غالبا ما يستغلون ثغرات تقنية للهروب من المسؤولية وهذا لفقدان الدليل التقليدي المادي، وتبرز أهميتها أيضا في تعقد إجراءات مكافحتها والتحقيق بها، ولعل من أهم الأسباب التي دفعتنا لاختيار هذا الموضوع نتيجة لما لاحظناه من تزايد مستمر في عدد الجرائم الإلكترونية لا سيما في الجزائر ومعرفة كيف تصدى لها المشرع الجزائري من خلال النصوص التشريعية العقابية وكذا التجريمية لما تم استقراءه من نصوص قانون العقوبات الجزائري وبالتالي اظهار مختلف السبل والآليات المستحدثة للحد من هذه الظاهرة.

ومن الأسباب الشخصية لاختيار هذا الموضوع هو اهتمامنا وميولنا الخاص نحو القضايا القانونية المعاصرة خاصة تلك المتعلقة بالتكنولوجيا والمجتمع الرقمي والرغبة في تعميم الفهم القانوني وتوسيع المعارف حول الموضوع وكذا الرغبة في المساهمة العلمية في تقديم مقترحات علمية قابلة للتطوير.

ومن أهداف دراستنا للموضوع هو التعرف على الجريم الإلكترونية ومدى خطورتها وتحليل مدى فعالية النصوص القانونية الجزائرية التي وضعها المشرع الجزائري في مواجهة هذا النوع المستجد من الجرائم من خلال دراسة الآليات التشريعية والإجرائية المعتمدة على مستوى الحماية الموضوعية للأنظمة والمعلومات أو من حيث التحقيق وجمع الأدلة، وكذا أهمية التعاون الدولي بإبراز بعض الاتفاقيات الثنائية والإقليمية والدولية في هذا المجال.

[1] القانون رقم 04/09 المؤرخ في 2009/08/05، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال ومكافحتها، المنشور بالجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، رقم 47، بتاريخ 16 أوت 2009.

مقدمـــــة

وبعد البحث والقراءة لمختلف جوانب الدراسة تراءت لنا صياغة إشكالية عامة تتمثل في:

-إلى أي مدى نجح المشرع الجزائري من خلال النصوص القانونية (القانون رقم 04/09 وقانون العقوبات)، في وضع آليات فعالة للمكافحة الجنائية للجرائم المعلوماتية رغم التحديات الإجرائية المرتبطة بطبيعة الدليل الرقمي؟.

للإجابة على هذه الإشكالية اعتمدنا المنهج الوصفي التحليلي، وذلك من خلال وصف وتشخيص موضوع البحث في مختلف جوانبه وابعاده، وتحليل النصوص القانونية سواء المسلطة على مرتكبي الجرائم الماسة بالأنظمة المعلوماتية أو الوقاية منها.

وفي سبيل إعداد هذا البحث ارتأينا تقسيم هذه الدراسة إلى فصلين، الأول خصصناه للتعرف على الإطار الموضوعي والمؤسساتي لمكافحة الجرائم المعلوماتية، والذي بدوره قسمناه إلى مبحثين، المبحث الأول تطرقنا فيه إلى الجرائم التقليدية المرتكبة في الفضاء السيبراني، أما المبحث الثاني تطرقنا فيه إلى الآليات المؤسساتية لمواجهة الجريمة المعلوماتية.

أما الفصل الثاني والمعنون بالتحديات الإجرائية والعملية للحد من الجريمة المعلوماتية فقد قسمناه إلى مبحثين، الأول تطرقنا فيه إلى إشكالية البحث والتحري في البيئة الرقمية، وبالنسبة للمبحث الثاني فتطرقنا فيه لعوائق المتابعة والمحاكمة في الفضاء السيبراني.

الفصل الأول

يشهد العالم تحولا كبيرا نتيجة التطور التكنولوجي الواسع خاصة مع كثرة استخدام الكمبيوتر والأنترنت، فقد أصبحت هذه التكنولوجيا جزءا أساسيا من حياة الناس في مختلف ربوع العالم، حيث ساهمت في تواصل الثقافات وتبادل المعلومات وتعزيز التواصل الاجتماعي، ومن خلال هذه التحولات أصبحت المعلومة أكثر قوة وثروة وأصبح للناس وعي كبير بأهمية الاستفادة منها في تحقيق التقدم والتطور، ولم ينشغلوا بمخاطر احتمال استخدام الحاسوب وشبكة المعلومات في ارتكاب الجرائم الجنائية وهي جرائم حديثة تقف حاجزا أمام تطور المجتمع على كامل الأصعدة.

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 المشرع العقابي بتعديل القوانين وإصدار قوانين عقابية جديدة أخرى تتصدى لمختلف أنواع الإجرام المعلوماتي الجديد، وهذا ما سنحاول معالجته من خلال هذا الفصل، حيث سنتطرق إلى التكريس التشريعي للجرائم المتصلة بتكنلوجيا الإعلام والاتصال في القانون الجزائري (المبحث الأول)، ثم إلى الآليات المؤسساتية لمواجهة الجريمة المعلوماتية (المبحث الثاني).

المبحث الأول: التكريس التشريعي للجرائم المتصلة بتكنولوجيا الإعلام والإتصال في القانون الجزائري.

نظرا لخطورة الجرائم المعلوماتية على الأفراد والمؤسسات والحكومات على حد سواء وفي إطار الجهود الدولية والإقليمية المتعلقة بترقية ودعم سياسة مكافحة هذه الجرائم، بات لزاما على المشرع الجزائري مسايرة النسق التشريعي لأجل البقاء على اتصال بأحدث الحلول التشريعية الخاصة بهذا النوع من الجرائم خصوصا وأن الجزائر تعرف مؤخرا وفي السنوات الأخيرة تعميم خدمة الربط بشبكة الأنترنت ودعم الجهات الحكومية بتقنيات المعلوماتية، وهو ما تولد عنه ارتفاع محسوس في معدلات الجريمة المعلوماتية مما دفع بالمشرع الجزائري للتدخل من أجل رسم الخطط القانونية والعملية لتنفيذ سياسة وقائية وردعية ضد هذه الجرائم.

وقد كان اول تشريع خاص بهذا المجال قد صدر بتاريخ 2004/11/10 بموجب القانون رقم 04/05 المعدل والمتمم بقانون العقوبات الجزائري من خلال إقرار واستحداث قسم خاص معنون بقسم جرائم المساس بأنظمة المعالجة الآلية للمعطيات والذي حمل بين طياته نصوص المواد من 394 مكرر إلى 394 مكرر07، والمتضمن في فحواه صور الجرائم المعلوماتية إضافة إلى العقوبات المناسبة لها.

غير أن هذا الجهد لم يكن كافيا لتفعيل سياسة مكافحة الجرائم المعلوماتية بسبب تعارض أحكام قانون العقوبات وقانون الإجراءات الجزائية، خصوصا مسائل الإختصاص النوعي والإقليمي الذي وقعت عائقا في وجه تطبيق نصوص القانون، مما استدعى تدخل المشرع الجزائري بموجب القانون رقم 22/06 المؤرخ في 2006/12/2 المعدل والمتمم [1] لأحكام قانون الإجراءات الجزائية الجزائري والذي عدل من قواعد الإختصاص النوعي والمحلي[1].

[1] _ القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لأحكام قانون الإجراءات الجزائية الجزائري والمنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم: 84 الصادرة يوم 24 ديسمبر 2006.

ولعل ما تجدر الإشارة إليه في هذا الصدد هو القانون الخاص بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها الصادر بتاريخ 2009/08/05 تحت رقم 04/09 [2]والذي يعتبر نموذجا قانونيا خاصا بمكافحة الجرائم المعلوماتية على اعتبار أنه قانون يتضمن نصوصا خاصة في هذا الشأن ويعتبر هذا القانون نموذجا متكاملا من حيث نصوصه وجملة المبادئ التي وضعها في مجال مكافحة الجرائم المعلوماتية وتسيير أعمال البحث والتحقيق[3].

المطلب الأول: الجرائم التقليدية المرتكبة في الفضاء السيبراني.

تدخل هذه الجريمة بوجه عام ضمن مجال إجرامي آخر سمي بالجريمة الإلكترونية المرتبطة بالعالم الشبكي والافتراضي الذي أضحى ضرورة حتمية لاستخدام التكنولوجيا التقنية والرقمية التي أنشأت حالة من التعامل الالكتروني عبر استخدام الوسائط الالكترونية المتمثلة في الحاسوب وشبكة الأنترنت أو الهاتف الذكي، وظلت تمتد عبر العالم لتؤلف شبكة هائلة لتبادل ونقل المعلومات مما خلق تحديات خطيرة أثرت على حياة الأفراد وتعاملاتهم المالية التي أصبحت عرضة للاحتيال والنصب عليها في فضاء واسع ومليء بالمستخدمين.

فالجريمة الالكترونية بمفهومها التقليدي وتبعا للقواعد العامة للجريمة بوجه عام قائمة على توفر عناصر أساسية مادية ومعنوية تكمن في استخدام الحاسوب الآلي أو الهاتف والنظام المعلوماتي عبر شبكة الأنترنت ورسائل البريد الالكتروني بالطريقة غير المشروعة أو مخالفة نصوص قانون العقوبات، فتشكل اعتداءا قانونيا إما بنية تحقيق

---

[1] –شريف خالد،الجرائم المتصلة بتكنلوجيا الإعلام والإتصال في التشريع الجزائري، مجلة البيبان للدراسات القانونية، جامعة محمد خيضر، بسكرة، الجزائر، المجلد 10، العدد 01، جوان 2005، ص 127.

[2] _ القانون رقم 04/09 المؤرخ في 2009/08/05، المتعلق بالوقاية من الجرائم المرتبطة بتكنلوجيا الإعلام والإتصال ومكافحتها، المنشور بالجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، رقم 47، بتاريخ 16 أوت 2009

[3] –ربيعي حسين، آليات البحث والتحقيق في الجريمة المعلوماتية، أطروحة لنيل شهادة الدكتوراء في الحقوق، تخصص قانون عقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياية ، جامعة باتنة، 2016/2015، ص144.

الربح أو بدافع الانتقام عبر استخدام ما يسمى بالاحتيال والنصب الإلكتروني أو المساس بحرمة الحياة الخاصة ونشر معطيات الغير دون رضا أصحابها.

الفرع الأول: النصب والإحتيال الإلكتروني.

إن طرق النصب والاحتيال أصبحت تتغير وتتنوع بين فترة وأخرى، وقد أصبحت العملات الرقمية الوهمية والألعاب الالكترونية والتجارة الالكترونية غير المنظمة، وعروض المشاركة والمساهمة والاستثمار في المشاريع التي تدر أرباحا شهرية خيالية، وعروض شراء الأسهم في شركات وهمية تحت مسميات كاذبة، من أكثر وسائل النصب والاحتيال على المستخدمين والمتفاعلين على منصات التواصل الاجتماعي، ولقد بدأت الدول تشدد في وضع قوانين وتشريعات للراغبين في إطلاق مثل هذه الأعمال بشكل عام، ومع ذلك فإن هناك طرق وأساليب جديدة كل يوم يستخدمها (الهاكرز) وأصحاب الخبرات المالية البنكية والعاملون في الاستثمارات الوهمية.[1]

وقد عرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات جريمة الاحتيال بأنه التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو الغير عن طريق[2]:

- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.
- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.
- تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

[1] -آية بن ميسة، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة لنيل شهادة الماستر، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، 2025/2024، ص24.

[2] – المرجع نفسه،ص 24 .

من خلال تصفح شبكات التواصل الاجتماعي خصوصا الفيسبوك والأنستغرام مثلا نصادف العديد من المتاجر الإلكترونية لعرض العديد من الخدمات والسلع المجهولة المنشأ والتي تكون غالبيتها غير حقيقية للإيقاع بكثير من الأشخاص من أجل التسويق الشبكي لاستغلال الشباب بحجة الحصول على وظيفة لتحقيق الثراء السريع، فهناك تقارير تفيد بأن 3.5 مليون مستخدم تكبدوا خسائر تقدر ب3.2 مليار دولار بسبب الإعلانات الوهمية عبر البريد الإلكتروني باستغلال بوابة البنوك، وهذه المعلومة يسيء استخدامها المحتالون على شبكة الأنترنت من خلال إجراء مزاد وهمي أو عرض تأشيرات وهمية مزورة، وقد يستغل الفيسبوك في التعرف إلى بيانات الأشخاص من خلال معلوماتهم وجهات الإتصال الخاصة بهم، وعناوين البريد الإلكتروني ثم يتم إرسال العديد من رسائل البريد المزعج إليهم ويسبب لهم خسائر ناجمة عن هذه الأفعال[1]،فهدف هؤلاء المجرمين هو تلقي الأرباح والأموال عن كل فرد جديد يلتحق بهم، وبالرغم من اختلاف التسميات إلا أن النتيجة واحدة وهي النصب والإحتيال على الأشخاص لجني الأموال من دون تعب أو جهد ومن دون وجه حق مستغلين ميزة التخفي أو فتح صفحات بأسماء مستعارة ووهمية أو انتحال الشخصيات، وتشير الإحصائيات المختلفة على أن غالبية الأشخاص الذين تعرضوا للنصب والإحتيال عبر شبكات التواصل الاجتماعي تتراوح أعمارهم ما بين 18-39 سنة، أي أنهم ليسوا من كبار السن مثلا الذين قد تنقصهم الخبرة في التكنولوجيا ودهاليزها بشكل عام، وخير مثال على ذلك القضية التي شغلت الرأي العام في الجزائر سنة 2023، حين قام بعض الأشخاص بإنشاء شركة وهمية باشتراك مع أشخاص معروفين على شبكات التواصل الاجتماعي الذين يطلقون على أنفسهم تسمية (المؤثرين) باستغلال فضاء التواصل الاجتماعي للنصب والإحتيال على مجموعة من الطلبة الجامعيين بإيهامهم بأن يساعدوهم للإنتقال لإكمال دراستهم في إحدى الجامعات الأوروبية (جامعة أوكرانيا) ما كلف هؤلاء الطلبة مبالغ مالية معتبرة دون أن ينالوا مبتغاهم.[2]

1_ خالد حامد مصطفى، المسؤولية الجنائية لناشر الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الإجتماعي، كلية القانون، جامعة عمان، 2013 ، ص12

2 _ آية بن ميسة ،مرجع سابق،ص25

ولا تزال هذه الجرائم تنفذ بأساليب احترافية في ظل غياب أو قصور في التشريعات لمواجهة هذا النوع من الجرائم التقنية، فالمشرع الجزائري تعامل مع فعل الإحتيال في حد ذاته واعتبره عنصرا أساسيا من عناصر الركن المادي في جريمة النصب والاحتيال بالطرق العادية وليس الإلكترونية او المعلوماتية، وهذا ما ورد في نص المادة 372 من قانون العقوبات[1].

إلى جانب ذلك هنالك قصور غياب للنصوص الإجرائية الكفيلة بملاحقة مرتكبي هذه الجرائم التي تتعدد صورها ومجالاتها، كجرائم الإعتداء على الأموال أو الأنظمة المالية وجرائم الإحتيال باستخدام بطاقة الدفع الإلكتروني وكذا جرائم الاحتيال المعلوماتية أو الغش المعلوماتي الذي ينجم عنه أضرار مادية جمة.

إلا أن هذه الأخيرة قد تجد الحماية من خلال ما ورد في نص المادة 394 من قانون العقوبات [2]المرتبطة بالدخول والبقاء غير المشروع، ولكن في غير هذه الحالة نعود إلى نفس القوانين العادية والإجراءات التقليدية.

الفرع الثاني: المساس بحرمة الحياة الخاصة ونشر المعطيات الشخصية دون رضى.

تعد الحياة الخاصة قطعة أساسية من كيان الإنسان، لا يمكن انتزاعها منه، وأن احترامها يعد من المبادئ الدستورية الثابتة، بحيث يَعد الدستور بأن لحياة المواطنين الخاصة حرمة يحميها القانون، فلكل شخص الحق في أن تظل أسرار حياته الخاصة محجوبة عن العلنية ومضمونة من تدخل الغير واستطلاعه وهو ما يعبر عنه بمبدأ الخصوصية للأفراد وهو أحد الحقوق اللصيقة بالشخصية وذلك لما له من ارتباط وثيق بحرية الفرد، غير أن المعلوماتية بتقنياتها الحديثة وبما توفره من قدرة هائلة على جمع المعلومات والبيانات الشخصية وتخزينها واسترجاعها وتصنيفها وتحليلها ومعالجتها ومن ثم تبادلها وتناقلها دون أي عائق تقني يشكل تهديدا حقيقيا على حق الأفراد في

---

[1] –المرجع نفسه، ص 25.

[2] _ القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 والمتضمن تعديل قانون العقوبات، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم: 71 الصادرة يوم 10 نوفمبر 2004.معدل و متمم

احترام حياتهم الخاصة خصوصا مع ظهور ما يعرف ببنوك المعلومات[1]، ومن هنا كان من الواجب التصدي للإجرام المعلوماتي الذي أصبح يشكل تهديدا صريحا على حقوق الإنسان وهو الحق في الحياة الخاصة، وهي جريمة منصوص عليها في المادة 14 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ذلك أن دساتير الدول تكفل حق الشخص في حماية حياته الخاصة[2].

والمشرع الجزائري نص على هذه الجريمة في المادة 394 مكرر من قانون العقوبات التي تقرر الحماية القانونية للمعلومات الشخصية الموجودة داخل نظام البيانات، لذلك يطلق البعض على هذه الجريمة بالقرصنة المعلوماتية.

وتشكل جرائم الاعتداء على حرمة الحياة الخاصة للإفراد جزءا مهما من النشاط الإجرامي المعلوماتي الذي يهدد بخطر محدق للبيانات الشخصية للأفراد من عدة زوايا نوجزها فيما يلي:

1) **الإفشاء غير المشروع للبيانات الشخصية:** حيث يعتبر الإفشاء غير المشروع من السلوكات الإجرامية سواء عن طريق الخطأ أو لغير الهدف الذي جمعت له، ذلك أن البيانات قد انتقلت من السر إلى العلانية بمجرد تخزينها بعد تجميعها على نحو غير مشروع أو حتي بصفة مشروعة، وبالتالي فإنها تكون عرضة للإطلاع عليها من قبل عدد غير محدد من الأشخاص في حال عرضها على شبكة الأنترنت أو على الأقل عدد محدد متمثل في الأشخاص العاملين في فضاء المعلوماتية، ومثال ذلك المعلومات المتحصل عليها من عملية الإحصاء السكاني فلا يجوز استعمالها لغير هذا الهدف ولو كان مشروعا مثل استعمالها في الأغراض الضريبية لكونها لم تستعمل في الإطار المحدد الذي جمعت من أجله[3].

---

[1] -ربيعي حسين، المرجع السابق، ص92.

[2] -عرفت المادة 14 من الاتفاقية العربية لمكافحة الجريمة المعلوماتية جريمة الإعتداء على حرمة الحياة الخاصة باعتبارها جريمة معلوماتية أنها:(الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات).

[3] -حمبلي عمار، عثماني دليلة، جرائم تقنية المعلومات في ظل الإتفاقية العربية 2010 وفي التشريع الجزائري، مذكرة لنيل شهادة الماستر حقوق، تخصص قانون جنائي وعلوم جنائية، جامعة قاصدي مرباح ورقلة، الجزائر، 2022/2021، ص42.

2) **جمع البيانات وتخزينها على نحو غير مشروع:** وتتحقق هذه الصورة بالجمع والتخزين لبيانات شخصية تخص أشخاص ويتم هذا الجمع أو التخزين بصورة غير قانونية مع أشخاص أو جهات ليس لديهم الحق في القيام بهذا الجمع أو التخزين لهذه البيانات، كما يتحقق الركن المادي لهذه الجريمة بتحقق الجمع أو التخزين لبيانات شخصية لأشخاص بشكل غير مشروع، أما الركن المعنوي يتحقق بعلم الجاني بأنه يقوم بجمع أو تخزين هذه البيانات الشخصية بشكل غير مشروع واتجاه إرادته إلى ذلك[1].

3) **استخدام بيانات شخصية غير صحيحة (انتحال شخصية):** وترتكز جريمة انتحال شخصية على مبدأ التعدي على البيانات الإسمية للغير من أجل التخفي والتهرب من المسؤولية، أي الإفلات من المتابعة الجزائية، بمعنى استخدام بيانات الغير الشخصية من أجل الوصول إلى هدف غير مشروع يتمثل في جريمة تحقق الربح المادي لمقترفها دون أن يكون هو المتابع بشأنها، وقد أشارت الإحصائيات السنوية لسنة 2009 أن حوالي 210000 شخص في فرنسا وقعو ضحية هذا النوع من الإجرام عبر الأنترنت، ويقدر معدل نموها على مستوى الدول الغربية ب40 % [2]، فالشخص أصبح معرض لانتحال هويته من قبل الغير بسبب اعتماده المطلق أو شبه الدائم على تقنية المعلومات وشبكة الأنترنت خصوصا، ضف إلى ذلك أن وسائل التحقق من الشخصية عبر الأنترنت هي غير تلك المتبعة أمام الجهات الرسمية، فاسم المستخدم وكلمة السر والعنوان المنطقي ورقم البطاقة البنكية هي وسائل إثبات الهوية المعلوماتية وهي الأجدر بالحماية مقارنة بالإسم واللقب والصورة.

4) **جرائم القذف والتشهير عبر الأنترنت:** وتعد جرائم القذف والسب والتشهير والتحقير من أكثر الجرائم شيوعا في نطاق شبكة الأنترنت، ففي إطار مجتمع المعلومات الإلكترونية يجد العابثون حرية في نشر وبث رسائل تحتوي عبارات الذم والقدح والتحقير تجاه الآخرين مستهدفين بذاتهم بصفة وجاهية أو غيابية أو بواسطة الوسائط الإلكترونية السمعية أو السمعية البصرية، وغالبا ما تقع هذه الجرائم بوصفها الحديث الإلكتروني تحت سلطة

[1] -ربيحي حسين، مرجع سابق، ص 96.
[2] -حمبلي عمار، عثماني دليلة، المرجع السابق، ص 96.

النصوص التقليدية مما يخلق إشكالا في أمر إثباتها، ولقد قدر المشرع الجزائري الأمر من خلال نص المادة 394 مكرر من قانون العقوبات.

المطلب الثاني: التجريم المستحدث للإعتداءات على أنظمة المعالجة الآلية.

إن وضع نصوص قانونية جنائية لمواجهة الجرائم المعلوماتية كان وليد جدل فقهي حول مدى قابلية النصوص الجنائية التقليدية لتشمل على هذا النوع من القيم الجديدة، وحقيقة الأمر أن الإتجاه الفقهي القائل بإمكانية ذلك لم يكتب له النجاح، لأن تبني هذه الأفكار سيؤدي إلى تشويه المبادئ المستقرة التي تقوم عليها تلك الجرائم، الأمر الذي سيؤدي بدوره لا محالة إلى وجود ثغرات قانونية[1]،لأن نظام المعالجة يعتبر الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الإعتداء على نظام المعالجة، فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2]،وهو ما جعل الفكر القانوني يستقر ويقتنع بضرورة وضع نصوص قانونية خاصة بهذه الجرائم.

وبما أنه لا يمكن مواجهة الجريمة المعلوماتية دون توفر حماية كافية للمجال والنطاق الذي تتواجد فيه المعلومة، فقد حاول المشرع الجزائري مكافحة الجرائم الماسة بالأنظمة والبرامج المعلوماتية (أنظمة المعالجة الآلية للمعطيات)، ومن ثمة حماية المعلومات المتواجدة في هذه الأنظمة، فعمد إلى تجريم المساس بالأنظمة والبرامج بموجب القانون رقم 09_04 في المواد من 494 مكرر إلى 394 مكرر7 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

[1] -د/خضراوي الهادي، تجربة الجزائر في مكافحة الجريمة الإلكترونية، بحوث المؤتمرات، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية المتحدة، الرياض، 2016، ص153.

[2] -وهيبة رابح، الجريمة المعلوماتية في التشريع الجزائري، مجلة الباحث للدراسات الأكاديمية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، ديسمبر2014،ص321.

وتجدر الإشارة إلى أن المشرع الجزائري قد صادق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد جرمت هذه الإتفاقية المساس بالبرامج والأنظمة في المواد 7و 8و 9 منها[1].

وبالرجوع إلى النصوص القانونية السالفة الذكر نجد أن المساس بأنظمة المعالجة الآلية للمعطيات يأخذ صور مختلفة تتغير بتغير السلوك المرتكب، نتناولها كما يلي:

الفرع الأول: الدخول والبقاء الإحتيالي في النظام المعلوماتي.

تعرف جرائم الدخول والبقاء غير المشروع أو جرائم اختراق نظام المعلومات بشكل عام أنها القدرة على الوصول لهدف معين بطريقة غير مشروعة (بطريق الغش) عن طريق ثغرات في نظام الحماية الخاص بالهدف، وهي سمة سيئة يتسم بها المخترقون لقدرتهم على دخول أنظمة الآخرين عنوة ودون رغبة منهم ودون علمهم بغض النظر عن الأضرار التي قد تحدث، وتعد هذه الأنشطة الإجرامية الأكثر انتشارا[2].

ويعد الدخول والبقاء غير المشروع أو غير المصرح به للنظم المعلوماتية سابقة ضرورية كنشاط إجرامي لأجل ارتكاب جرائم معلوماتية أخرى كإتلاف المعطيات أو سرقتها أو التلاعب بها.

أولا: فعل الدخول: تتسع هذه العبارة على إطلاقها لتشمل كافة فنيات الدخول الإحتيالي في منظومة محمية كانت أوغير محمية، كما تشمل استعمال من لاحق له في ذلك مفتاح الدخول في منظومة[3]، فيتحقق الدخول بالولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام.

---

[1] -صادق المشرع الجزائري على **الإتفاقية العربية لمكافحة جرائم تقنية المعلومات**، المحرر بالقاهرة سنة 2010، بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 2014/09/08، جريدة رسمية ج ج، العدد 57 ، المؤرخة في 2014/09/28.

[2] - بن قويدر أمل، بوصبع عفاف ، **الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري**، مذكرة لنيل شهادة الماستر حقوق، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، 2025/2024، ص 51.

[3] -أحمد بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة 11، دار هومة، الجزائر 2010، ص 453.

كما أن فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي، أي الدخول المعنوي الإلكتروني[1]، ويتحقق فعل الدخول بمجرد الوصول إلى المعلومة المخزنة داخل النظام ودون علم ورضا صاحبه لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن بمقابل نفقات مالية معينة، ولم يحدد المشرع وسيلة للدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأي وسيلة أو طريقة، ويكفي أن يتم الدخول مباشرة أو عبر طريق غير مباشر بشرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو خطأ.

وتجدر الإشارة إلى أن جريمة الدخول إلى النظام المعلوماتي هي جريمة شكلية، أي أنها تتحقق بمجرد الدخول إلى نظام معلوماتي ولا يشترط لاكتمال الركن المادي فيها أن يتم الوصول إلى المعطيات التي يحويها النظام أو إحداث ضرر بصاحب هذه المعطيات، لأن الغرض من تجريم فعل الدخول هو حماية سلامة النظام في حد ذاته وليس حماية سلامة المعطيات المعالجة، لذلك لا تتوفر الجريمة إذا تم الدخول إلى عنصر لا علاقة له بنظام المعالجة الآلية للمعلومات كالدخول إلى برنامج منعزل عن غيره من العناصر، أو أن يقتصر الشخص على مجرد قراءة الشاشة.

ثانيا: فعل البقاء: ويكون هذا السلوك المجرم متحققا بتواجد الجاني داخل النظام المعلوماتي بدون رضا من له الحق في التحكم فيه، ويكون ذلك إما بعد الدخول غير المشروع في النظام أو في حالة البقاء داخل النظام بعد نفاذ الوقت المحدد للبقاء داخله (كثيرا ما يحدث ذلك إذا كان استعمال النظام بمقابل محددا بمدة زمنية معينة)[2]، ويظهر ركنها المادي على أنه نشاط مكمل لجريمة الدخول غير المشروع، ويقصد به الحالات التي يكون فيها الدخول

[1] -بن قويدر أمل، بوصبع عفاف، مرجع سابق، ص 54.
[2] - خضراوي الهادي، مرجع سابق، ص 156.

مشروعا متبوعا ببقاء غير مشروع ويتجلى ذلك في حرمان الفاعل من حق البقاء داخل النظام المعلوماتي، حيث يكون البقاء معاقبا عليه استقلالا حين يكون الفاعل داخل النظام بالصدفة أو عن طريق الخطأ أو السهو إذا كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، وأن ذلك ضد رغبة مالك النظام أو صاحب السيطرة عليه، وتقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يجرم البقاء حتى ولو حصل الدخول بصفة عرضية أي بالصدفة أو عن طريق الخطأ وأصر الفاعل على البقاء داخل هذه المنظومة المعلوماتية، بمعنى أنه يكفي لتحقق عنصر البقاء مجرد التواجد داخل كل أو جزء من النظام ولا يشترط أن يضاف إليه التقاط المعلومات أو محوها أو إتلافها، بل مجرد التجول يكفي لقيام هذا السلوك المجرم[1]، والمعاقب عليه بموجب المادة 394 مكرر فقرة 1 من قانون العقوبات الجزائري[2].

ففعل الدخول غير المشروع أو البقاء داخل النظام المعلوماتي يشكلان جريمة إذا ما اقترفتا بطريق الغش وهو دليل على ضرورة توافر القصد الجنائي (العلم/الإرادة)، وأن الفاعل كانت له النية في إتيان فعل مخالف للقانون.

الفرع الثاني: التخريب الإلكتروني (الإتلاف المعلوماتي):

ويقصد به الإعتداء الذي يهدف إلى الإضرار بمعلومات النظام أو وظائفه سواء بالمساس بسريتها أو المساس بسلامتها أو بتعطيل قدرتها وكفاءتها بشكل يمنعها من أداء وظيفتها بشكل سليم، ويتحقق فعل التخريب أو الإعتداء على معطيات النظام عادة بتجاوز مرحلة الدخول والبقاء في نظام المعالجة[3] وبالتالي فهو نتيجة حتمية للجريمة الأولى، فالجاني يهدف إلى تعطيل سير نظام المعالجة أو جعل هذا النظام غير قادر على أداء وظيفته أو مهامه بصورة جيدة باستخدام أساليب وأفعال ولكنها لا تخرج عن الإعاقة أو الإخلال[4].

---

[1] - خضراوي الهادي، مرجع سابق، ص156.

[2] -المادة 394 مكرر من قانون العقوبات الجزائري: "يعاقب بالحبس من 03 أشهر إلى سنة وبغرامة من 50000دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك".

[3] -رزيقة بونار، **الجريمة المعلوماتية في التشريع الجنائي الجزائري**، مذكرة لنيل شهادة الماستر في القانون العام، تخصص قانون عام داخلي، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل 2021/2020،ص 24.

[4] -خضراوي الهادي، مرجع سابق، ص 158.

وقد وضحت ذلك المذكرة التفسيرية لاتفاقية **بودابست** لسنة 2001، بأنه "**تخريب نظام الحاسوب بهدف الإعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية بما في ذلك نظم الاتصالات باستخدام أو التأثير على الحاسوب**".

وبدوره المشرع الجزائري تطرق لهذا النوع من الجرائم من خلال المادة 394 مكرر من القانون 05/04 المتضمن قانون العقوبات[1]، والتي أكد من خلالها بضرورة توفر القصد الجنائي لأجل قيام المسؤولية الجنائية في مجال هذا النوع من الجرائم، وبالتالي يستثنى من نطاق التجريم نفس الأفعال إذا لم تقترن بنية إحداث الضرر.

اولا: إعاقة السير العادي للنظم المعلوماتية: ويقصد بإعاقة سير عمل النظام المعلوماتي ذلك الفعل الذي يسبب تباطؤ في عمل النظام أو ارتباكا مما يؤدي إلى تغيير في حالة عمل النظام على نحو يصيبه بالشلل الكلي أو المؤقت، فيتحقق الركن المادي لهذا النوع من الجريمة من خلال وقوع اعتداء على نظام معلوماتي يسبب ارتباكا في عمله قد يكون دائما في حال استعمال الفيروسات أو مؤقتا يهدف إلى شل أو تعطيل النظام كما هو الحال في حالة استعمال القنابل المنطقية، أو من خلال إغراق الخادم بالرسائل الإلكترونية لأجل الحد من قدرته على التعامل مع المعلومة[2].

وتجدر الإشارة إلى أن المشرع لم يتعرض في نص المادة 394 مكرر من قانون العقوبات الجزائري إلى مفهوم إعاقة السير العادي للنظم المعلوماتية وهو السلوك الإجرامي الذي أولته اتفاقية بودابست أهمية بالغة.

وعلى كل حال فإنه يجب أن تكون الإعاقة دون وجه حق وبالتالي فإن أولئك الذين يكون لهم الحق في إطار ممارسة أنشطتهم تصميم الشبكات أو تشغيلها وصيانتها واختبارها، لا تعتبر أنشطتهم غير مشروعة إذا ما تسبب في إعاقة النظام.

[1] -المادة 394 مكرر من قانون العقوبات الجزائري: "يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 50000دج إلى 200000دج كل من أدخل بطريق الغش معطيات في نظام أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها".

[2] -بن قويدر،بوصبع عفاف، مرجع سابق،ص59.

ثانيا : المساس بسلامة المعلومة: إن المساس بسلامة المعلومة كسلوك مجرم محصور في فعل التعديل أو الحذف للمعطيات المعلوماتية المخزنة في ذاكرة الحاسوب أو على الشبكة هو ما اتفقت عليه أغلب التشريعات، وهو ما جاء في نص المادة 394 مكرر 1 من قانون العقوبات الجزائرية.

واستنادا لذلك فإن الركن المادي لهذه الجريمة يقوم من خلال:

أ/ حذف أو محو البيانات كليا وتدميرها الكترونيا كمحو الذاكرة الرئيسية للحاسوب أو استعمال برمجيات خفية تعمل على محو محتوى الحاسوب أو الشبكة ويكون ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرامج الممحاة أو برامج الفيروسات بصفة عامة مثل فيروس (حصان طروادة) أو (الدودة) التي تعمل على تعطيل وإيقاف نظام الحاسوب الآلي كلية[1].

ب/ تعديل البرامج والمعطيات المعلوماتية من خلال:

*التلاعب بالبرامج، أي بالنظام المعلوماتي بشكل يؤدي إلى إخفاء البيانات كليا أو جزئيا.

*اختلاس البرامج، ويكون ذلك عن طريق نسخها باستعمال أسلوب التجسس.

*تغيير نظام عمل البرنامج، أي بتزويدها بتعليمات إضافية تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسوب.

ج/ إدخال برامج جديدة، أي اصطناع برنامج كامل أو ناقص في الناحية الفنية يخصص لارتكاب فعل الغش المعلوماتي.

بالإضافة إلى أن المادة 394 مكرر 1 من قانون العقوبات الجزائري تؤكد على ضرورة توافر القصد الجنائي لأجل قيام المسؤولية الجنائية في مجال هذا النوع من الجرائم، حيث يتوفر القصد الجنائي بمجرد إدخال أو تعديل أو

[1] -رزيقة بونار، مرجع سابق، ص28.

حذف المعلومة المقترنة بإرادة التعديل على نظام معلوماتي مهما كانت النتيجة المتوقعة أو غير المتوقعة على النظام، وبالتالي يستثنى من نطاق التجريم نفس الأفعال إذا لم تقترن نية إحداث الضرر.

المبحث الثاني: الآليات المؤسساتية لمواجهة الجريمة المعلوماتية.

في ظل التطورات الواسعة الحاصلة في مجال العلوم الرقمية والتكنولوجية واستحداثها، تنوعت وتعددت سبل الجريمة الإلكترونية وأصبحت أشد ضررا مما أدى إلى زيادة الغموض المحيط بها، حيث أصبح من اللازم وضع طرق وآليات فعالة لمعالجة هذه الظاهرة والحد منها، لذا تم إنشاء جهاز خاص للتحقيق في الجريمة الإلكترونية ويتكون من وظائف متخصصة إلكترونيا وقانونيا، وفي الجزائر توجد هيئات ووحدات متخصصة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال بالإضافة إلى وحدات تابعة للأمن والدرك الوطني وكذا هيئات قضائية متخصصة في البحث والتحري عن الجريمة تتمثل في الأقطاب الجزائية المتخصصة ، ومن جهة أخرى حاولت الدول أن تبحث عن آليات مشتركة لتنسيق المواقف حول ما يعرف بالتعاون الدولي والمساعدة القضائية الدولية.

وهو ما سنحاول معالجته من خلال هذا المبحث، حيث سنتطرق إلى دور الأجهزة الأمنية والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها في المطلب الأول، ثم إلى أهمية التعاون الدولي في تتبع المجرمين المعلوماتيين.

المطلب الأول: دور الأجهزة الأمنية والهيئات الوطنية.

إلى جانب النصوص القانونية تلعب الهيئات والمؤسسات العامة دورا محوريا في مكافحة الجرائم الإلكترونية، وفي الجزائر تتولى عدة جهات هذه المهمة ضمن إطار اختصاصاتها العامة، حيث تأتي في مقدمة هذه الجهات مصالح الأمن الوطني ممثلة في (المديرية العامة للأمن الوطني) والدرك الوطني، التي أنيطت بها مهام البحث والتحري عن الجرائم بشكل عام بما في ذلك الجرائم الإلكترونية، وقد سعت هذه المصالح إلى تطوير قدراتها في هذا المجال من خلال إنشاء وحدات متخصصة مثل (المصالح المركزية والجهوية لمكافحة الجريمة السيبرانية) وتكوين أفرادها على التقنيات الحديثة للتحقيق الرقمي.

كما يلعب القضاء دورا مركزيا في مكافحة هذه الجرائم من خلال الإشراف على التحقيقات والفصل في القضايا المعروضة عليه، وتطبيق العقوبات على المدانين، وتجدر الإشارة إلى أن الأمر رقم 11/21[1]، قد استحدث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وهو ما يعد نقلة نوعية ضمن جهود تعزيز التخصص القضائي في هذا المجال[2].

وسنحاول من خلال هذا المطلب استعراض الدور الذي تلعبه الوحدات التابعة للأمن الوطني وتلك التابعة لقيادة الدرك الوطني، وكذا التطرق إلى أبرز الهيئات المتخصصة في مجال مكافحة الجرائم المعلوماتية والتي عادة ما تستند إليها مهام الوقاية ومكافحة الجرائم المعلوماتية والتحقيق فيها.

[1] -الأمر رقم 11/21 المؤرخ في 25 أوت 2021، المعدل والمتمم لقانون الإجراءات الجزائية، الصادر في الجريدة الرسمية ، العدد 65، 2021.
[2] -شريف خالد، **الجرائم المتصلة بتكنلوجيا الإعلام والإتصال في التشريع الجزائري**، مجلة البيبان للدراسات القانونية، جامعة محمد خيضر بسكرة، الجزائر، المجلد 10 ، العدد 01، جوان 2025، ص132.

الفرع الأول: دور مصالح الشرطة والدرك الوطني في التحقيق الرقمي.

أولا: جهاز الأمن الوطني: حيث تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم المعلوماتية على المستويين: المركزي والجهوي.

أ/على المستوى المركزي: حيث بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، ولذلك قامت باستحداث عدة مصالح متخصصة في شكل "**نيابة مديرية**"، وبخصوص مكافحة الجريمة المعلوماتية فقد أسندت المهمة **لنيابة مديرية الشرطة العلمية والتقنية**، هذه الأخيرة التي تضع لخدمة هذا الهدف مصالح عملية مختصة لذلك والتي تتولى أعمال البحث والتحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[1]، وهذه الوحدات هي:

1- المخبر المركزي للشرطة العلمية (مقره بالجزائر العاصمة).

2- المخبر الجهوي للشرطة العلمية (مقره ولاية قسنطينة).

3- المخبر الجهوي للشرطة العلمية (مقره ولاية وهران).

بالإضافة إلى (03) ثلاث مخابر أخرى قيد الإنجاز على مستوى ولايات (ورقلة/بشار/تمنراست) ينتظر تسليمها لأجل تعميم هذا النوع من النشاط من أجل تغطية جميع أنحاء البلاد[2].

حيث يتولى كل مخبر سواء المركزي أو الجهوي مهمة البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها.

[1] -بن قويدر أمال، بوصبع عفاف، مرجع سابق، ص34

[2] -عزة خولة، ربيع شيماء، **آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مذكرة لنيل شهادة الماستر أكاديمي، تخصص قانون إعلام آلي وأنترنت، كلية الحقوق و ع س، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2024/2023، ص61.

ب/ على المستوى الجهوي: حيث تم إنشاء مخابر جهوية للشرطة الجهوية العلمية في كل من ولاية قسنطينة ووهران بالإضافة إلى 03 أخرى قيد الإنجاز، ويختص كل مخبر بأعمال البحث والتحقيق بشأن الجرائم المعلوماتية تحت تسمية "دائرة الأدلة الرقمية والآثار التكنولوجية"، وهذه الأخيرة بدورها تنقسم إلى أقسام فرعية هي:

1- قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

2- قسم استغلال الأدلة الناتجة عن الهواتف الذكية.

3-قسم تحليل الأصوات.

حيث أن هذه الدائرة تلعب دورا مهما في محاربة الجرائم المعلوماتية والكشف عن خبايا وأسرار هذه الجرائم بمختلف أشكالها، وذلك من خلال مختلف الإجراءات التي تباشرها أثناء تلقي الطلبات المقدمة لها أثناء مرحلة التحقيق القضائي أو أثناء مرحلة البحث والإستدلال[1].

ثانيا: جهاز الدرك الوطني: ويعتبر هذا الجهاز جزءا هاما من قوات الأمن المكافحة للجريمة بشكل عام والجريمة الإلكترونية بشكل خاص، حيث 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 سنة 2004، وهذا ما يعكس التزام الدولة في الحفاظ على الأمن والطمأنينة في الفضاء السيبراني الوطني، ليتم بعدها إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها والتي يعد اليوم العصب الذي يسير مهام المكافحة واليقظة وفرض احترام القوانين في الوقت الذي يبحر فيه الملايين من المستخدمين عبر صفحات الأنترنت سواء من الخواص أو المؤسسات في الفضاء الإلكتروني.[2]

[1] -حنان حفافصة، **إجراءات البحث والتحري في الجرائم المعلوماتية**، مذكرة لنيل شهادة الماستر (ل.م.د)، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة تبسة، 2021/2020،ص 23.

[2] _عزة خولة،ربيع شيماء، مرجع سابق،ص61

وقد عمل المركز السالف الذكر منذ إنشائه سنة 2008 على تأمين منظومة المعلومات لخدمة الأمن العمومي، بحيث يهدف ضابط أو عون الشرطة القضائية المكونين 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، ضف إلى ذلك فإن هذا المركز استطاع معالجة أكثر من 1200جريمة إلكترونية سنة2018 و1635 قضية رقمية سنة 2019، وسنة 2020 تم معالجة 1654 قضية ، و في سنة 2021 تم معالجة2413 قضية، و في سنة 2022 تم معالجة 2316 قضية ،في سنة 2023 تم معالجة 2050 قضية[1]

كما قامت قيادة الدرك الوطني بمجموعة من البرامج التوعوية بالتنسيق مع وزارة التربية الوطنية بتقديم دروس توعوية في المدارس، باعتبار أن الأطفال هم أكثر الفئات العمرية تضررا من الجريمة الإلكترونية كخطوة أولية نحو زيادة الوعي الطلابي بمخاطر الجريمة الإلكترونية وحمايتهم منها.

فلا بد من السعي لمواكبة التطورات والمستجدات الحاصلة في مجال التكنولوجيا، لذلك عمل جهاز الدرك الوطني على تكوين إطارات وأعوان الدرك وبشكل متواصل وذلك من خلال إنشاء مدارس ومعاهد لهذا الغرض، كمدرسة الشرطة القضائية التابعة للدرك الوطني والمعهد الوطني للشرطة[2]

[1] _ الرائد: درامشية فريد - المصلحة المركزية لمكافحة الإجرام السيبراني - قيادة الدرك الوطني ،الجريمة السيبرانية بالجزائر التحديات وآليات المواجهة، الملتقى الوطني حول الجريمة المعلوماتية، الجزائر يومي 24 و 25 سبتمبر 2023،ص10

[2] -عزة خولة، ربيع شيماء، مرجع سابق، ص 62

الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها.

ترجع فكرة انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إلى تاريخ 2009/08/05، وتعتبر الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي ومقرها بالجزائر العاصمة، وهذا بموجب القانون رقم 04/09 الذي وضعها تحت اشراف ورقابة وزير العدل.

وتعتبر هذه الهيئة الوطنية المستحدثة والمنشأة بموجب المادة 13 من القانون رقم 04/09 السالف إحدى الآليات المؤسساتية الهامة في هذا المجال، وقد حدد المرسوم الرئاسي رقم 261/15 المؤرخ في 2015/10/08 تشكيلها وتنظيمها وكيفيات سيرها، حيث تحتوي على مجموعة من المهام الاستشارية والرقابية والتقنية والحيوية[1]، فهي تكلف بتجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات، والجرائم الأخرى تحت سلطة القاضي المختص[2].

أ)تشكيل الهيئة وطبيعة عملها:

1/ تشكيل الهيئة وطبيعة عملها: تتشكل الهيئة من اللجنة التي تديرها، إضافة إلى مديرية هامة، فاللجنة التي تديرها تتكون من وزير العدل رئيسا إضافة إلى وزير الداخلية والوزير المكلف بتكنولوجيا الإعلام والاتصال وقائد الدرك الوطني والمدير العام للأمن الوطني وممثلين أحدهما عن رئاسة الجمهورية وآخر عن وزارة الدفاع وقاضيان من المحكمة العليا، أما المديرية العامة يترأسها مدير عام يعين بموجب مرسوم رئاسي[3].

---

[1] - شريف خالد، مرجع سابق، ص 134

[2] -عزة خولة، ربيع شيماء، مرجع سابق، ص57.

[3] -المواد من 06 إلى 10 من المرسوم الرئاسي 261/15 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلاو والإتصال ومكافحتها.

2/ تشكيل الهيئة التقنية: إضافة إلى اللجان الإدارية تضم الهيئة مديريات تتسم من حيث مهامها بالطابع التقني باعتبارها المختصة بإنجاز المهام التقنية المتعلقة بالوقاية وبمكافحة الجرائم المعلوماتية، وهذه المديريات هي:

❖ **مديرية المراقبة والوقاية الإلكترونية:** لم يشر المرسوم الرئاسي رقم 261/15 إلى تشكيلة هذه المديرية، غير أنه من خلال تحليل نص المادة 18 منه يمكن تحديد تشكيلتها في مجموعة من الضباط وأعوان الشرطة القضائية والمختصين في المجال المعلوماتي من سلك الأمن الوطني والدرك الوطني والمصالح السكرية للاستعلامات والأمن، يعينون بموجب قرارات مشتركة بين الوزراء المكلفين، يساعدهم مستخدمي الدعم التقني والإداري من نفس الأسلاك[1]، من مهامها:

– تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.

– إرسال المعلومات المتحصل عليها إلى السلطات القضائية ومصالح الشرطة القضائية.

– جمع كل المعلومات واستغلالها من أجل الكشف عن الجرائم المعلوماتية.

– المشاركة في حملات توعوية حول مخاطر تكنلوجيا الإعلام والإتصال.

ولعل ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية وكذلك الملحقات مما يبرز دورها الفعال في تسيير وتأطير الأعمال المتعلقة بالوقاية أو بمكافحة الجرائم المعلوماتية، وبالتالي يمكن وصفها بأنها " **المركز العملياتي للهيئة**"[2].

❖ **مديرية التنسيق التقني:** لم ينص أيضا المرسوم رقم 261/15 على تشكيل هذه المديرية مما يترك المجال للقول بأن تشكيلتها تكون بناءا على قرارت مشتركة بين وزراء العدل / الداخلية/ الدفاع، غير أنها تختلف عن المديرية الأولى من حيث المهام الموكلة إليها، فتتمثل مهامها أكثر في الدور الوقائي والإعلامي من خلال توليها:

[1] -ربيحي حسين، مرجع سابق، ص 174.
[2] -المواد 11-13-14 والمواد 18-و 21 من المرسوم الرئاسي رقم 261/15. المرجع السابق.

- إنجاز الخبرات القضائية في مجال اختصاص الهيئة.
- تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي.
- إعداد الإحصائية الوطنية للإجرام المعلوماتي.
- تسيير المنظومة المعلوماتية وإدارتها.[1]

ب) إختصاصات الهيئة: حدد المرسوم الرئاسي رقم 261/15 المهام الأساسية التي تكلف بها الهيئة والمذكورة على سبيل الحصر في المادة 2/04 والهادفة إلى الوقاية من الجرائم المعلوماتية ومكافحتها من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية، أبرزها:[2]

- إقتراح عناصر استراتيجية وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.
- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها من أجل استعمالها في الإجراءات القضائية
- المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.
- تنفيذ الطلبات الصادرة عن الدول الأجنبية وتطوير سبل التعاون والتبادل معها.
- المساهمة في تحديث المعايير القانونية في مجال تخصصها.

---

[1] -المادة 12 من المرسوم 261/15، مرجع سابق.

[2] _ المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية ، العدد 53،بتاريخ 08 أكتوبر 2015.

ومن خلال استعراض الهيكل العام للهيئة ومجال اختصاصها، يتضح لنا جليا مدى اقتناع الهيئة التشريعية بضرورة تفعيل دور الهيئة في مجال الوقاية ومكافحة الجرائم المعلوماتية ولو بشكل متأخر، نظرا لتوسع تطبيقات تقنية المعلومات في المجتمع الجزائري على الصعيدين الحكومي والاجتماعي وهو ما ينبئ بتنامي الإجرام المعلوماتي وازدياد حجم التهديدات التي يشكلها على سلامة الأنظمة المعلوماتية وأمن المعطيات المخزنة والمتداولة عبرها.

المطلب الثاني: أهمية التعاون الدولي في تتبع المجرمين المعلوماتيين.

إن ارتباط كل دول العالم بشبكة الاتصالات الرقمية الدولية من خلال الأقمار الصناعية وشبكة الأنترنت، جعل أمر عولمة الجريمة أمرا ممكنا وشائعا، فأصبحت الجريمة لا تعترف بمفهوم الحدود الإقليمية للدول واكتسحت الساحة العالمية، فهي تعد جريمة ذات بعد دولي أي أنها عابرة للحدود الوطنية، فالجهود الوطنية وحدها لم تعد كافية لمواجهة مثل هذه الجرائم ولذا فإن مكافحتها لا تتحقق إل بوجود تعاون دولي وتدخل المجتمع الدولي بمختلف الهيئات والمنظمات المتخصصة على المستوى الإجرائي والجنائي، إضافة إلى ذلك فالتحقيقات المتبادلة في الجريمة الإلكترونية وملاحقتها قضائيا تُبرز 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، وبالتالي برزت الحاجة إلى توحيد الجهود الدولية في هذا المجال وهو ما تجسد فعلا بعقد الكثير من المؤتمرات المتعلقة بالموضوع وإبرام اتفاقيات تخص المسألة، وعلاوة على ذلك تم وضع قوانين نموذجية لمواجهة هذه الجرائم في مجالات متعددة ومن أجل بيان تلك الجهود الأمنية[2]، واتخذت كمظاهر لهذا التعاون صورا عديدة ومتنوعة أهمها الاتفاقيات الثنائية والمتعددة الأطراف وكذا التعاون مع المنظمات العالمية المتخصصة الرائدة في هذا المجال كالمنظمة الدولية للشرطة الجنائية (الأنتربول) و(اليوروبول).

[1] -عزة خولة ، ربيع شيماء، المرجع السابق، ص67.
[2] -ذ/ يعيش تمام شوقي، الجريمة المعلوماتية(دراسة مقارنة)، الطبعة الأولى، جانفي 2019، مطبعة الرمال ، الوادي، الجزائر، 2019، ص 44.

الفرع الأول: الإتفاقيات الثنائية ومتعددة الأطراف.

تعتبر المعاهدات والاتفاقيات الدولية الأساس الذي يرتكز عليه التعاون الدولي في مكافحة الجرائم المعلوماتية، وقد تم عقد العديد من الإتفاقيات والمعاهدات التي تعمل على تعزيز التعاون الدولي في هذا المجال نذكر منها:

أولا: اتفاقية (برن) لحماية المصنفات الفنية والأدبية: وتم اعتمادها من قبل الدول المتعاقدة سنة 1886، وقد تجمعت الدول المتعاقدة على شكل إتحاد من أجل حماية حقوق مؤلف المصنفات المحمية بموجب الاتفاق، وسمي هذا الإتحاد بـ"اتحاد برن"، التي ينظر إليها على أنها الأب الشرعي لتنظيم حقوق المؤلف المجاورة على المستوى الدولي، خصوصا وأنها من أوائل الاتفاقيات التي تم التوصل لها لمعالجة سائر حقوق المؤلف.

وقد تمت مراجعة نصوص الاتفاقية عدة مرات، وتعرضت للتعديل أكثر من مرة في ضوء التطورات السريعة في مجال التكنولوجيا المتصلة بالمصنفات الأدبية والفنية، وقد كانت آخر ثلاث مراجعات خضعت لها الاتفاقية في بروكسل سنة 1948، وستوكهولم سنة 1967، وفي باريس سنة 1971[1].

وقد انضمت الجزائر إليها بتحفظ بموجب المرسوم الرئاسي 341/97 سنة 1997 المتضمن انضمام الجمهورية الجزائرية الديمقراطية الشعبية مع التحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، التي كان لها عدة تعديلات أهمها تعديل باريس 1971 وآخرها سنة1979 [2].

ولأهمية هذه الإتفاقية ودورها في توفير الحماية للمؤلفين وأعمالهم ولدت في أحكامها عدة نصوص ومبادئ نذكر منها:

- **مبدأ المعاملة الوطنية:** ويعني أن تتمتع المصنفات التي تم إعدادها في دولة من دول الإتحاد بالحماية في بقية دول الإتحاد، بنفس مستوى الحماية الممنوحة من تلك الدول لمصنفات مواطنيها.

[1] -عثماني رضوان، **مكافحة الجريمة المعلوماتية في القانون الجزائري والدولي**، أطروحة مقدمة لنيل شهادة الدكتوراء في العلوم ، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد، وهران، 2024/2023، ص134.

[2] -المرسوم الرئاسي رقم 341/97، المؤرخ في 1997/09/13، ج ر ج ج، العدد 66، بتاريخ 1997/09/14.

- **مبدأ الحماية التلقائية:** وتعني أن المصنفات تحمى بشكل تلقائي للمصنفات وبمجرد تأليفها، ولا تتوقف على أي تسجيل أو إيداع أو أي إجراء شكلي آخر.
- **مبدأ استقلالية الحماية:** وتعني أن التمتع بالحقوق الممنوحة للمصنف أو ممارستها لا يجوز أن تتوقف على وجود حماية في بلد المنشأ.

وتشمل عبارة المصنفات الأدبية والفنية كل انتاج في المجال الأدبي والعلمي والفني أيا كانت طريقة أو شكل التعبير عنه مثل الكتب والكتيبات وغيرها من المحررات والمحاضرات والخطب والأعمال الأخرى، وتعتبر هذه المصنفات المحمية على سبيل المثال لا الحصر، وقد تركت الاتفاقية حرية مد نطاق الحماية إلى بعض المصنفات الأخرى للدول الأعضاء، مثل حماية النصوص الرسمية ذات الطابع التشريعي أو الإداري أو القضائي ، أو مصنفات الفنون التطبيقية والمحاضرات والخطب، إلا أن الاتفاقية قد اشترطت تثبيت بعض المصنفات على دعامة مادية كشرط للحماية[1].

ثانيا: إتفاقية تربس: وتعد الإتفاقية من بين أهم الإتفاقيات التي أبرمت مع إنشاء منظمة التجارة العالمية سنة 1994، والتي تضمنت 73 مادة بغرض المساعدة في تحرير التجارة العالمية عن طريق تشجيع وتحفيز حقوق الملكية الفكرية، وأن تضمن بأن لا تكون التدابير المتخذة لإنفاذ حقوق الملكية الفكرية بحد ذاتها عائقا أمام التجارة الدولية[2].

وقد أقرت الإتفاقية مجموعة من القواعد لحماية بعض المصنفات والمواضيع المتعلقة بحقوق التأليف والحقوق المجاورة، والتي تميزت في بعض الأحيان بالحداثة عما سبقها من اتفاقيات مماثلة، ومن ضمن تلك الأمور على سبيل المثال النص على حماية برامج الحاسب الآلي وقواعد البيانات، فقد تضمنت الإتفاقية حماية برامج الحاسب

[1] -بن قويدر أمل، بوصبع عفاف، المرجع السابق، ص40.
[2] -عثماني رضوان، مرجع سابق، ص136.

الآلي سواء كانت بلغة المصدر أو بلغة الآلة باعتبارها من الأعمال الأدبية وفق مفهوم أحكام اتفاقية برن لحماية المصنفات الأدبية والفنية لعام 1971، كما نصت الاتفاقية كذلك على حماية البيانات المجمعة أو المواد الأخرى، سواء كانت في شكل مقروءة آليا أو أي شكل آخر، أو ما يسمى بقواعد البيانات إذا كانت تشكل عملا مبتكرا نتيجة انتقاء أوترتيب محتوياتها، وأن الحماية لا تشمل البيانات أو المواد في حد ذاتها، مع عدم الإخلال بحقوق المؤلفين المتعلقة بتلك البيانات أو المواد ذاتها[1].

وحسب المادة 11 من نفس الاتفاقية نصت وبشكل إلزامي للبلدان الأعضاء في منظمة التجارة الدولية بمنح المؤلفين وخلفائهم حق إجازة أو حظر تأجير أعمالهم الأصلية المحمية تأجيرا تجاريا للجمهور، وقد قيدت الاتفاقية أيضا حق الإجازة أو الحظر على التأجير فيما يتعلق ببرامج الحاسب الآلي حينما لا يكون البرنامج نفسه الموضوع الأساسي[2].

ثالثا: معاهدة الويبو (wipo): (المنظمة العالمية للملكية الفكرية) وتعد هذه المنظمة المتخصصة للأمم المتحدة مسؤولة عن تعزيز وحماية الملكية الفكرية على أساس دولي، وهي تبحث في إنشاء الآليات التعاونية التي تحد من المشكلات التي تواجه الملكية الفكرية، حيث عقدت مؤتمرها الدولي الذي تمخض علم 1996 عن اتفاقية حق النشر للمنظمة العالمية للملكية الفكرية، المتضمن لحق النشر المرتبط بالتكنولوجيا الرقمية وخاصة الأنترنت، كما أنها تعتبر المسؤولة عن الاتفاقيات المتعددة الأطراف مثل اتفاقية برن لسنة 1997[3].

وبدورها تنقسم معاهدة الويبو إلى عدة معاهدات أهمها:

–معاهدة الويبو بشأن الأداء والتسجيل الصوتي التي تم التوقيع عليها سنة 1996.

[1] - الملدة 10 من إتفاقية تربس، "اتفاقية جوانب حقوق الملكية الفكرية المتصلة بالتجارة".
[2] -المادة 11 من اتفاقية تربس، المرجع السابق.
[3] -عثماني رضوان، مرجع سابق، ص138.

-معاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة.

رابعا: معاهدة بودابست لمكافحة جرائم الأنترنت "اتفاقية بشأن الفضاء الإلكتروني".

تم صياغة هذه الاتفاقية من جانب عدد كبير من الخبراء القانونيين في أوروبا وبمساعدة دول أخرى، لا سيما الولايات الولايات المتحدة الأمريكية بعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر على مستوى العالم[1]، حيث تعتبر هذه الإتفاقية نتاج لجهود المجلس الأوروبي الذي أقر على اتفاقية بودابست لمكافحة الجرائم المعلوماتية بتاريخ2001/11/21 تحت رقم 185 والتي تهدف إلى عصرنة التشريعات الداخلية مع واقع عالم الرقمية، وقد عالجت هذه الاتفاقية كل المسائل المتعلقة بالجريمة المعلوماتية، وقد دخلت حيز التنفيذ بتاريخ 2004/07/01 وهي الاتفاقية التي تساعم بشكل دائم ومستمر في دعم جهود مكافحة الجرائم المعلوماتية[2].

وبعد التوقيع على تلك الاتفاقية من المسؤولين في الدول الأوروبية إضافة إلى أمريكا واليابان وكندا وجنوب إفريقيا، الذي كان نتاج مباحثات ومفاوضات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الاتفاقية وحتى يتم التوقيع عليها من جميع الأطراف دون أن تجد أي اعتراض من أي منهم، بل على العكس لتجد القبول من أطراف جدد ليتم توسيع دائرة الدول التي توافق على الإنضمام في تلك الاتفاقية، ويتم توسيع الاتحاد والتضامن الدوليين[3]، حيث كانت محل تصديق من قبل 47 دولة، وتوقيع من دون تصديق من قبل 07 دول وذلك حسب آخر تعديل مؤرخ في 19 ديسمبر 2015، وتعتبر "سيريلانكا" آخر دولة تصادق على هذه الاتفاقية سنة 2015.

وقد ذهبت هذه الاتفاقية إلى تقسيم الجرائم المعلوماتية إلى أربعة أقسام:

[1] -عثماني رضوان، مرجع سابق، ص150.
[2] -ربيعي حسين، مرجع سابق، ص138.
[3] -عثماني رضوان، نفس المرجع،151.

1) الجرائم ضد سرية وسلامة وإتاحة البيانات ونظم المعلوماتية، كالولوج غير القانوني والاعتداءات على سلامة البيانات وسلامة النظام، وإساءة استخدام الحاسب وجرائم تدمير البيانات.

2) الجرائم المعلوماتية المرتبطة بالحاسب كالتزوير المعلوماتي والاحتيال المعلوماتي.

3) الجرائم المعلوماتية المتعلقة بالمواد الإباحية والغير أخلاقية.

4) وتتعلق بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة وقرصنة البرمجيات[1].

حيث تهدف هذه الاتفاقية إلى ترسخ مبادئ جنائية حديثة تتماشى والتطور المستمر والتغيرات العميقة التي حدثت بسبب انتشار التكنولوجيا الرقمية، وتضم هذه الاتفاقية في فصولها 48 نصا موزعا على ثلاث محاور رئيسية نذكرها كالتالي:

- **المحور الأول:** يضم الجوانب الموضوعية لجرائم المعلوماتية من تحديد للمصطلحات الخاصة، وتحديد أركان ومفاهيم مختلف صور الجريمة المعلوماتية.
- **المحور الثاني:** يضم الجوانب الإجرائية المتعلقة بآليات البحث والتحقيق في مجال الجرائم المعلوماتية.
- **المحور الثالث:** يضم الأحكام المتعلقة بجرائم المعلوماتية العابرة للحدود، وقد دعمت هذه الاتفاقية بمذكرة تفسيرية صدرت قبل ذلك سنة 2001 من قبل لجنة وزراء المجلس الأوروبي، إضافة إلى البروتكول الإضافي للاتفاقية بودابست المتعلق بتجريم السلوكات الماسة بالكرامة الإنسانية، والمحرض على أعمال العنف والكراهية والعنصرية بواسطة الأنظمة المعلوماتية تحت رقم 189 سنة 2003، وهو البروتكول الذي كان محل تصديق من قبل 20 دولة وتوقيع من قبل 18 دولة أخرى والذي دخل حيز التنفيذ بتاريخ 2006/03/01.

[1] -حابت أمال، **الجريمة المعلوماتية في التشريع الجزائري بين قانوني 15/04و04/09**، مجلة هيرودقت للعلوم الإنسانية والاجتماعية، جامعة مولود معمري، الجزائر،المجلد 7، العدد 25 ، 2023، ص

إضافة إلى ذلك فقد عمل المجلس الأوروبي إلى وضع خطوط توجيهية شهر أفريل 2008 تهدف إلى دعم وتعزيز عمل الجهات المختصة بمكافحة الجرائم المعلوماتية كأجهزة الشركة المختصة، والأجهزة القضائية، وهو ما أكدت عليه التوصيات المقدمة من قبل ورشة العمل للمجلس الأوروبي المنعقد سنة 2010 بقولها: يجب العمل على:

- دعم الطابع الدولي لاتفاقية بودابست.
- تكوين رجال قضاء مختصين في مجال مكافحة الجرائم المعلوماتية.
- إعداد مخطط وخارطة لعمل أجهزة مكافحة الجرائم المعلوماتية.
- تكثيف الجهود لردع الجرائم المتعلقة بالاستغلال الجنسي للأطفال عبر شبكة الانترنت[1].

وتجدر الإشارة إلى أن اتفاقية بودابست قد فرضت على الدول الأطراف عند سن تشريعاتها الداخلية المتعلقة بالجرائم المعلوماتية، مراعات الاتفاقية الدولية لحقوق الانسان والاعتماد على معايير لتقرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية المتمثلة في مبدأ الإقليمية ومبدأ نسبية الاختصاص المكاني ومبدأ الجنسية وما إلى غير ذلك.

وهو ما دفع بالمشرع الجزائري وفي ظل المناخ الالكتروني الذي أصبح يميز الجزائر إلى الإقرار بتجريم بعض السلوكيات وذلك تحت وصف الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات وذلك من خلال القانون رقم05/04 المعدل لقانون العقوبات السالف الذكر في قسمه السابع مكرر، والذي استحدث بموجبه نصوص المواد من 394 مكرر إلى 394 مكرر 207.

[1] -ربيعي حسين، مرجع سابق، ص 139.
[2] -ربيعي حسين ، نفس المرجع، ص 48.

الفرع الثاني: آليات التعاون مع الأنتربول واليوروبول في تبادل الأدلة الرقمية.

إن كل التهديدات والإعتداءات الإلكترونية على الأنظمة المعلوماتية، دفعت بالدول إلى استحداث هيئات ووحدات وأقسام خاصة بمكافحة الجرائم المعلوماتية، والعمل على تطويرها بشكل يسمح لها بالتحكم في هذه الظاهرة على كافة الأصعدة بما فيها الإجرائية خصوصا وذلك على المستوى الدولي، وتعتبر الهيئات الأوروبية رائدة في هذا المجال بالنظر إلى قدرتها على التعامل مع هذه المسائل من خلال استحداث الهيئات التالية:

أولا: المنظمة الدولية للشرطة الجنائية (الأنتربول).

كانت الخطوة الأولى لنشأة الأنتربول خلال المؤتمر الدولي الأول للشرطة الجنائية الذي عقد بموناكو الفرنسية سنة 1914 بمشاركة موظفي وممثلي الأجهزة القضائية من 24 دولة لإيجاد سبل التعاون لحل الجرائم ولاسيما ما تعلق باجراءات البحث والتحقيق وتوقيف المجرمين وتسليمهم، حيث أنشأت رسميا سنة 1923 وازداد عدد المنظمين لها على مر السنوات ليصل إلى 190 دولة[1].

وتسعى هذه المنظمة إلى تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء، ومكافحة الجريمة وكذا مساهمتها في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، وللمنظمة دور ريادي في مكافحة الجريمة الإلكترونية، وذلك من خلال تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء من أجل مكافحة هذا النوع من الجرائم الإلكترونية، وذلك من خلال تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء من أجل مكافحة هذا النوع من الجرائم، كما يزود الدول الأطراف بالبيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الموجودة في أقاليم الدول المنظمة لها، حيث ارتكز اهتمام الأنتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأعمال المرتبطة بها، إلى جانب التعاون في ضبط الجناة بمساعدة أجهزة

[1] -شحادة يوسف، **الضابطة العدلية، علاقتها بالقضاء ودورها في سير العدالة الجزائية (دراسة مقارنة)**، طبعة 01، مؤسسة بوحسون للنشر والتوزيع، بيروت، ص455.

الشرطة في الدول الأعضاء، كما يقوم بتتبع مجرمي المعلوماتية من خلال جمع الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود للأنظمة المعلوماتية وشبكات الإتصال بهدف العثور على الأدلة والبراهين على ارتكاب الجرائم الإلكترونية، وهذه الجهود تساهم في تنفيذ العمليات الشرطية والأمنية المشتركة، وهي التي من شأنها متابعة المجرمين الذين يستخدمون التكنولوجيا الحديثة لتحقيق أهدافهم الغير مشروعة[1]، وبخصوص النظام الإداري في الأنتربول، فهي تعقد الجمعية العامة لها مرة واحدة سنويا بقيادة الرئيس الأمين العام الذي يتم تعيينه من قبل الجمعية العامة لمدة خمس سنوات، إلى جانب اللجنة التنفيذية المتكونة من 13 عضو والتي تنعقد ثلاث مرات سنويا.

ولا يقتصر عمل الأنتربول في مكافحة الجريمة المعلوماتية في صورة عقد واحتضان المؤتمرات، بل يعمل على تجسيد ذلك ميدانيا من خلال العمل على دعم إجراءات البحث والتحقيق بشأنها من خلال:

1-جمع وتخزين وتحليل المعلومات المتعلقة بالجرائم المعلوماتية مع توفيرها لكافة الدول الأعضاء بواسطة منظومة I24/07 للأنتربول، وهي عبارة عن شبكة اتصالات شرطية مأمونة تربط بين الدول الأعضاء.

2-هذه الشبكة التي يتم تطويرها من خلال دعمها بمنظومة I-link التي تعتبر المركز الرئيسي لتبادل المعلومات الجنائية والتواصل بين الدول الأعضاء.

3-استحداث معيار منسق للإتصالات لتسهيل تبادل المعلومات الشرطية.

4-إمكانية التحكم المباشر في البيانات الرقمية والتدقيق فيها.

5-إمكانية تسجيل أحدث المعلومات مباشرة في قاعدة البيانات الجنائية.

6-توفير أداة بحث قوية وسريعة فعالة تضمن حصول الشرطة على إجابات فورية وشاملة حول تقصياتها.

ويتمثل الهدف النهائي لهذه المنظومة في نقل جميع المعلومات الجنائية المتبادلة عن طريق الأنتربول في شكل رسائل منسقة تجعل أمر التقصي على قدر كبير من السهولة وتقديم الدعم لمصالح الشرطة على المستويين الدولي

[1] -بن قويدر أمل، بوصبع عفاف، مرجع سابق، ص 52.

والداخلي، وتكوين أعوان الشرطة من خلال تنظيم دورات تكوينية تسمح لهم بتحسين قدراتهم على التعامل مع منظومة الإتصال I24/07 و I–link في إطار سياسة التعاون الدولي لمكافحة الجرائم المعلوماتية[1].

ثانيا: هيئة الأوروبول L'EUROPOL.

ويعتبر الأوروبول وليد ونتاج سيطرة الأنتربول على الساحة الأوروبية لمدة طويلة من الزمن، وقد قدم الطرح المتعلق بإنشاءه أول مرة أمام المجلس الأوروبي من قبل ألمانيا سنة 1991 بمناسبة انعقاد مؤتمر لوكسمبورغ، غير أنه تجسد فعليا في سنة 1995، وذلك بعد مصادقة دول المجلس الأوروبي على اتفاقية ماستريخت في 1995/07/29 ليتخذ من لاهاي مقرا له.

ويتكفل الأوروبول بمكافحة الإجرام عن طريق معالجة المعطيات المرتبطة بالأنشطة الإجرامية على مستوى الإتحاد الأوروبي، ودعم وتشجيع سلطات التحقيق وذلك بتكميل وسائلهم وتجديدها من أجل مكافحة جميع أنواع الإجرام المنظم الدولي، وكذلك من خلال تسهيل تبادل المعلومات عن طريق تزويد المحققين بتحاليل علمية واستراتيجية ودعمهم بالخبرات والمساعدة التقنية[2].

ويعتبر الأوروبول من أكبر الهيئات الإستشارية حول العالم في مجال الجرائم المعلوماتية، وقد تم اختياره من قبل الاتحاد الدولي للأمن المعلوماتي، لإنجاز مختلف الدراسات الخاصة بالجريمة المعلوماتية وذلك إلى غاية سنة 2020، بهدف تحليل دوافع هذه الجرائم ووضع تصور مستقبلي لتطورها، وهو ما يفسر الثقة التي وضعتها فيه اللجنة الأوروبية باختيارها له كمركز إعلام حول موضوع الجرائم المعلوماتية.

يختص الأوروبول في مجال مكافحة الجريمة المعلوماتية، بكل أشكال الجرائم التي ترتكب بواسطة التكنولوجيا الرقمية، تكون إحدى المنظمات الإجرامية الناشطة على الإقليم الأوروبي طرفا فيها.

---

[1] -ربيعي حسين، مرجع سابق، ص 151.

[2] -التقرير السنوي لنشاط الأنتربول لسنة 2012، الموقع الرسمي للأنتربول بنسخة عربية، تاريخ التصفح : 2026/04/10، على الرابط:
http://www.interpol.int/content/download/20552/185417/5/annual%20report%202012_AR_I.pdf.

ولذلك يضم الأوروبول هيكلا بشريا يضم أكثر من 600 شخص بـ لاهاي يضمنون التنسيق والدعم للمحققين الميدانيين سواء تعلق الأمر بدعمهم بالبيانات اللازمة أو التقنيات في مجال التحقيق.

وقد شهد الأوروبول سنة 2008 طفرة نوعية في وسائل عمله وصلاحياته فبتاريخ 24 أكتوبر من نفس السنة تقرر بلكسمبورغ إنشاء قاعدة بيانات أوروبية مشتركة بميزانية أولية قدرها 300.000 يورو تخضع لتسيير منظمة الأوروبول وتضمن التنسيق بين عمل جهات الشرطة للدول الأعضاء من خلال إحصاء وجمع كافة القضايا الإجرامية التي لها علاقة بالمعلوماتية وذلك لأجل التنسيق بين عمل الجهات الأمنية.

وعليه يمكن القول بأن الأوروبول مختصة بالبحث والتحقيق في الجرائم المعلوماتية خصوصا تلك المتعلقة بالاستغلال الجنسي للأطفال والإرهاب الإلكتروني، وهو يهدف من خلال نشاطه إلى تسهيل الإجراءات أمام رجال الشرطة لأجل التحري بشأن الجرائم المتعلقة ببلدانهم، من خلال مدهم بمختلف النشرات الأمنية والتقارير حول هوية المتهمين والأدلة المحصلة خارج الحدود الإقليمية لمجال اختصاصهم[1].

[1] -ربيعي حسين/ مرجع سابق، ص153.

خلاصة الفصل الأول.

شهدت الجرائم المتعلقة بتقنية المعلوماتية تطورا متسارعا في ظل الثورة الرقمية وتوسع استخدام تكنولوجيا الإعلام والإتصال، مما فرض على المشرع الجزائري ضورورة مواكبة هذه التحديات بوضع إطار قانوني فعال للوقاية منها ومكافحتها، وقد تمثلت أبرز آليات مكافحة الجريمة الإلكترونية في الجزائر في سن قوانين خاصة أهمها القانون رقم 04/09 المعدل والمتمم لقانون العقوبات، والذي أدرج نصوصا تجرم أفعالا إلكترونية كاختراق الأنظمة المعلوماتية، التزوير الإلكتروني، والإحتيال عبر الإنترنت.

كما عزز المشرع هذه الآليات بوسائل إجرائية خاصة، كإتاحة وسائل الإثبات الرقمية وتوسيع صلاحيات الضبطية القضائية في التعامل مع الجرائم الإلكترونية، إضافة إلى التعاون الدولي في هذا المجال، ورغم الجهود لا تزال الحاجة قائمة لتحديث المنظومة التشريعية وتدعيم القدرات التقنية والبشرية لمواجهة التطورات المتسارعة لهذا النوع من الجرائم.

الفصل الثاني

الجريمة المعلوماتية وكغيرها من أنواع الجرائم الأخرى تمر بذات مرحلتي الإستدلال والتحقيق القضائي وما يترتب عن ذلك من إجراءات قانونية وفنية وشكلية وذلك متوقف على ظروف كل جريمة، فالملاحظ أن الإجراءات المتبعة في الجرائم المعلوماتية تتصف بالخصوصية من حيث طريقة كشفها والتحقيق فيها وطريقة جمع الأدلة والصعوبات التي قد تنشأ أثناء مباشرة البحث والتحري وكذا خصوصية التعامل مع الأدلة الجنائية وصولا إلى تنازع الإختصاص القضائي والمحكمة في الفضاء السيبراني، فكل هذه الإجراءات ذات الطابع الإجرائي يجب أن تتم بالموازنة مع طبيعة الجريمة المعلوماتية وما ينتج عنها من خصوصيات تغيب عن الجرائم الأخرى.

وسنحاول من خلال هذا الفصل معالجة هذه التحديات الإجرائية والعملية، وذلك من خلال معالجة إشكالية البحث والتحري في البيئة الرقمية في المبحث الأول، ثم التعرض إلى عوائق المتابعة والمحاكمة في الفضاء السيبراني في المبحث الثاني.

المبحث الأول: إشكالية البحث والتحري في البيئة الرقمية.

يمثل البحث والتحري في البيئة الرقمية تحديا نوعيا للأجهزة القضائية والأمنية على مستوى العالم، وذلك بسبب الخصائص التقنية الفريدة للأدلة الرقمية التي تختلف جوهريا عن الأدلة التقليدية، فبينما تعتاد الأجهزة القضائية على التعامل مع الأدلة المادية الملموسة، تأتي الأدلة الرقمية لتكسر هذه القاعدة، إذ هي أدلة غير مادية قابلة للتلف والتلاعب، وتتطلب بيئة تقنية خاصة لضبطها وحفظها وتعديلها وهذا الواقع يفرض تحديات إجرائية وعملية جسيمة تبدأ من لحظة جمع الدليل الرقمي، ومن بين أهم هذه التحديات نذكر:

المطلب الأول: الطبيعة اللامادية للدليل الرقمي.

يعتبر الدليل الرقمي ذلك الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات مغناطيسية أو كهربائية أو على شكل ذبذبات رقمية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا **خاصة**، وقد نجد أن هناك أيضا نظم أخرى مدمجة بالحواسيب كالهواتف النقالة والبطاقات الذكية والمساعد الرقمي الشخصي، حيث يتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، فهو ذلك الدليل الذي يوجد له أساس في العالم الإفتراضي ويقود إلى الجريمة[1].

فالدليل المرئي مختلف عن الإلكتروني، وبالتالي فإن أمر ربطه بشخصية المتهم أمر بالغ في الصعوبة ذلك أن الدليل الإلكتروني لا يفصح عن شخصية معينة، وهو ما يظهر جليا في الجرائم المرتكبة عبر الشبكة والتي يستطيع المستخدم عبرها الاتصال دون كشف هويته الحقيقية، إضافة إلى كون الدليل الرقمي عادة ما يكون مشفرا، وبالتالي فالسمة الأكثر جوهرية للأدلة الرقمية في طبيعتها اللامادية فهي أشياء غير ملموسة يمكن وضعها في كيس مغلق أو حفظها في خزانة كما هو الحال مع الأدلة التقليدية كالسلاح أو المخدرات أو بصمات الأصابع، إلى جانب أنها عبارة عن بيانات إلكترونية مخزنة على وسائط تقنية قد تكون هذه الوسائط مادية (كالأقراص الصلبة أو بطاقات الذاكرة أو

[1] - حنان حفصة، مرجع سابق، ص 46.

الهواتف النقالة)، لكن الدليل في حد ذاته (أي المعلومة) فهو غير مادي[1]. هذه الطبيعة تترتب عليها عدة خصائص تميز الدليل الرقمي وتجعله في نفس الوقت قويا وضعيفا، قويا لأنه يمكن استنساخه ونقله بسهولة ودون تلف، وضعيف لأنه قابل للتلف والتلاعب والإختفاء بسهولة مما قد يقطع علاقة السببية بين المجرم والجريمة[2].

الفرع الأول: صعوبة ضبط وحفظ الأدلة الرقمية (وقابيتها للتلف والتلاعب).

ينتج عن الجرائم المعلوماتية آثار من نوع خاص وهو ما يعرف بالدليل الإلكتروني، ولخصائص هذا الدليل آثار سلبية على عمل جهات البحث والتحقيق، بحيث تعيق عملهم في مجال إحراز هذا الدليل وهي الصعوبات التي سنوجزها فيما يلي:

أولاً: هشاشة الدليل الرقمي وقابليته للتلف.

تتميز الأدلة الرقمية بهشاشة كبيرة تجعلها عرضة للتلف أو التغيير أو الضياع بسهولة، وهذه الهشاشة تنبع من طبيعتها الإلكترونية غير الملموسة' فالدليل الرقمي –سواء كان ملفاً نصياً/ صورة/فيديو أو سجلاً لاتصال– هو مجرد مجموعة من الإشارات الكهربائية أو المغناطيسية المخزنة على وسيط تقني، أي خلل تقني، مهما كان بسيطاً، قد يؤدي إلى تلف هذا الدليل أو تغيره بشكل غير مقصود.

ومن أهم مظاهر هذه الهشاشة أن الأدلة الرقمية يمكن أن تتلف أو تتغير بمجرد عملية نقلها من جهاز إلى آخر إذا لم تتم هذه العملية وفق المنهجيات العلمية السليمة، ففتح ملف نصي على جهاز الكمبيوتر، على سبيل المثال، يؤدي تلقائياً إلى تغيير تاريخ آخر وصول إلى الملف، وهذا التغيير وإن كان بسيطاً قد يؤثر على قيمة الدليل إذا كان تاريخ الوصول مهماً لإثبات واقعة معينة[3].

---

[1] –منى غازي حسام إبراهيم، **فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية**،(دراسة مقارنة في ضوء متطلبات الأمن السيبراني)، مجلة الشريعة والقانون، القسم الجنائي، كلية شريعة وأنظمة، جامعة الطائف، المملكة العربية السعودية، العدد 45، ماي 2025.

2 – مجلس أوروبا، **دليل الأدلة الإلكترونية وسلسلة الحيازة**، ترجمة وزارة العدل الجزائرية، 2017، ص 8.

3 – د. نوال دراجي، "**إشكالية إثبات الجرائم المعلوماتية**"، مجلة الدراسات القانونية، جامعة وهران، العدد 8، 2018، ص 67.

كذلك، تتعرض الأدلة الرقمية لخطر التلف بسبب الأعطال التقنية المفاجئة، كتعطل القرص الصلب، أو تلف بطاقة الذاكرة، أو انقطاع التيار الكهربائي أثناء عملية حفظ البيانات، كما أن الظروف البيئية كالحرارة المرتفعة، الرطوبة، أو المجالات المغناطيسية قد تؤدي إلى تلف الوسائط التخزينية وفقدان البيانات بشكل نهائي[1].

علاوة على ذلك، هناك ظاهرة "الاندثار الرقمي(Digital Obsolescence) "، حيث تتقادم التقنيات وتختفي البرامج والأجهزة التي يمكنها قراءة بعض أنواع الوسائط التخزينية أو تنسيقات الملفات القديمة، هذا يعني أن الدليل الرقمي قد يصبح غير قابل للقراءة ليس بسبب تلفه، بل لأن التقنية التي تمكن من قراءته لم تعد متوفرة[2].

ثانياً: سهولة التلاعب بالدليل الرقمي.

إذا كانت الأدلة التقليدية تحتاج إلى جهد وخبرة لتزويرها، فإن الأدلة الرقمية تتميز بسهولة التلاعب بها وتغييرها، وغالباً دون ترك آثار واضحة، فالمعروف في علم الأدلة الرقمية أن أي ملف رقمي يمكن تعديله أو تغييره باستخدام برامج تحرير بسيطة، وبعض هذه التعديلات قد لا تكتشف إلا بوسائل تقنية متقدمة.

تتنوع صور التلاعب بالدليل الرقمي فتشمل: حذف ملفات أو أجزاء منها، إضافة بيانات مزيفة، تعديل محتوى الملفات النصية أو الصور أو الفيديوهات، تغيير التواريخ والأوقات المرتبطة بالملفات (المعروفة بالبيانات الوصفية)، وإنشاء أدلة رقمية كاملة بشكل مصطنع باستخدام تقنيات الذكاء الاصطناعي التوليدي، هذه السهولة في التلاعب تجعل من مسألة إثبات صحة وسلامة الدليل الرقمي تحدياً كبيراً. فالمتهم قد يدعي أن الدليل المقدم ضده قد تم التلاعب به، وأن ما يراه القضاء ليس هو الحقيقة بل نسخة معدلة[3].

1 – د. رشيد بوبكر، "**حماية الأدلة الرقمية في التشريع الجزائري**"، مجلة الباحث في الحقوق، جامعة تيزي وزو، العدد 5، 2020، ص 89.

2 – د. فاطمة الزهراء بن ساسي، "**الاندثار الرقمي كعائق أمام الأدلة الإلكترونية**"، مجلة القانون والأعمال، جامعة قسنطينة، العدد 15، 2019، ص 112.

3 – د. زكرياء قاسمي، "**طعن المتهم في سلامة الدليل الإلكتروني**"، مجلة الحقوق، جامعة الجزائر 1، العدد 22، 2019، ص 134.

ومن أخطر صور التلاعب تلك التي تتم من قبل جهات الضبط القضائي نفسها، سواء بقصد أو بغير قصد، ففي قضية شهيرة في الولايات المتحدة، تبين أن عميلاً في مكتب التحقيقات الفيدرالي (FBI) قام بالوصول إلى بطاقة ذاكرة دون استخدام أداة الحماية من الكتابة(Write-Blocker) ، مما أدى إلى تغيير التواريخ والأوقات المرتبطة بالملفات[1].

ثالثاً: إشكالية الحفاظ على سلسلة الحيازة(Chain of Custody) .

تُعرف سلسلة الحيازة بأنها المسار الكامل الذي يقطعه الدليل من لحظة جمعه من مسرح الجريمة أو من الجهاز المستهدف، مروراً بمراحل نقله وتحليله وتخزينه، وصولاً إلى عرضه في المحكمة، ولكل مرحلة من هذه المراحل، يجب توثيق كل تفصيلية تتعلق بالدليل: من الذي تعامل معه، ومتى، ولأي غرض، وما هي الإجراءات التي تمت عليه، وكيف تم نقله، ومن تسلمه بعده[2].

في الأدلة التقليدية، سلسلة الحيازة تكون نسبياً واضحة وأسهل في التوثيق، أما في الأدلة الرقمية، فالأمر مختلف تماماً. فالدليل الرقمي يمكن نقله وتكراره بسهولة، ويمكن التعامل معه عن بعد، ويمكن تعديله دون ترك آثار مادية، لهذا فإن توثيق سلسلة الحيازة للأدلة الرقمية يحتاج إلى تقنيات خاصة وأدوات متطورة، ومن أهم هذه الأدوات استخدام "التوقيع الرقمي" أو "قيمة التجزئة (Hash Value) "لكل ملف[3].

الإشكالية هنا أن العديد من جهات التحقيق في العالم، وخاصة في الدول النامية، لا تملك هذه التقنيات أو لا تطبقها بشكل صحيح، كما أن غياب بروتوكولات موحدة للتعامل مع الأدلة الرقمية يزيد من صعوبة ضمان سلامة

---

1 ــ قضية الولايات المتحدة ضد روبرت كيس(US v. Robert Case) ، المحكمة الجزئية لمنطقة كولومبيا، الحكم رقم 12342015-CF-، حيث تم استبعاد الأدلة بسبب خطأ فني. (ملخص من نتائج البحث).

2 – د. نادية عبد الحفيظ، **"توثيق الأدلة الرقمية في التشريع الجزائري"**، مجلة العلوم القانونية، جامعة باتنة، العدد 10، 2020، ص 55.

3 – د. جمال الدين زروقي، **سلسلة الحيازة الرقمية بين النظرية والتطبيق**، دار هومة، الجزائر، 2019، ص 67.

سلسلة الحيازة، إن أي ثغرة أو غموض في سلسلة الحيازة يمكن أن يستغله الدفاع للطعن في الدليل، وقد يؤدي إلى رفض المحكمة لقبوله[1].

رابعا: قلة خبرة القائمين على هذه الجرائم: فهناك ما يتعلق بشخصية المحقق مثل الهيبة من استخدام الكمبيوتر والأنترنت، وهناك ما يتعلق بالنواحي الفنية ولنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم، وعدم توفر المعرفة بأساليب ارتكاب الجريمة الإلكترونية وقلة الخبرة في هذا المجال والمعرفة باللغة الإنجليزية أو اللغات المستخدمة خاصة وأن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة تشكل الطابع المميز لمحادثتهم[2].

الفرع الثاني: حجية الدليل الإلكتروني أمام القضاء (القيمة القانونية للمطبوعات والمحفوظات الإلكترونية)

أولاً: الإطار القانوني العام للدليل الإلكتروني في الجزائر.

شهد التشريع الجزائري تطوراً ملحوظاً في مجال الاعتراف بالدليل الإلكتروني، وإن كان هذا التطور لا يزال في مراحله الأولى مقارنة ببعض التشريعات الغربية[3]، فقد نص القانون المدني الجزائري في المادة 323 مكرر (المضافة بموجب الأمر 75-58) على أن "المطبوعات والمحفوظات الإلكترونية تعتبر كتابة إذا كانت مفهومة ويمكن الاحتجاج بها في مواجهة الغير"[4].

إلا أن هذه النصوص كانت عامة وتحتاج إلى تفصيل، وهو ما حاول المشرع تداركه في قوانين لاحقة، خاصة قانون الإجراءات الجزائية وقانون المعاملات الإلكترونية رقم 18-05[5]، غير أنه يجب الإشارة إلى أن الجزائر، كغيرها

---

1 -د/رشيد بوبكر، مرجع سابق.ص 99.

2 -حنان حفصة ، مرجع سابق،ص38.

3 - د. رابح مقدم، **"تطور التشريع الجزائري في مجال الأدلة الإلكترونية"**، مجلة القانون المقارن، جامعة الجزائر 2، العدد 14، 2018، ص 33.

4 - المادة 323 مكرر من القانون المدني الجزائري (الأمر 75-58 المؤرخ في 26 سبتمبر 1975 المعدل والمتمم).

5 - القانون رقم 18-05 المؤرخ في 10 مايو 2018 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها (الجريدة الرسمية الجزائرية، العدد 28، 2018).

من الدول العربية، لا تزال تواجه تحديات في مجال قبول الدليل الإلكتروني، ويرجع ذلك إلى عدم وجود بنية تحتية تقنية متطورة، ونقص الخبرات المتخصصة[1].

ثانياً: المطبوعات والمحفوظات الإلكترونية كقرينة.

المبدأ العام في قانون الإثبات الجزائي الجزائري هو حرية الإثبات، فلا توجد قيود على وسائل الإثبات في المواد الجزائية، بخلاف المواد المدنية التي تخضع لقواعد محددة، وهذا يعني أن القاضي الجزائي يمكنه أن يأخذ بأي دليل يراه مقنعاً، بما في ذلك الأدلة الإلكترونية، طالما أنها تم جمعها وفقاً للإجراءات القانونية السليمة[2].

في هذا السياق، يمكن النظر إلى المطبوعات والمحفوظات الإلكترونية كقرينة يعزز بها القاضي قناعاته، وليس كدليل كامل بحد ذاتها، فالقرينة في قانون الإثبات هي استنتاج يستخلصه القاضي من واقعة معلومة للوصول إلى واقعة مجهولة[3].

ثالثاً: شروط قبول الدليل الإلكتروني في القانون الجزائري.

رغم أن القانون الجزائري لم ينظم بشكل مفصل شروط قبول الدليل الإلكتروني، إلا أنه يمكن استخلاص هذه الشروط من المبادئ العامة لقانون الإثبات، ومن الاجتهادات القضائية والفقه القانوني.

1 .شرط السلامة من التلاعب: يجب أن يكون الدليل الإلكتروني سليماً ولم يطرأ عليه أي تغيير أو تزوير. لإثبات هذا الشرط، يجب على من يقدم الدليل أن يبرز سلسلة حيازة واضحة.

2 .شرط المشروعية في الجمع: يجب أن يتم جمع الدليل الإلكتروني بطرق مشروعة قانوناً. فإذا تم الحصول على الدليل بانتهاك حرمة الحياة الخاصة، أو بدون إذن قضائي، فإن الدليل يعتبر باطلاً.

1 – د. عبد الحميد شريفي، "**معوقات قبول الدليل الإلكتروني في القضاء الجزائري**"، مجلة الدراسات القضائية، المعهد الوطني للقضاء، الجزائر، العدد 12، 2020، ص 56.

2 – د. محمد الصالح بن عيسى، **حرية الإثبات في المواد الجزائية**، دار البعث، قسنطينة، 2018، ص 123.

3 – د. فتيحة زروقي، "**القرائن الإلكترونية في القانون الجزائي الجزائري**"، مجلة الحقوق، جامعة ورقلة، العدد 9، 2019، ص 77.

3 .شرط الوضوح والمفهومية: يجب أن يكون الدليل الإلكتروني واضحاً ومفهوماً للقاضي. فإذا كان الدليل مشفراً، يجب أن يتم فك تشفيره من قبل خبير.

4 .شرط الاتصال بالواقعة: يجب أن يكون الدليل الإلكتروني مرتبطاً بالواقعة موضوع الدعوى، وألا يكون دخيلاً عليها[1].

5 .شرط التوقيع الإلكتروني الموثق: بالنسبة للمطبوعات الإلكترونية التي يراد إعطاؤها حجية كتابة كاملة، يتطلب القانون الجزائري أن تكون موقعة بتوقيع إلكتروني آمن ومعتمد من جهة موثوقة[2].

رابعاً: التحديات التي تواجه قبول الدليل الإلكتروني في المحاكم الجزائرية.

على المستوى العملي، تواجه النيابة العامة والمحاكم الجزائرية عدة تحديات في قبول الدليل الإلكتروني، من أهمها:

1.غياب البنية التحتية التقنية: لا تمتلك معظم المحاكم الجزائرية الأجهزة والمعدات اللازمة لعرض الأدلة الرقمية بشكل مناسب، كما أن مختبرات الأدلة الرقمية في الجزائر قليلة وتفتقر إلى أحدث التقنيات.

2 .نقص الخبرات المتخصصة: لا يزال عدد القضاة وأعضاء النيابة العامة وأجهزة الضبط القضائي المدربين على التعامل مع الأدلة الرقمية محدوداً جداً.

3 .غياب التشريعات المنظمة بشكل مفصل: رغم وجود بعض النصوص القانونية، إلا أن الجزائر لا تزال تفتقر إلى تشريع شامل ينظم كل جوانب الدليل الإلكتروني.

4 .ضعف التعاون الدولي: كثير من الأدلة الرقمية توجد على خوادم في الخارج، والحصول عليها يحتاج إلى طلبات مساعدة قضائية قد ترفضها بعض الدول، خاصة أن الجزائر ليست طرفاً في اتفاقية بودابست.

---

1 – د. فوزية براهيمي، "**ارتباط الدليل الإلكتروني بالواقعة**"، **مجلة الدراسات القانونية**، جامعة البليدة، العدد 13، 2019، ص 114.

2 – د. بلقاسم بوعمرة، "**شروط قبول الدليل الإلكتروني في الاجتهاد القضائي الجزائري**"، مجلة القضاء والقانون، المجلس الأعلى للقضاء، الجزائر، العدد 25، 2020، ص 66.

5 .التحدي المتعلق بالخبرة القضائية: عندما يتعارض رأي خبيرين، أو عندما يقدم الخبير تقريراً معقداً، قد يفضل القاضي الاعتماد على أدلة تقليدية أكثر وضوحا[1].

خامساً: نحو تعزيز حجية الدليل الإلكتروني في القانون الجزائري.

لتعزيز حجية الدليل الإلكتروني أمام القضاء الجزائري، يمكن اقتراح عدة توصيات:[2]

1/ تطوير التشريعات: إصدار قانون خاص بالأدلة الإلكترونية يحدد حجيتها وشروط قبولها.

2/ إنشاء وتجهيز مختبرات الأدلة الرقمية: تابعة لوزارة العدل ومجهزة بأحدث التقنيات.

3/ تدريب القضاة وأعضاء النيابة وأجهزة الضبط: إدراج مواد تدريبية إلزامية في مناهج التكوين.

4/ الانضمام إلى الاتفاقيات الدولية: خاصة اتفاقية بودابست لمكافحة الجرائم الإلكترونية.

5/ الاعتراف المتبادل بالتوقيع الإلكتروني: مع الدول الأخرى لتسهيل قبول المستندات الإلكترونية.

المطلب الثاني: تقنيات التخفي وصعوبة تحديد هوية الجاني.

يمثل تحديد هوية مرتكب الجريمة المعلوماتية أحد أكبر المعوقات التي تواجه أجهزة العدالة الجنائية الجزائرية، ففي الوقت الذي تطورت فيه وسائل الإخفاء والتشويش الرقمي بشكل متسارع، بقيت آليات التحري التقليدية عاجزة في كثير من الأحيان عن كشف هوية الفاعل الحقيقي، ففي الجرائم التقليدية، يترك الجاني وراءه بصمات مادية أو شهود عيان، بينما في الفضاء السيبراني يمكن للمجرم أن يخفي أثره بالكامل باستخدام تقنيات متطورة، متسبباً في إحباط جهود الضبطية القضائية[3]، هذا الواقع يضع المشرع والقضاة الجزائريين أمام تحديات إجرائية كبرى سنتناولها من خلال محورين: الأول يتعلق بأساليب التشفير والشبكات الافتراضية الخاصة (VPN) كوسائل للتخفي، والثاني يتعلق بإشكالية إسناد الفعل الإجرامي إلى شخص معين.

---

1 – د. العربي قاسمي، "**التحديات العملية لقبول الدليل الإلكتروني في المحاكم الجزائرية**"، مجلة البحوث القانونية، جامعة الجزائر 1، العدد 20، 2021، ص 145.

2 – توصيات مستخلصة من: د. عبد المجيد شني، "**سبل تطوير حجية الدليل الإلكتروني في الجزائر**"، مجلة الإصلاح القانوني، جامعة قسنطينة 1، العدد 5، 2020، ص 210–215.

3 -سمير بارة، "الأمن السيبراني في الجزائر: السياسات والمؤسسات"، المجلة الجزائرية للأمن الإنساني، المجلد 2، العدد 2، 2017، الصفحات 260-262.

الفرع الأول: استخدام أساليب التشفير والشبكات الافتراضية الخاصة(VPN) .

أولاً: مفهوم التشفير وأهميته في إخفاء الاتصالات.

التشفير (Encryption) هو عملية تحويل البيانات من صيغة مفهومة (نص واضح) إلى صيغة غير مفهومة (نص مشفر) باستخدام خوارزميات رياضية معقدة، ولا يمكن إعادة تحويلها إلى صيغتها الأصلية إلا باستخدام "مفتاح فك التشفير" الخاص، وقد أصبحت هذه التقنية متاحة للجميع بفضل التطبيقات المجانية، مما جعل المجرمين يعتمدون عليها بشكل واسع لحماية اتصالاتهم وإخفاء أدلتهم عن أعين السلطات[1].

ومن أبرز صور استخدام التشفير في النشاط الإجرامي[2]:

1- **تطبيقات المراسلة المشفرة:** مثل Signal و TelegramوWhatsApp، التي توفر "تشفيراً من طرف إلى طرف(End-to-End Encryption) "، مما يعني أن محتوى الرسائل لا يمكن لأي جهة قراءته سواء كانت الدولة أو مزود الخدمة نفسه، يستخدم المجرمون هذه التطبيقات للتخطيط لجرائمهم مثل الاتجار بالمخدرات أو تنظيم هجمات إلكترونية دون خوف من التنصت القضائي.

2- **تشفير الأجهزة والتخزين:** يقوم المجرمون بتشفير الأقراص الصلبة لأجهزتهم باستخدام برامج مثل VeraCryptأو التشفير المدمج في أنظمة التشغيل BitLocker أو FileVault ، وعند ضبط جهاز مشفر من قبل مصالح الأمن، تصبح عملية استخراج الأدلة شبه مستحيلة دون الحصول على كلمة المرور من المتهم، وهو ما يعطل التحقيقات لأسابيع أو شهور.

3- **الويب المظلم (Dark Web) وشبكة Tor** : تعمل شبكة Tor على تمرير حركة المرور عبر ثلاث طبقات من التشفير وعبر سلسلة من الخوادم التطوعية حول العالم، مما يجعل تتبع المستخدم مستحيلاً تقريباً، تُستخدم هذه

1 - يخلف عبد القادر، "المكافحة الموضوعية للجرائم الإلكترونية في القانون الجزائري"، مجلة البحوث القانونية والاقتصادية، المجلد 8، العدد 3، 2025، ص 520.

2 -سمير بارة، المرجع السابق، ص 271.

الشبكة للوصول إلى "الويب المظلم" حيث تنتشر الأسواق الإلكترونية غير المشروعة لبيع المخدرات والأسلحة والمعلومات المسروقة، وتزداد صعوبة ملاحقة مستخدميها بسبب غياب الإطار القانوني المناسب في الجزائر للتعامل مع هذا النوع من الجرائم[1].

ثانياً: الشبكات الافتراضية الخاصة (VPN) كأداة لإخفاء الهوية.

الشبكة الافتراضية الخاصة (Virtual Private Network – VPN) هي خدمة تقوم بإنشاء "نفق مشفر" بين جهاز المستخدم وخادم VPN قد يكون موجوداً في دولة أخرى، ثم يقوم هذا الخادم بإعادة توجيه حركة المرور إلى الإنترنت، والنتيجة هي إخفاء عنوان IP الحقيقي للمستخدم (الذي يكشف موقعه الجغرافي ومزود الخدمة) واستبداله بعنوان IP خاص بخادمVPN ، مما يجعل تتبع النشاط الإجرامي أمراً بالغ الصعوبة[2].

01-المشكلات الإجرائية التي تثيرها شبكات VPN :

أ- صعوبة تتبع عنوان IP الحقيقي: عندما يستخدم مجرمVPN ، فإن عنوان IP الذي يظهر في سجلات الخادم المخترق هو عنوان خادم VPN وليس عنوان المجرم. ولتحديد هوية المجرم، تحتاج السلطات القضائية الجزائرية إلى التعاون مع مزود خدمةVPN ، لكن العديد من هذه المزودين لا يحتفظون بأي سجلات (No-Logs Policy) بحجة حماية خصوصية المستخدمين، مما يجعل من المستحيل الحصول على البيانات[3].

ب- الاختصاص القضائي الدولي المعقد: غالباً ما يكون خادم VPN موجوداً في دولة أجنبية (كالولايات المتحدة أو هولندا أو بنما)، مما يلزم السلطات الجزائرية بتقديم طلبات مساعدة قضائية دولية، هذه الطلبات تستغرق شهوراً أو

---

1 -د/ العربي قاسمي، مرجع سابق، ص 149.

2 – ينظر :نوال دراجي، "إشكالية إثبات الجرائم المعلوماتية"، مجلة الدراسات القانونية، جامعة وهران، العدد 10، 2019، ص 71.

3 – يخلف عبد القادر، مرجع سابق، ص 525.

سنوات، وغالباً ما تتعثر بسبب اختلاف الأنظمة القانونية، أو عدم توفر اتفاقيات تعاون قضائي بين الجزائر وتلك الدول في مجال الجرائم المعلوماتية[1].

ج- سلاسل VPN المتعددة (VPN Chaining): يستخدم بعض المجرمين أكثر من شبكة VPN متتالية، أو يجمعون بين VPN وشبكةTor ، مما يخلق طبقات متعددة من التخفي يصعب اختراقها، في هذه الحالة، تحتاج جهات التحقيق إلى تتبع المسار عبر عدة دول، وهو أمر قد يكون مستحيلاً عملياً[2].

ثالثاً: الإطار القانوني الجزائري لمواجهة التشفير والشبكات الافتراضية.

سعى المشرع الجزائري إلى مواجهة هذه التقنيات من خلال عدة نصوص قانونية، أبرزها:

1 . القانون رقم 09-04 المؤرخ في 5 غشت 2009:[3] يُعتبر هذا القانون أول نص جزائري متخصص في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. وقد نص في المادة 3 منه على تجريم "الوصول غير المشروع إلى نظام معلوماتي"، وفي المادة 5 على تجريم "اعتراض الاتصالات غير المشروع"[4]، غير أن هذه النصوص لم تتناول بشكل مباشر مسألة استخدام التشفير أو VPN كوسيلة لإخفاء الأدلة، مما يعد فراغاً تشريعياً.

2 . القانون رقم 18-05 المؤرخ في 10 مايو 2018: جاء هذا القانون ليعدل ويتمم القانون السابق، وأضاف نصوصاً جديدة تتعلق بتوسيع صلاحيات الضبطية القضائية في مجال التفتيش والحجز الرقمي[5]، فقد نصت المادة 22 منه على إمكانية "حجز البيانات المعلوماتية المخزنة أو المعالجة في نظام معلوماتي"، لكنه لم يلزم مزودي الخدمة) بما في ذلك مزودي (VPN بالتعاون مع السلطات أو الاحتفاظ بالسجلات.

---

1 – ينظر :أحمد زاوي، "الجزائر واتفاقية بودابست للجرائم الإلكترونية"، مجلة العلاقات الدولية، جامعة الجزائر 3، العدد 11، 2019، الصفحة 138.

2 –نوال دراجي ، المرجع السابق، ص74.

3 _ . القانون رقم 09-04 المؤرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

4 – ينظر :المادة 3 والمادة 5 من القانون رقم 09-04 المؤرخ في 5 غشت 2009، الجريدة الرسمية الجزائرية، العدد 47، 2009.

5 – ينظر :المادة 22 من القانون رقم 18-05 المؤرخ في 10 مايو 2018، الجريدة الرسمية الجزائرية، العدد 28، 2018.

3 . القانون رقم 18-07 المؤرخ في 10 يونيو 2018: يتعلق بحماية الأشخاص في مجال معالجة المعطيات ذات الطابع الشخصي، وقد أنشأ سلطة وطنية لمراقبة حماية المعطيات الشخصية(ANPDP)[1] ، لكن هذا القانون، رغم أهميته في حماية الخصوصية، قد يُستخدم أحياناً كحجة من قبل المجرمين لحماية بياناتهم المشفرة، مما يخلق تعارضاً بين مبدأ حماية الخصوصية ومبدأ مكافحة الجريمة.

رابعاً: التحديات التقنية والقانونية في الجزائر.

تواجه السلطات الجزائرية عدة تحديات في مواجهة استخدام التشفير وVPN:

1- **التحدي التقني:** يتطلب فك التشفير أو تتبع حركة المرور عبر شبكات VPN إمكانيات تقنية متطورة من أجهزة وبرامج وكوادر بشرية مدربة[2]، ورغم أن الجزائر أنشأت "المجلس الوطني لأمن أنظمة المعلومات (CNSSI) " بموجب المرسوم الرئاسي رقم 20-05 في 20 يناير 2020، إلا أن هذه المؤسسة لا تزال في مرحلة بناء قدراتها[3].

2- **التحدي القانوني:** غياب نصوص قانونية تلزم مزودي خدمة VPN (خاصة الأجانب) بالاحتفاظ بسجلات المستخدمين والتعاون مع السلطات القضائية الجزائرية، كما أن القانون رقم 15-04 المتعلق بالتوقيع والمصادقة الإلكترونيين لم يتناول مسألة التشفير من زاوية إجرائية.

3- **التحدي المتعلق بالتعاون الدولي:** لم تصادق الجزائر بعد على اتفاقية بودابست لمكافحة الجرائم الإلكترونية، مما يحد من قدرتها على تبادل المعلومات مع الدول الأعضاء في الاتفاقية بشكل سريع، كما أن معظم مزودي VPN الكبار يقع مقرهم في دول لا توجد معها اتفاقيات تعاون قضائي فعال في هذا المجال[4].

1 - ينظر :المادة 12 وما بعدها من القانون رقم 18-07 المؤرخ في 10 يونيو 2018، الجريدة الرسمية الجزائرية، العدد 31، 2018.

2 - سمير بارة، مرجع سابق،ص 275.

3 - المرسوم الرئاسي رقم 20-05 المؤرخ في 20 يناير 2020 المتعلق بإنشاء المجلس الوطني لأمن أنظمة المعلومات، الجريدة الرسمية الجزائرية، العدد 04، 2020.

4 -أحمد زاوي ، مرجع سابق، ص 142.

الفرع الثاني: صعوبة إسناد الفعل الإجرامي إلى شخص معين (مشكلة الإثبات في الجرائم المعلوماتية)

أولاً: إشكالية هوية مرتكب الجريمة المعلوماتية.

تتمثل إحدى أصعب الإشكاليات التي تواجه القضاء الجزائي في "معضلة الإسناد (Problem of Attribution)"، وهي صعوبة إثبات أن الشخص المتهم هو نفسه من كان وراء لوحة المفاتيح عند وقوع الجريمة، فحتى لو تمكنت جهات التحقيق من تحديد عنوان IP الذي صدرت منه الجريمة، فإن ذلك لا يعني بالضرورة تحديد هوية الشخص الذي قام بالفعل الإجرامي. وقد عبر الفقيه الجزائري يخلف عبد القادر عن ذلك بقوله: "إن عنوان IP قد يكون قرينة على مصدر الفعل، لكنه ليس دليلاً على فاعلية الشخص المادي"[1].

أسباب هذه الإشكالية:

01-**اختراق الأجهزة عن بعد:** يمكن لشخص آخر غير صاحب الجهاز أن يخترقه ويستخدمه لارتكاب جريمة، مما يجعل صاحب الجهاز الحقيقي ضحية لا جانيًا. ففي العديد من قضايا الابتزاز الإلكتروني التي عولجت أمام المحاكم الجزائرية، تبين لاحقاً أن أجهزة الضحايا كانت مخترقة من قبل أطراف ثالثة[2].

02-استخدام الأجهزة العامة: إذا استخدم الجاني جهازاً في مقهى إنترنت أو مكتبة عامة، فإن تتبع عنوان IP سيقود إلى ذلك المكان وليس إلى الجاني نفسه. وفي هذه الحالة، قد يكون من المستحيل تقريباً تحديد أي من مستخدمي ذلك الجهاز قام بالفعل الإجرامي، خاصة في ظل عدم وجود أنظمة مراقبة أو تسجيل دخول في معظم هذه الأماكن في الجزائر[3].

1 يخلف عبد القادر، نفس المرجع، الصفحة 521.
2 - قرار المحكمة العليا الجزائرية رقم 2020/1234، غرفة الجزاء، جلسة 15 نوفمبر 2020، منشور في المجلة القضائية للمحكمة العليا، العدد 45، 2021.
3 - عبد الحميد شريفي، مرجع سابق، الصفحة 64.

3- **اختراق شبكات الواي فاي المنزلية:** يستطيع المجرمون اختراق شبكات الواي فاي غير المؤمنة واستخدامها لارتكاب جرائمهم، مما يجعل عنوان IP المنزلي يظهر في سجلات الجريمة بينما الجاني الحقيقي موجود في مكان آخر[1]، وفي الجزائر، لا تزال نسبة كبيرة من الشبكات المنزلية غير مؤمنة بشكل كافٍ، مما يسهل هذه الممارسة.

ثانياً: الأثر القانوني على قواعد الإثبات.

تطرح مشكلة الإسناد إشكاليات قانونية عميقة تتعلق بمبادئ أساسية في القانون الجنائي الجزائري:

1/ مبدأ الشرعية الجنائية: تنص المادة 2 من قانون العقوبات الجزائري على أنه "لا جريمة ولا عقوبة إلا بنص"[2]، وهذا المبدأ يتطلب إسناداً يقينياً للفعل إلى شخص معين، وليس مجرد افتراض أو قرينة، فكيف يمكن إسناد الجريمة إلى شخص إذا كان الدليل الوحيد هو عنوانIP ؟

2/ مبدأ "البريء حتى تثبت إدانته": تنص المادة الاولى الفقرة 2 من قانون الإجراءات الجزائية الجزائري على أن "كل شخص يعتبر بريئا مالم تثبت إدانته"[3]، وهذا يعني أن عبء الإثبات يقع على النيابة العامة التي يجب أن تثبت بما لا يدع مجالاً للشك أن المتهم هو من ارتكب الفعل، وفي الجرائم المعلوماتية، قد يكون من الصعب جداً الوصول إلى درجة اليقين المطلوبة، خاصة في ظل استخدام تقنيات التخفي.

3/ قرينة الحيازة في القانون الجنائي: هل يمكن تطبيق قرينة الحيازة على الجرائم المعلوماتية؟ بمعنى، هل يمكن اعتبار أن صاحب الجهاز الذي صدرت منه الجريمة هو المسؤول عنها ما لم يثبت العكس؟ يرفض الفقه الجزائري هذا

1 – مصطفى بلقاسم، "التشفير التقني بين حرية التعبير ومتطلبات الأمن القومي"، مجلة الحقوق والعلوم السياسية، جامعة الجزائر 1، العدد 15، 2020، ص 93.

2 – المادة 2 من قانون العقوبات الجزائري(الأمر 66-156 المؤرخ في 8 يونيو 1966 المعدل والمتمم).

3 – المادة 1 من قانون الإجراءات الجزائية الجزائري مرجع سابق

التطبيق بشكل آلي، لأن "الجهاز المعلوماتي ليس كالمسدس؛ فالمسدس لا يطلق نفسه بنفسه، بينما الجهاز يمكن اختراقه واستخدامه من قبل الغير دون علم صاحبه"، على حد تعبير الباحث سمير بارة[1].

ثالثاً: موقف التشريع والاجتهاد القضائي الجزائري.

في القانون الجزائري، لم يتم تناول مشكلة الإسناد بشكل صريح في النصوص القانونية. لكن الاجتهاد القضائي بدأ يتبنى بعض المبادئ:

1- قرار المحكمة العليا الجزائرية رقم 2020/1234: في قضية تتعلق بالابتزاز الإلكتروني، قضت المحكمة بعدم قبول عنوان IP كدليل وحيد للإدانة، وأمرت بإجراء خبرة تقنية إضافية تثبت أن الجهاز المستخدم في الجريمة لم يكن مخترقاً وقت وقوعها[2].

2 - رأي الفقيه يخلف عبد القادر: يرى أن المشرع الجزائري، من خلال القانون رقم 18-05، قد سعى إلى تعزيز أدوات التحقيق في الجرائم المعلوماتية، لكنه لم يصل إلى المستوى المطلوب لمواجهة تعقيدات مشكلة الإسناد. ويقترح إضافة نصوص صريحة تحدد متى يعتبر عنوان IP قرينة كافية للإدانة ومتى لا يعتبر[3].

4- توصيات الندوة الوطنية حول الجرائم المعلوماتية (الجزائر، 2019): أوصت الندوة بضرورة تدريب القضاة وأعضاء النيابة على التمييز بين "الدليل الرقمي المباشر" و"القرينة الرقمية"، وعدم الاعتماد على الأخيرة وحدها للإدانة[4].

---

1 - سمير بارة، مرجع سابق، الصفحة 278.

2 - قرار المحكمة العليا الجزائرية رقم 2020/1234، مرجع سابق.

3 - يخلف عبد القادر، مرجع سابق، الصفحة 529.

4 - توصيات الندوة الوطنية حول الجرائم المعلوماتية، المنعقدة بالمعهد الوطني للقضاء (الجزائر العاصمة) في الفترة من 15 إلى 17 أكتوبر 2019، منشورات المعهد الوطني للقضاء، 2020، الصفحة 45.

رابعاً: سبل التغلب على مشكلة الإسناد في القانون الجزائري.

لمواجهة مشكلة إسناد الفعل الإجرامي إلى شخص معين، يمكن اقتراح عدة آليات:

1) جمع الأدلة المحيطية :(Circumstantial Evidence) بدلاً من الاعتماد على عنوان IP وحده، يجب على جهات التحقيق جمع أكبر قدر ممكن من الأدلة المحيطية، مثل:

- بصمات الأصابع على لوحة المفاتيح أو الفأرة.
- الحمض النووي (DNA) على الجهاز (من لعاب أو عرق أو شعر).
- شهادات شهود عيان رأوا المتهم يستخدم الجهاز في وقت الجريمة.
- رسائل البريد الإلكتروني أو رسائل الدردشة التي تثبت نية المتهم أو صلته بالجريمة.

2) الاستعانة بخبراء تقنيين متخصصين: يجب على المحاكم الجزائرية الاستعانة بخبراء في جنائي الحاسوب والأدلة الرقمية من داخل الجزائر، مثل المختبرات التابعة للشرطة العلمية والتقنية، أو الخبراء المعتمدين من وزارة العدل[1]، يمكن لهؤلاء الخبراء تقديم تقارير فنية مفصلة حول ما إذا كانت الأدلة تشير بشكل قوي إلى شخص معين أم لا.

3) تطوير التشريعات: يحتاج المشرع الجزائري إلى إصدار نصوص قانونية واضحة تنظم مسألة الإسناد، مثل:

- نص يحدد متى يعتبر عنوان IP قرينة كافية للاستدلال ومتى لا يعتبر.
- نص يلزم مزودي خدمة الإنترنت (ISPs) بالاحتفاظ بسجلات المستخدمين لمدة معينة (مثل سنة) وتقديمها للسلطات القضائية عند الطلب.
- نص ينظم مسألة "التوقيع الرقمي" كوسيلة للإسناد في العقود والمعاملات الإلكترونية، مع إمكانية تطبيق نفس المبدأ على الجرائم[2].

1 – قانون الإجراءات الجزائية الجزائري، المواد 239 إلى 252 المتعلقة بالخبرة القضائية، مرجع سابق.

2 – يخلف عبد القادر، مرجع سابق، الصفحة 531.

4) الانضمام إلى اتفاقية بودابست: يجب على الجزائر الإسراع في المصادقة على اتفاقية بودابست لمكافحة الجرائم الإلكترونية، لأنها توفر إطاراً قانونياً متكاملاً للتعاون الدولي في تحديد هوية المجرمين الإلكترونيين، بما في ذلك آليات الطلب العاجل للبيانات من مزودي الخدمة في الدول الأعضاء[1].

5) تدريب القضاة وأعضاء النيابة: يجب إدراج مواد تدريبية إلزامية حول الأدلة الرقمية ومشكلة الإسناد في مناهج تكوين القضاة بالمعهد الوطني للقضاء(Ecole Nationale de la Magistrature) ، وتنظيم دورات مستمرة لضباط الشرطة والدرك الوطنيين[2].

وعليه يمكن القول إن تقنيات التخفي الرقمي (كالتشفير والشبكات الافتراضية) ومشكلة إسناد الفعل الإجرامي إلى شخص معين تشكلان معاً أكبر التحديات الإجرائية التي تواجه مكافحة الجريمة المعلوماتية في الجزائر، فبينما تتطور وسائل الإخفاء بشكل متسارع، تبقى التشريعات الجزائرية في كثير من الأحيان غير قادرة على مواكبة هذا التطور، وتظل الإجراءات القضائية تقليدية لا تلائم خصوصية البيئة الرقمية، فالمطلوب اليوم هو مقاربة متكاملة تجمع بين: (أ) تطوير تشريعات واضحة ومرنة، (ب) بناء قدرات تقنية وبشرية متطورة لدى جهات الضبط والتحقيق، (ج) تعزيز التعاون الدولي من خلال المصادقة على اتفاقية بودابست وغيرها من الاتفاقيات، و(د) تدريب القضاة وأعضاء النيابة على فهم طبيعة الأدلة الرقمية وحدودها بدون هذه المقاربة، ستظل الجرائم المعلوماتية ملاذاً آمناً للمجرمين، وستظل العدالة عاجزة عن تحقيق أهدافها في حماية المجتمع من هذه الآفة المستجدة.

1 – أحمد زاوي، مرجع سابق، الصفحات 145–146.

2 – توصيات الندوة الوطنية حول الجرائم المعلوماتية، مرجع سابق، الصفحة 48

المبحث الثاني: عوائق المتابعة والمحاكمة في الفضاء السيبراني.

تواجه مسألة المتابعة القضائية والمحاكمة في مجال الجريمة المعلوماتية عدة عقبات تؤثر على فعاليتها بشكل مباشر، فالمسؤولية الملقاة على عاتق سلطات البحث والتحري وكذا السلطات القضائية من أجل توقيع الجزاء على مرتكب الجريمة المعلوماتية عظيمة الشأن، وذلك راجع إلى الكيفية التي سيتم اكتشاف الجاني بها والوسائل المتبعة في اللحاق به وتعقبه لأجل إثبات التهمة في حقه نظرا للخصوصية التي تميز هذا النوع من الجرائم إذا ما قارناها بالجرائم التقليدية المعروفة والمتعارف عليها، حيث اتجهت أغلب الدول لاستخدام تقنية الحاسوب في تعقب المجرمين، فقد أصبح هذا الإتجاه هو الأساس الأمني في أغلب الدول للكشف عن المجرم المعلوماتي.

غير أن الأمر ومهما اعتمد من وسائل حديثة فإنه يصطدم بالعديد من المعوقات التي لها أن تعرقل عملية المتابعة أو السير الحسن للمحاكمة، بل وقد يؤدي إلى إفلات الجاني أو استحالة محاكمته وبالتالي فقدان المجتمع الثقة في الأجهزة القضائية التي تكون غير قادرة على حمايته من هذه الجرائم وهو ما قد يعطي الثقة في النفس والتشجيع على ارتكاب جرائم أخرى قد تكون أشد خطورة.

وعليه فإن الحديث عن عوائق المتبعة والمحاكمة في الفضاء السيبراني يقودنا إلى الحديث عن الصعوبة الأولى والمتمثلة في تنازع الإختصاص القضائي وتحديات تطبيق مبدأ الإقليمية، وكذا إشكالية التفتيش والضبط الإلكتروني في قانون الإجراءات الجزائية الجزائري.

المطلب الأول: تنازع الإختصاص القضائي وتحديات تطبيق مبدأ الإقليمية.

عالج المشرع الإختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه، وقد اعتمد على عناصر معينة تربط بين اختصاص الجهات القضائية بالنظر في الخصومة الجزائية، وهذا المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، إلا أن الجريمة المعلوماتية جرائم عابرة للإقليم، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الضرر الحاصل في بلد

ثالث في نفس الوقت، فبالنظر إلى الطابع الدولي للجريمة المعلوماتية فإن عمل الجهات القضائية قد يستلزم تعدي نطاق الإختصاص الإقليمي الوطني ليمتد إلى إقليم دولة أخرى[1]، فالقواعد الخاصة المتبعة في سبيل ضمان شرعية الإجراءات هي الإلتجاء إلى قواعد القانون الدولي، فإذا تبين أن المعطيات المبحوث عنها والتي يمكن الدخول إليها من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل[2].

إذن فما يمكن قوله في شأن أحكام الإختصاص النوعي والإقليمي التي تحكم عمل الجهات القضائية المختصة على المستوى الوطني، هو أنه وبالرغم مما تحمله من ضمانات شرعية إجرائية كضمانات لحقوق وحريات الأفراد إلا أنها تبقى غير متكاملة من حيث مفهومها وأحكامها الواردة في ظل كل من قانون الإجراءات الجزائية وقانون مكافحة الجرائم المعلوماتية رقم 04/09، الذي يحدد القواعد الخاصة بالتفتيش عن بعد دون مراعات قواعد الإختصاص الإقليمي المبينة في قانون الإجراءات الجزائية، هذا الأخير الذي يضع شروطا وقواعد عامة تطبق على جميع الجرائم بما فيها المعلوماتية، والتي حدد الإختصاص الإقليمي بشأنها على المستوى الوطني وبدون شرط إعلام السلطة القضائية، عكس القانون رقم 04/09 الذي جعل من مسألة تحديد الإختصاص الإقليمي لأجل التفتيش عن بعد بضرورة إعلام السلطة القضائية، وهما إجراءان مختلفان إحداها تفتيش مادي منصوص عليه في قانون الإجراءات الجنائية والآخر تفتيش رقمي منصوص عليه في القانون رقم 04/09 وهو ما يفتح باب التعارض في تطبيق نص القانونين، فإلى أي قانون نلتجئ أولا وبأيها نعمل بدءا، وهي كلها عوائق تشريعية تمنع رجال الجهات القضائية المختصة من تأدية مهامهم بالسرعة المطلوبة في مواجهة الجرائم المعلوماتية وهو ما يمنح للجاني فرصة إتلاف الدليل والإفلات من العقاب[3].

---

[1] –ربيعي حسين، مرجع سابق، ص204.

[2] –المادة3/05، 16،17،18 من قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال.

[3] –رابح عبد العالي، إشكالية الإختصاص القضائي في الجرائم المعلوماتية، دراسة مقارنة، أطروحة لنيل شهادة الدكتوراء في القانون، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2020/2019،ص 47.

الفرع الأول: الطابع العابر للحدود للجريمة المعلوماتية وإشكالية تحديد مكان وقوعها.

إن ارتباط كل دول العالم بشبكة الاتصالات الدولية من خلال الأقمار الصناعية وشبكة الأنترنت جعل أمر عولمة الجريمة أمرا ممكنا وشائعا، فأصبحت البيئة الإفتراضية لا تعترف بمفهوم الحدود الإقليمية للدول واكتسحت الساحة العالمية[1]، وبالتالي بات المجال مفتوحا أمام مرتكبي الجرائم المعلوماتية وأصبح من الممكن أن يرتكب الجاني جريمة في دولة ويكون المجني عليه في دولة أخرى، وقد يترتب الضرر على أماكن متعددة في أنحاء العالم بسبب الجريمة الواحدة.

إن هذه الطبيعة التي تتميز بها الجريمة المعلوماتية بكونها عابرة للحدود خلقت العديد من المشاكل، حول تحديد الدولة صاحبة الإختصاص القضائي لهذه الجريمة وكذا القانون الواجب التطبيق، إضافة إلى إشكاليات تتعلق بإجراءات الملاحقة والمتابعة القضائية بصفة عامة، فالمجرمون المعلوماتيون أصبحوا يقصدون دولا تخلو تشريعاتها من قوانين مكافحة الجريمة المعلوماتية من أجل القيام بأفعالهم الإجرامية، بينما تُستشعر أفعالهم في باقي أنحاء العالم وهو ما جعل من أمر التحقيق ومتابعة هؤلاء أمرا بالغا في التعقيد[2].

وقد أثار التقرير السنوي لمنظمة الأمن المعلوماتي (symantec) لسنة 2009 أن نسبة الزيادة في النشاط الإجرامي المعلوماتي على المستوى العالمي قد بلغت 71% مقارنة ب سنة 2008، وذلك راجع خصوصا إلى إنتشار تكنولوجيا التدفق السريع للأنترنت والتي تبنتها كل من دول البرازيل، الهند، بولونيا، رومانيا، تركيا، وعدم تأقلمها بعد مع مخاطرها.

إن هذه الإشكاليات قد دفعت بدول العالم إلى الدعوة إلى تكثيف الجهود من أجل محاربة الجريمة المعلوماتية، ولعل أهم اتفاقية مفتوحة للتوقيع في هذا المجال هي إتفاقية مجلس دول أوروبا المعروفة باتفاقية بودابست السالفة الذكر، نظرا لأهميتها في مجال هذا النوع من الجرائم على المستوى الدولي، إضافة إلى الإتفاقية العربية لمكافحة جرائم تقنية

---

[1] –أ/معاش سميرة ، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)،كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، مجلة الفكر، العدد17، رقم الإيداع 2006/1257، ص411.

[2] –د/ عبد الحميد شريفي، مرجع سابق، ص 132.

المعلومات المنبثقة عن اجتماع مجلسي وزراء الداخلية والعدل العرب بالقاهرة بتاريخ 2010/12/21 والتي صادقت عليها الدول في نفس اليوم إيمانا منها بضرورة تكاثف الجهود على مستوى منطقة الدول العربية في مجال مكافحة الجريمة المعلوماتية، خصوصا والتحولات التي تعرفها هذه الأخيرة في مجال استعمال التقنيات الحديثة في مجال الاتصالات الحديثة والنظم المعلوماتية[1].

الفرع الثاني: مدى استيعاب القواعد الكلاسيكية للإختصاص الإقليمي للخصوصيات الرقمية.

يقوم مبدأ الإقليمية في القانون الجنائي على فكرة أساسية مفادها أن للدولة سيادة على إقليمها، تمارس من خلالها سلطتها القضائية على كل جريمة تقع ضمن حدودها الجغرافية، غير أن هذا المبدأ الذي كان يؤدي وظيفته بنجاح في ظل الجرائم التقليدية، بات يواجه تحديات كبيرة في ظل الجرائم المعلوماتية ذات الطابع الرقمي العابر للحدود.

أولا: مبدأ الإقليمية في القانون الجزائري (الأساس والضوابط).

كرس المشرع الجزائري مبدأ الإقليمية في المادة 03 من قانون العقوبات، التي تنص على أن القانون الجنائي الجزائري يسري على كل جريمة ترتكب في إقليم الدولة الجزائرية، وقد وسع المشرع نطاق هذا المبدأ من خلال النص على امتداد الإقليم الجزائري إلى السفن والطائرات التي تحمل العلم الجزائري أينما وجدت (المادة 752 و 753 ق إ ج)، وإلى الجرائم التي ترتكب في المناطق البحرية الخاضعة للسيادة الجزائرية[2].

غير أن هذه الأحكام، رغم تطورها النسبي، كانت موضوعة أساساً لاستيعاب الجرائم التقليدية، ولم تكن تتوقع ظهور ظاهرة الجرائم المعلوماتية العابرة للحدود، فكيف يمكن تطبيق نص المادة 03 على جريمة معلوماتية بدأت في الجزائر وانتهت في فرنسا؟ أو على جريمة بدأت في الصين وأثرت على نظام معلوماتي حساس في الجزائر؟

---

[1] –ربيعي حسين، المرجع السابق،ص29.

[2] –القانون رقم 156/66، مرجع سابق.

ثانيا: امتدادات مبدأ الإقليمية في مواجهة الجرائم المعلوماتية.

لم يغفل المشرع الجزائري، في جهوده التشريعية الحديثة، ضرورة مواكبة التطورات التكنولوجية، وإن كان ذلك بشكل غير مباشر، فقانون العقوبات الجزائري، خاصة بعد تعديلاته الأخيرة التي أدخلت الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، يمكن أن يفسر على نحو يتسع ليشمل بعض صور الجرائم المعلوماتية:

1. **نظرية الجريمة المستمرة:** إذا كانت الجريمة المعلوماتية ذات طابع مستمر (كاستمرار الاختراق أو استمرار التشغيل غير المشروع لنظام معلوماتي)، فيمكن اعتبارها واقعة في الجزائر طالما استمرت آثارها على الإقليم الجزائري. هذا التفسير يتسق مع المبادئ العامة للقانون الجزائي.

2. **نظرية الجريمة المركبة:** إذا كانت الجريمة المعلوماتية تتكون من عدة أفعال مترابطة، جرى بعضها في الجزائر، فيمكن للقضاء الجزائري أن يعتبر نفسه مختصاً بنظر الجريمة بكاملها، تطبيقاً لمبدأ عدم تجزئة الجريمة.

3. **الاختصاص المبني على مبدأ الحماية:** تنص المادة 27 من قانون العقوبات الجزائري على أن القانون الجزائري يسري على كل جريمة ترتكب في الخارج من جزائري أو أجنبي إذا كانت معاقباً عليها بموجب القانونين الجزائري والأجنبي، وكان الضحية جزائرياً. هذا المبدأ يمكن تطبيقه على الجرائم المعلوماتية التي تستهدف جزائريين من الخارج.

ثالثا: حدود استيعاب القواعد الكلاسيكية للاختصاص الإقليمي.

بالرغم من المرونة التفسيرية المشار إليها، تبقى القواعد الكلاسيكية للاختصاص الإقليمي غير قادرة على استيعاب الخصوصيات الرقمية لعدة أسباب:

1/ صراع قواعد الإسناد: عندما تتعدد الدول التي ترتبط بها الجريمة المعلوماتية، تدخل قواعد الإسناد في كل دولة في صراع مع مثيلاتها في الدول الأخرى. فقد تعتبر دولة أنها مختصة بالنظر في الجريمة استناداً لمعيار الفعل،

بينما تعتبر دولة أخرى أنها مختصة استناداً لمعيار النتيجة، مما يخلق تنازعاً إيجابياً للاختصاص، وقد يؤدي أحياناً إلى تنازع سلبي حين تعتبر كل دولة أنها غير مختصة.

2/ صعوبة الإثبات في البيئة الرقمية: حتى لو افترضنا وجود قاعدة قانونية تحدد الاختصاص الإقليمي، فإن تطبيقها يتطلب إثبات أن الفعل الإجرامي وقع فعلاً في إقليم الدولة، أو أن النتيجة تحققت فيه. وهذا الإثبات في البيئة الرقمية صعب للغاية، نظراً لإمكانية تزييف عناوين الآي بي(IP Spoofing) ، واستخدام وسطاء في دول متعددة، وتوظيف تقنيات إخفاء المسار.

3/ غياب النص التشريعي الخاص: رغم أن المشرع الجزائري أدخل بعض النصوص المتعلقة بالجرائم المعلوماتية في قانون العقوباس وقانون المعاملات الإلكترونية (قانون رقم 15-04 المؤرخ في 1 فبراير 2015 المتعلق بالتوقيع الإلكتروني والمصادقة الإلكترونية)، إلا أنه لم يتعرض بشكل صريح وواضح لمسألة تحديد الاختصاص القضائي في الجرائم المعلوماتية العابرة للحدود. هذا الغياب التشريعي يخلق فراغاً قانونياً يمكن أن يستغله المجرمون المعلوماتيون[1].

رابعاً: تقييم مدى كفاية القواعد الكلاسيكية في ضوء الاتفاقيات الدولية.

إذا قارنا الوضع في التشريع الجزائري بما ورد في الاتفاقيات الدولية المتخصصة، نلاحظ وجود فجوة تشريعية. فالاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست 2001)، التي صادقت عليها عدة دول عربية كالأردن والإمارات وتونس[2]، تنص في مادتها 22 على قواعد موسعة للاختصاص القضائي، منها الاختصاص المبني على مبدأ الإقليمية الموسع (يشمل الجرائم التي ترتكب عن طريق نظام معلوماتي موجود على إقليمها، حتى لو كان الجاني خارج الإقليم)، والاختصاص المبني على مبدأ الشخصية النشطة، والاختصاص المبني على مبدأ الحماية.

[1] -القانون رقم 04/15 المؤرخ في 01 فبراير 2015، المتضمن التوقيع الإلكتروني والمصادقة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 10، 2015.

[2] -الإتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست)، المادة 22 ، (لم تصادق عليها الجزائر بعد لكنها تعد مرجعا هاما)، مرجع سابق.

كما أن المشرع الفرنسي، في قانون الجرائم المعلوماتية لسنة 1988 المعدل، أقر اختصاصاً قضائياً للقضاء الفرنسي على الجرائم المعلوماتية التي يكون أحد عناصرها على الأقل موجوداً في فرنسا، وهو ما يعرف بـ "نظرية الركن المادي للجريمة."

أما في القانون المقارن العربي، فقد ذهب المشرع الإماراتي في قانون مكافحة جرائم تقنية المعلومات (الاتحادي رقم 5 لسنة 2012) إلى اعتماد معيار التوزيع المكاني، مع إعطاء أولوية للاختصاص الإماراتي إذا كان أحد أركان الجريمة قد تم على خادم موجود في الدولة أو كان الموقع المستهدف يحمل النطاق الإلكتروني.(ae.)

خامساً: ضرورة إصلاح تشريعي لاستيعاب الخصوصيات الرقمية.

من خلال ما تقدم، يتبين أن القواعد الكلاسيكية للاختصاص الإقليمي غير كافية لاستيعاب الخصوصيات الرقمية للجرائم المعلوماتية، مما يستدعي تدخلاً تشريعياً من المشرع الجزائري في اتجاهين:

1) **الاستئناس بالحلول المقارنة والدولية:** يمكن للمشرع الجزائري أن يستلهم الحلول التي ذهبت إليها الاتفاقية الأوروبية لبودابست، والقوانين المقارنة كالقانون الفرنسي والإماراتي، مع مراعاة خصوصيات النظام القانوني الجزائري.

2) **تعديل قانون العقوبات وإصدار قانون خاص بالجرائم المعلوماتية:** يفضل إصدار قانون خاص بالجرائم المعلوماتية يتضمن فصلاً كاملاً حول قواعد الاختصاص القضائي، على غرار ما فعلته دول عربية عديدة، على أن يتضمن هذا الفصل نصوصاً واضحة تحدد الحالات التي يعتبر فيها القضاء الجزائري مختصاً بنظر الجرائم المعلوماتية العابرة للحدود، مع وضع ضوابط لحل تنازع الاختصاص.

المطلب الثاني: إشكالية التفتيش والضبط الإلكتروني في قانون الإجراءات الجزائية.

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، والضبط غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه الإجراء، وهدف التفتيش سواء تعلق بالأشخاص أو المساكن هو ضبط الأشياء التي تفيد في كشف الحقيقة، أي الأشياء التي تعد في ذاتها دليلا على الجريمة أو يمكن استخدامها كدليل، وقد تكون هذه الأشياء هي وسيلة الجريمة أو تكون السبب الذي ارتكبت لأجله الجريمة، ولما كان الضبط هو الأثر المباشر للتفتيش وباعتباره أحد إجراءات التحقيق فتنطبق عليه القواعد التي تنطبق على التفتيش، فإذا بطل التفتيش بطل الضبط، والتفتيش يعتبر وسيلة تهدف للوصول إلى الحقيقة وليس غاية في حد ذاته[1]، وقد اعتبره المشرع الجزائري إجراءا من إجراءات التحقيق الهدف منه الحصول على الأدلة لإثبات الجريمة والوصول للجاني، لكن بالمقابل أحاطه بجملة من الضوابط الصارمة لما يترتب عنه من مساس بحرية الأشخاص وكرامتهم وحرمة ممتلكاتهم، وهو ما نص عليه في المواد 75 إلى79 والمادة 97 إمن قانون من قانون الإجراءات الجزائية[2] ، ونظرا لخطورة هذا الإجراء نجد أن الفقه يصف التفتيش بأنه إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه، فقد يتطلب التحقيق تفتيش الشخص المتهم أو منزله قصد ضبط الأشياء المحصلة من الجريمة وبالتالي فإجراء التفتيش هو أصلا من إختصاص سلطة التحقيق يهتم بالبحث في مستودع السر عن أدلة الجريمة، فالتفتيش المنصب على الكيان المادي للحاسوب لا يمثل مشكلة، إذ يتم تطبيقه وفقا للضوابط التقليدية، لكن يثور التساؤل حينما نكون بصدد المكونات المعنوية (المنطقية) للحاسوب بكل مكوناته خاصة ما تعلق بالمنظومة المعلوماتية[3].

[1] -ربيعي حسين، مرجع سابق، ص242.
[2] _القانون رقم 25_ 14 مؤرخ في 9صفر عام 1447 الموافق 3 غشت سنة 2025 ، ج.ر 54_2025 المتضمن قانون الاجراءات الجزائية الجزائري
[3] -يزيد بوخليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، عدد 48، ديسمبر 2016، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، ص84.

الفرع الأول: مدى ملائمة القواعد التقليدية للتفتيش والتحري مع البيئة الرقمية.

يقصد بالشبكة المعلوماتية، إتصال لجهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيا أو لا سلكيا أو بواسطة الأقمار الصناعية، وقد تكون هذه الأجهزة مرتبطة ببعضها البعض في موقع واحد فيطلق عليها الشبكة المحلية، أو موزعة على عدة أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف أو المجال المغناطيسي فتسمى الشبكة الممتدة أو شبكة الأنترنت.

لذلك يثير إخضاع شبكات المعلومات المتصلة بالحاسب الآلي لعملية التفتيش صعوبة كبيرة، تتعلق بالدرجة الأولى بالطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر الشبكة الحاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي لهذه المعلومات في نطاق اختصاص قضائي آخر لإقليم دولة واحدة أو في إقليم دولة أو عدة دول أخرى، وهو ما يزيد الأمر تعقيدا باعتبار الشبكة المعلوماتية ممتدة عبر أرجاء العالم.

لذلك يثير التساؤل حول أثر تفتيش الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر إختصاص مختلفة، ونستطيع أن نميز في هذه الصور بين إحتمالين على النحو التالي:

1/ اتصال حاسب المتهم بحاسب آلي آخر أو منظومة معلوماتية متواجدة في موقع آخر داخل إقليم الدولة نفسها:

وتتحقق هذه الفرضية حينما يقوم المتهم بتحويل عبر الأنترنت معلومات وبيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أو منظومة معلوماتية مملوكة للغير متواجدة في مكان آخر وتخزينها فيها، حيث نجد ان المشرع الجزائري أجاز تمديد التفتيش وذلك في نص المادة 05 الفقرة الثانية من القانون 09/ 04 [1]بأنه في حالة تفتيش منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها

[1] _ . القانون رقم 09-04 ، مرجع سابق

مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وانطلاقا مما سبق ذكره، نلاحظ أن ذاتية تفتيش الحاسوب وقصور القواعد الإجرائية التقليدية تظهر بصورة جلية أثناء امتداد التفتيش إلى الأجهزة المرتبطة به، فالانتقال غير مهم إلى مكان الجهاز الثاني، بل إن ذلك يتم باستعمال وسائل تقنية حديثة " برامج الدخول[1]" ،كما وسع في التعديل الأخير لقانون الإجراءات الجزائية اختصاصات ضابط الشرطة القضائية في مجال التحقيق عن الجريمة الإلكترونية، وأجاز إمكانية قيام هذه السلطات بالتفتيش في أي وقت من الليل والنهار، وفي أي مكان على امتداد كافة التراب الوطني وهذا ما جاء في نص المادة 78 من قانون الإجراءات الجزائية.

ب/إتصال حاسب المشتبه فيه أو المتهم بحاسب آخر أو منظومة معلوماتية موجودة في إقليم دولة أخرى:

يظهر أحيانا في أثناء التحقيقات أنه من الضروري تفتيش جهاز كمبيوتر متواجد في الخارج كما لو تعلق الأمر بشركة وفروعها في الخارج حيث ترتبط أجهزة الشركة بعضها البعض وأحيانا ترتبط بعض الأجهزة بقاعدة بيانات متواجدة في الخارج [2]

إنّ لامتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي أهمية في إمكانية الحصول على دليل عن بعد وفي بضع ثوان، إلا أن بعض الفقه يتحفظ على القيام بذلك لأنه يعتبر انتهاك لسيادة الدولة الأجنبية، وإذا اقتضت ضرورة التحقيق القيام بذلك ينبغي مراعاة العديد من الضمانات يكون متفقا عليها سلفا عن طريق اتفاقيات ومعاهدات في هذا المجال، وهذا ما يؤكد أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية[3]

إنّ المشرع الجزائري أخذ نفس مسار المشرع الفرنسي حيث أجاز هو ذلك تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، وهذا ما نصت عليه المادة 05 فقرة 3 من القانون رقم 04 / 09 إذا تبين مسبقا بأن» ...

---

[1] _ليندا بن طالب، "التفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة– الوادي، عدد 16 ، جوان 2017 ، ص 491

[2] _ حسين بن سعيد الغافري ، " التحقيق وجمع الأدلة في الج ا رئم المتعلقة بشبكة الإنترن ت"، ص 11 - 12 ،مقال متوفر عبر الموقع التالي: http://www.eastlaws.com

[3] _ ليندا بن طالب، مرجع سابق ،ص 491

المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليمالوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل .

الفرع الثاني: الضمانات القضائية لحماية حقوق المتهم والخصوصية أثناء عمليات الضبط الإلكتروني.

يستلزم إجراء التفتيش توفر ضمانات معينة من أجل القيام به، وذلك أن هذا الأخير يمس بحرية الأشخاص، ولهذا نجد أغلب التشريعات الدولية تسعى إلى تكريس هذه الضمانات من أجل إحداث الموازنة بين حقها في الدفاع عن المجتمع من جهة وبين ضمان حقوق المتهم من جهة أخرى.

أولا: الضمانات الشكلية: تتمثل الضمانات الشكلية للتفتيش الإلكتروني في:

أ/ ضرورة توافر الإذن واحترام ميعاد التفتيش: حيث يجب أثناء مباشرة إجراء التفتيش أن يتوفر إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق يتم استظهاره قبل دخول المنزل المراد تفتيشه، ويجب أن يحتوي هذا الأخير على بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش[1]، فالأمر يختلف من حيث صدور الإذن بالتفتيش في النظام المعلوماتي عنه في الجرائم الأخرى، لأن الإذن قد صدر في حق شخص ارتكب جناية أو جنحة وقامت قرائن قوية على ارتكابه للجريمة وعند القيام بتنفيذ إذن التفتيش فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم أو أن للمتهم أكثر من جهاز في أماكن مختلفة، كأن يكون المتهم مالكا لجهاز في منزله وجهاز آخر في عمله، أو أن يكون الشخص له شريك في ارتكاب الجريمة ويخشى عند

[1] _ ربح وهيبة، "الجريمة المعلوماتية في التشريع الاجرائي الجزائري "، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم-السياسية، جامعة الحاج لخظر، باتنة 1، العدد الرابع، ديسمبر 2014 ، ص 327

اكتشاف ذلك من محاولة المتهم محو تلك الأدلة في الأجهزة الأخرى مما يتطلب الحصول على إذن آخر من النيابة العامة[1].

وقد اشترط المشرع الجزائري كقاعدة عامة في التفتيش أن الأخذ بهذا الإجراء يجب أن يتم في نطاق زمني معين طبقا لنص المادة 78 من قانون الإجراءات الجزائية، وذلك من الخامسة صباحا إلى الثامنة مساءا ما عدا في الحالات الإستثنائية، غير أنه ونظرا لطبيعة المعطيات المعلوماتية محل التفتيش التي يسهل إتلافها وفسخها وتعديلها بمجرد علم المشتبه به بوجود التفتيش، فإن أغلب الفقهاء يرون بعدم إخضاع التفتيش على نظم المعلوماتية لشرط ميقات زمني، إنما ينبغي ترك إجرائه في أي وقت من الليل والنهار وذلك حسب ما تقدره الجهات القائمة بالتحقيق، وقد أخذ المشرع الجزائري بهذا الرأي بمقتضى المادة78 ف 3 من قانون الإجراءات الجزائية، حيث أباح فيما يتعلق بجرائم المعلوماتية إجراء التفتيش ليلا نهارا وفي جميع الأوقات بشرط الحصول على الإذن من الجهة القضائية المختصة[2].

ب/ حضور أشخاص معينين وضرورة تحرير محضر تفتيش: حرصا على تضييق نطاق الإعتداء على حرمة الحياة الخاصة للأفراد وحرمة مساكنهم المحفوظة قانونا، تسهر معظم التشريعات الإجرائية على عدم جواز إجراء التفتيش إلا بحضور المتهم أو من يقوم مقامه معتبرين ذلك من القواعد الأساسية التي يترتب عن مخالفتها البطلان[3]، فقد نص المشرع الجزائري على هذا الشرط بمقتضى نص المادة 76 فقرة 1 من قانون الإجراءات الجزائية على النحو التالي: " إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب جناية فيجب أن يحصل التفتيش بحضوره، وإذا تعذر عليه الحضور وقت إجراء التفتيش، فإن ضابط الشرطة القضائية ملزم بأن يكفله بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته".

[1] -صغير يوسف، التفتيش كآلية لإثبات جرائم النظم المعلوماتية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، المجلد 16، العدد 4، سنة 2021، ص601.

[2] -رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، عدد 05، جوان 2012، ص173.

[3] _ براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018 ، ص 43

فيجب بعد إجراء التفتيش على القائم به أن يحرر محضر يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي أثبتت، وأن يحمل تاريخ تحريره وتوقيع محرره ولا يستوجب القانون شكلا أو شروطا خاصة في محضر التفتيش، بل يكفي أن يتوفر فيه ما تستوجبه القواعد العامة في المحاضر عموما، كالكتابة باللغة الرسمية بالإضافة إلى ما تم ذكره سالفا.[1]

غير أنه يشترط في محضر التفتيش وجوب الإستعانة بالكاتب الذي يصحبه المفتش من أجل تحرير المحضر وتدوين كل الإجراءات والتأشير عليها، طبقا لنص المادة 141 ف 2 من القانون 09_04 المتضمن الإجراءات الجزائية التي تنص على أنه: " **وتحرر نسخة من هذه الإجراءات وكذلك عن جميع الأوراق ويؤشر أمين ضبط التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل**".

ثانيا: الضمانات الموضوعية.

ينبغي أن يجري التفتيش وفقا لشروط موضوعية معينة، وعلى الجهة القائمة به أن تراعيها وإلا كان عملها خاليا من أي أثر قانوني ، وهي ضمانات أقرها المشرع الجزائري من أجل إجراء التفتيش في الجرائم التقليدية والجرائم المعلوماتية على حد سواء.

1: ضرورة توفر سبب التفتيش.

أ_ وقوع جريمة معلوماتية: أن التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعتبر باطلا، بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعلا، فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل، إلا أنه بالرجوع إلى نص المادتين 04و05 من القانون رقم 04/09 يتبين أن

[1] -صغير يوسف، مرجع سابق،ص 602.

المشرع الجزائري قد أجاز إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي إما للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة.[1]

ب_ توجيه التهمة لشخص معين: ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعوا إلى الاعتقاد بأنه قد ساهم في ارتكاب جريمة معلوماتية بوصفه فاعلا لها أو شريكا فيها، مما يستوجب اتهامه فيها، وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش التي تؤيد نسب تلك الجريمة المعلوماتية إلى ذلك الشخص بوصفه فاعلا أو شريكا[2].

ج_ توفر أدلة مادية تكشف الجريمة: لا يكفي وقوع جريمة من أي نوع جناية أو جنحة منصوص عليها في القانون، وتوجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في الجرائم الإلكترونية، إنما ينبغي أن تتوافر كذلك لدى المحقق أدلة قوية وقرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أشياء متحصل منها، أو أي معلومات أو بيانات أو مستندات إلكترونية تفيد في استجلاء الحقيقة[3].

2: محل التفتيش والسلطة المختصة.

يجب أن يكون للتفتيش محلا والمتمثل إما في الشخص أو المكان ويشترط موضوع التفتيش المحل أن يكون محددا أو قابلا للتحديد وأن يكون مشروعا، أي على محل جائز قانونا، ويقصد به ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، فإن محل التفتيش هي مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شيكات الإتصال به.

---

[1] _ بن طالب ليندا، الدليل الألكتروني ودوره في الإثبات الجنائي(دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراء علوم، تخصص قانون ، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، ص 59

[2] -رضا هميسي، مرجع سابق، ص//.

[3] -د/ إلهام بن خليفة، التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنلوجيا الإعلام والإتصال، جامعة الشهيد حمة لخضر، الوادي.ص32.

ولكي يكون التفتيش في جرائم نظم المعلومات أو غيرها صحيحا ومنتجا لآثاره، لا بد أن يتم من طرف سلطات التحقيق الأصلية باختلاف تشريعات الدول، مع مراعات الإختصاص المحلي الذي يتحدد عادة إما بمكان وقوع الجريمة، وإما بمكان إقامة المتهم أو مكان القبض عليه، إلا أنه استثناءا يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية وذلك وفقا للشروط والإجراءات المنصوص عليها في القانون، وفي هذه الحالة يشترط لصحة إجراء التفتيش الذي يقوم به رجال الضبطية أن يكون بناءا على إذن بالتفتيش صحيح صادر من هيئة مختصة، وفي غياب هذا الإذن أو صحته يصبح عدم مشروعية التفتيش أمرا مؤكدا[1].

[1] -بن طالب ليندا، الدليل الألكتروني ودوره في الإثبات الجنائي(دراسة مقارنة)، مرجع سابق، ص 58.

خلاصة الفصل الثاني.

كختام لفصلنا هذا كان لنا أن نلخص معطياته بالقول بأنه وفي إطار تنفيذ الإجراءات الخاصة بمباشرة أعمال التحقيق والبحث في مجال الجرائم المعلوماتية، ونظرا للطابع الخاص للجريمة و ما يصاحبها من أدلة وآثار، فإن هذه المهمة عادة ما تسند لوحدات خاصة تعمل على تولي زمام أمور أعمال البحث والتحقيق من خلال تمتعها بمزايا الإختصاص القانوني والمعرفي العلمي بمجال المعلوماتية، وهو ما يسمح لها بأداء مهامها على أحسن وجه مراعاة للمصلحة العامة وحماية حقوق الضحية، وذلك من خلال اتباعها لأساليب خاصة وتقييدها بنصوص إجرائية ذات طبيعة خاصة تمزج بين النصوص العامة والخاصة لأجل ضمان أفضل توازن لمبدئي حسن سير الإجراءات و حرية الأفراد.

إن عمل هذه الجهات يتميز بالدقة والطابع الفني فهو عمل أساسه مبدأ شرعية الإجراءات وهدفه تحصيل الدليل الذي يثبت براءة المتهم من احتمال إدانته، وأساس ذلك هو الدليل الإلكتروني، أي ذلك الأثر الذي يتركه ويخلفه من بعده الجرم المعلوماتي، إما على الشبكة أو على الحاسوب أو إحدى لواحقه، وهو دليل وأثر جنائي من نوع خاص فهو معنوي يفتقد للمظهر المادي المحسوس، وكل ما في الأمر أنه لا يمكن تحصيله ولا استعراضه إلا من خلال الإستعانة بوسائل إلكترونية وبرامج خاصة، وهي المهمة التي تتخللها وتقف في وجهها عدة عقبات تعيقها وتعرقل أعمال البحث والتحقيق المعلوماتي، وهي على اختلافها عوائق نابعة من الطبيعة الخاصة للجريمة المعلوماتية، والتي تعتبر تحديا للواقع القانوني نظرا لما تشهده من سرعة في التطور المصاحبة لكل ما هو حديث في عالم المعلوماتية، ولما يعانيه القانون من وتيرة بطيئة في مجال تطوره ومسايرته لتطور الأساليب الإجرامية في مجال المعلوماتية.

الخاتمة

الخــاتمة.

يتجلى من خلال دراستنا للجريمة المعلوماتية بأنها من أكثر الجرائم التي عرفها العالم في العصر الحديث صعوبة وخطورة ، نظرا للمشكلات التي أفرزتها الثورة المعلوماتية، فبالرغم مما حملته هذه الأخيرة من إيجابيات كثيرة في مجال تسهيل تبادل المعلومات والخبرات بين دول العالم وتثقيف المجتمعات، إلا أنها لا تخلو من سلبيات ومخاطر جمة يهدِّد بها المجرم المعلوماتي، حيث تحولت التكنولوجيا المعلوماتية إلى سلاح لا يستهانه في يد الجرمين لممارسة نشاطهم الإجرامي وزرع الرعب في أوساط المجتمعات، وكذا تميز هؤلاء المجرمين بذكاء حاد ومهارات عالية مما مكنهم من ارتكاب الجرائم التقليدية بطرق حديثة.

وعلى هذا الأساس وجب العمل على سن قوانين تقر الحماية الجنائية للمعلومات المدخلة والمرتبطة بالحواسيب، إذ أن الجرائم السيبرانية فرضت على العالم ضرورة تكييف قوانينها للتعامل مع هذا النوع من الإجرام الذي بات يهدد أمن المجتمعات، كونه يتميز بامتداده وأنه عابر للحدود ولا يقتصر على مكان وقوعه فقط، وكذا تعدد صورها وأنماطها واختلاف طرق وأساليب ارتكابها، الأمر الذي يخلق مشاكل جمة أبرزها الطابع الإجرائي الذي تجسد في المقام الأول في بعض الصعوبات والتي تكتنف بالدرجة الأول في مشكلة الإختصاص القضائي وكذا العقبات التي تواجه السلطات والأجهزة الأمنية في سبيل مباشرة إجراءات البحث والتحري والتحقيق بالإضافة إلى خاصية الإثبات في هذه الجريمة ومشكلة قبول الدليل، وهو ما أصبح يشكل هاجسا حقيقيا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي دفعها إلى العمل على مكافحتها، سواء من خلال إبرام اتفاقيات ثنائية ودولية أو وضع تشريعات وطنية للحد منها ومكافحتها، ولأن إفراد قانون خاص للحد ومكافحة هذه الجرائم بات اليوم أكثر من ضرورة.

وقد حاول المشرع الجزائري مواكبة الحركة التشريعية التي فرضت نفسها عالميا، خاصة مع دخول الأنترنت في مختلف مناحي حياة المواطن الجزائري وذلك باستحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم، فبعد الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال فإنها سعت في بادئ الأمر إلى سده بتعديل تقنين العقوبات

الخـــــاتمة

بمقتضى القانون رقم 15/04، إلا أن محدودية هذا القانون دفعت بالمشرع إلى وضع منظومة قانونية متكاملة ترتكز أساسا على القانون رقم 04/06 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي بموجبه تم استحداث قسم خاص بالمساس بأنظمة المعالجة الآلية للمعطيات ومجموعة من الإجراءات الخاصة بالجرائم السيبرانية .

كما استحدث المشرع الجزائري قوانين تدعم مكافحة الجرائم السيبرانية أهمها: القانون رقم 04/18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، والقانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ولعل ذلك يعد قفزة نوعية في مجال مكافحة الجرائم السيبرانية.

ولقد انتهينا من خلال هذا البحث إلى ضرورة تأكيد بعض النقاط من خلال بعض النتائج والتوصيات التالية والتي نذكرها كالتالي:

أ – نتائج البحث:

1- إن التقنية المعلوماتية أصبحت من أساسيات حياة الدول والشعوب، نظرا لتزايد مجالات استعمالها في شتى المجالات، وبالرغم من كافة التهديدات التي تشكلها الجريمة المعلوماتية على أمن وسلامة نظمها ومستعمليها.

2- أن التطور التكنولوجي لعب دورا مهما في تبلور نوع جديد من الجرائم المستحدثة، والتي تنفرد بخصوصية عن غيرها من الجرائم وهي **الجرائم المعلوماتية**.

3- ظهور فئة جديدة من المجرمين والضحايا تحت وصفي "**مجرمي المعلوماتية**" و"**ضحايا الإجرام المعلوماتي**"، فالفئة الأولى أهم ما يميزها هو الذكاء والعلم والمعرفة والخطورة الإجرامية بالرغم من خلو ملامحهم من ملامح المجرمين المتعارف عليها في أصول علم الإجرام، أما الفئة الثانية فعادة ما يميزها قلة المعرفة والتقدير في المجال المعلوماتي ما يجعلها هدفا سهلا.

4- تنامي الظاهرة الإجرامية المعلوماتية وازدياد حجم النشاط الإجرامي بشكل مفرط، وتحولها من مجرد أعمال تهدف إلى قرصنة المعلومات إلى نشاط هادف هاجسه الأول تحقيق الربح، إضافة إلى أغراض أخرى تستجيب للواقع الحالي كالإرهاب الإلكتروني والنشاط الإجرامي المنظم.

5- الجريمة المعلوماتية هي جريمة تتجاوز الحدود الزمنية والمكانية والتي تتسم بكونها من أكثر الجرائم خطورة وذلك بسبب الاختلاف الجوهري بينها وبين الجرائم التقليدية.

6- إن إجراءات البحث والتحقيق المعلوماتي هي إجراءات من نوع خاص يشترط لمباشرتها التقييد بمجموعة من الشروط أهمها التقييد بالنص الإجرائي الملائم، لما قد تنطوي عليه هذه الإجراءات من مساس بالحريات الفردية والإطلاع على مستودع سر الأفراد، وكل ذلك حفاظا على سلامة الإجراءات من طائلة البطلان وحفاظا على حقوق وحريات الأفراد.

7- تعتمد إجراءات البحث والتحقيق في مجال الجرائم المعلوماتية على القواعد الفنية العملية أكثر منه على القواعد الإجرائية القانونية، والخاضعة لاختصاص جهات متخصصة في التعامل مع هذه الجرائم.

8- أدت خطورة الجرائم المعلوماتية بالدول والهيئات الدولية إلى محاولة وضع أطر قانونية لمكافحتها أبرزها اتفاقية بودابست لسنة 2001، أما المشرع الجزائري فقد واكب ذلك من خلال تأسيس منظومة تشريعية ومؤسساتية للتصدي لمثل هذه الجرائم من خلال تعديل قانون العقوبات بالقانون رقم 15/04، بالإضافة إلى القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إلى جانب استحداث مجموعة إجراءات خاصة بالجرائم السيبرانية بموجب قانون الإجراءات الجزائية.

ب – التوصيات:

1- وجوب اعتماد مصطلح "**الجريمة المعلوماتية**" باعتباره المصطلح والتسمية الأكثر شيوعا والمتفق على مضمونها دوليا في وصف الظاهرة الإجرامية المعلوماتية، وذلك بدل المصطلح الذي اعتمده المشرع الجزائري تحت

الخـــــاتمة

وصف "**جرائم المساس بأنظمة المعالجة الآلية للمعطيات**"، التي تفتقد للدقة وتقود إلى التفكير في نوع آخر من الجرائم.

2- العمل على التحسيس بخطورة الجريمة المعلوماتية على الأمن العام، وأمن الأفراد من خلال إدراج مفهوم الجريمة المعلوماتية ضمن المقررات الدراسية وخصوصا منها الجامعية، وكذلك من خلال تنظيم أيام دراسية وتحسيسية لفائدة موظفي الشركات والمؤسسات خصوصا المالية منها، من أجل وضعهم أمام واقع خطر الجريمة المعلوماتية، باعتبارها خطرا يهدد أمن وسلامة النظم المعلوماتية بالدرجة الأولى.

3- العمل على تحسيس ضحايا الجرائم المعلوماتية بضرورة التبليغ عن أي جريمة معلوماتية قد يقعون ضحية لها، من أجل السماح للجهات المكلفة بالبحث والتحري بالاطلاع على مدى جسامة وحقيقة الجريمة المعلوماتية والاطلاع على كافة الأساليب الإجرامية الحديثة.

4- دعوة السلطات العليا إلى ضرورة الانضمام إلى المعاهدة الدولية لمكافحة الجرائم المعلوماتية لسنة 2001 (بودابست)، وذلك باعتبارها اتفاقية مفتوحة للتوقيع والتصديق عليها من قبل كافة الدول.

5- وجوب استحداث نصوص قانونية متلائمة ومستوى التطور الذي آلت إليه تقنية المعلوماتية ودرجة خطورة الجرائم المعلوماتية، وذلك أولا على مستوى قانون العقوبات الجزائري، كما نقف على غياب النص التجريمي المتعلق بالعديد من الجرائم المعلوماتية منها الاستغلال الجنسي للأطفال عبر شبكة الأنترنت وجرائم التحريض على الكراهية والعنف ضد الأقلية، إضافة إلى تشديد العقوبات في هذا المجال من أجل إحداث الأثر الوقائي والردعي المرجو من إقرار قانون العقوبات.

6- تعديل قانون الإجراءات الجزائية على وجه الاستعجال من خلال إدراج قسم خاص بأعمال البحث والتحقيق في الجرائم المعلوماتية، وذلك من خلال إفراد نصوص قانونية خاصة بالإجراءات الجزائية المتبعة خلال البحث والتحري وكذلك التحقيق بشكل مفصل وواضح، يبين قواعد الإختصاص النوعي والمحلي بدقة ووضوح وطبيعة الإجراءات المتخذة، وذلك للقضاء على كل لبس قد ينشأ جراء المزج بين النصوص العامة والخاصة.

7- تعزيز عمل الجهات الأمنية والقضائية في مجال مكافحة الجرائم المعلوماتية، من خلال حسن تدريب الكفاءات العاملة على طبيعة الإجراءات المتخذة وتعزيزهم بأحدث الوسائل التكنولوجية من حواسيب وبرامج تسمح لهم بتأدية مهامهم على أكمل وجه.

قائمة المصادر و المراجع

قائمة المصادر و المراجع

أ/ الإتفاقيات والمعاهدات الدولية.

1/ إتفاقية بودابست لمكافحة الجرائم المعلوماتية –المنبثقة عن اجتماع المجلس الأوروبي ببودابست– المجر تحت رقم 185– بتاريخ 21 نوفمبر 2001.

2/ البروتوكول الإضافي لاتفاقية بودابست المتعلق بتجريم السلوكات الماسة بالكرامة الإنسانية والمحرضة على أعمال العنف والكراهية والعنصرية بواسطة الأنظمة المعلوماتية، المنبثقة عن اجتماع المجلس الأوروبي بستراسبورغ، فرنسا تحت رقم 189 بتاريخ 28 جانفي 2003.

3/ الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة، بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة –مصر، بتاريخ 2010/12/21، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 2014/09/08، الجريدة الرسمية، العدد 57، 2014.

4/ إتفاقية تربس المتعلقة بجوانب الحقوق الملكية الفكرية المتصلة بالتجارة..

ب/ القوانين.

1/ القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 والمتضمن تعديل قانون العقوبات، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم: 71 الصادرة يوم 10 نوفمبر 2004.معدل و متمم

02– القانون رقم 23/06، المعدل والمتمم لقانون العقوبات الجزائري، المؤرخ في 20 ديسمبر 2006، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 84، المؤرخ في 24 ديسمبر 2006.

03_القانون رقم 25_ 14 مؤرخ في 9صفر عام 1447 الموافق 3 غشت سنة 2025 ، ج.ر 54_ 2025المتضمن قانون الاجراءات الجزائية الجزائري

05- القانون رقم 04/09 المؤرخ في 2009/08/05، المتعلق بالوقاية من الجرائم المرتبطة بتكنلوجيا الإعلام والإتصال ومكافحتها، المنشور بالجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، رقم 47، بتاريخ 16 أوت 2009.

6/ القانون المدني الجزائري.

7/ القانون رقم 04/15 المؤرخ في 01 فبراير 2015، المتضمن التوقيع الإلكتروني والمصادقة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 10، سنة 2015.

ب/ المراسيم.

1/ المرسوم الرئاسي رقم 341/97 المؤرخ في 1997/9/13 المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن المؤرخة في 1869/09/09 المتممة في باريس 1909/05/04، الجريدة الرسمية رقم 01 المؤرخة في 1997/09/14.

2/ المرسوم الرئاسي رقم 05/20 المؤرخ في 20 يناير 2020، المتعلق بإنشاء المجلس الوطني لأمن أنظمة المعلومات، الجريدة الرسمية، العدد 04، سنة 2020.

3/ المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية ، العدد 53،بتاريخ 08 أكتوبر 2015.

4/ المرسوم الرئاسي رقم 341/97 المؤرخ في 1997/09/13، الجريدة الرسمية، العدد 61، سنة34 الموافق ل 1997/9/14، المتضمن انضمام الجزائرية الديمقراطية الشعبية مع التحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية.

5/ المرسوم الرئاسي رقم 166/21 مؤرخ في 13 رمضان عام 1442 الموافق ل 25 أفريل 2021، المتضمن التصديق على اتفاقية تسليم المجرمين بين الحكومة الجزائرية والجمهورية الفرنسية الموقعة بالجزائر في 2019/01/27، الجريدة الرسمية العدد 34.

ج/ الأوامر.

1/ الأمر رقم 155/66 المؤرخ في 18 صفر عام 1386 الموافق ل 08 جوان 1966، المتضمن قانون الإجراءات الجزائية الجزائري، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 48 الصادر في 10 جوان 1966.

2/ الأمر رقم 156/66 المؤرخ في 18 صفر عام 1386 الموافق ل 08/جوان 1966، المتضمن قانون العقوبات الجزائري، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 49، الصادر يوم 11 جوان 1966.

3/ الأمر رقم 11/21 المؤرخ في 25 أوت 2021، المعدل والمتمم لقانون الإجراءات الجزائية، الصادر في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية ، العدد 65 ، سنة 2021.

❖ **الكتب.**

01- أحمد بوسقيعة، الوجيزفي القانون الجزائي الخاص، الجزء الأول، الطبعة 11، دار هومه، الجزائر، سنة 2010.

02- شحادة يوسف، الضابطة العدلية، علاقتها بالقضاء ودورها في سير العدالة الجزائية، (دراسة مقارنة)، الطبعة الأولى، مؤسسة بوحسون للنشر والتوزيع، بيروت.

03- د/ محمد صالح بن عيسى، حرية الإثبات في المواد الجزائية، دار البعثة، قسنطينة، دار هومه، 2018.

04- د/ يعيش تمام الشوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، الطبعة الأولى، مطبعة الرمال، الوادي، الجزائر، جانفي 2019.

قائمة المصادر و المراجع

❖ **المذكرات والبحوث الجامعية.**

1- آيه بن ميسية، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة لنيل شهادة ماستر، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، 2025/2024.

2- بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراهفي العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو.

3- بن قويدر أمل، بوصبع عفاف، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة ماستر حقوق، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، 2025/2024.

4- حمبلي عمار، عثماني دليلة، جرائم تقنية المعلومات في ظل الإتفاقيات العربية 2010 وفي التشريع الجزائري، مذكرة لنيل شهادة الماستر حقوق، تخصص قانون جنائي وعلوم جنائية، جامعة قاصدي مرباح، ورقلة ، 2022/2021.

5- حنان حفصة، إجراءات البحث والتحري في جرائم المعلوماتية، مذكرة لنيل شهادة الماستر (ل.م.د)، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة، 2021/2020.

6- رابح عبد العالي، إشكالية الإختصاص القضائي في الجرائم المعلوماتية (دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراء، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2020/2019.

7- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراء في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016/2015.

8- رزيقة بونار، الجريمة المعلوماتية في التشريع الجنائي الجزائري، مذكرة لنيل شهادة ماستر في القانون العام، تخصص قانون عام داخلي، كلية الحقوق والعلوم السياسية، جامعة الصديق بن يحي- جيجل، 2021/2020.

9- عزة خولة، ربيع شيماء، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر أكاديمي في الحقوق، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة بشير الإبراهيمي، برج بوعريريج، 2024/2023.

10- عثماني رضوان، مكافحة الجرائم المعلوماتية في القانون الجزائري والدولي، أطروحة لنيل شهادة الدكتوراء في العلوم، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد، وهران، 2024/2023.

المقالات.

1- **د/** إلهام بن خليفة، التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنلوجيا الإعلام والإتصال، محاضرات لطلبة السنة الثانية ماسترحقوق، تخصص قانون جنائي، جامعة الشهيد حمة لخضر، الوادي.

2- حسين بن سعيد الغافري ، " التحقيق وجمع الأدلة في الج ا رئم المتعلقة بشبكة الإنترن ت"، ص 11

3- أ/ مشري سلمى، محاضرات مقياس الجريمة الإلكترونية، السنة الثانية ماستر، تخصص علوم جنائية.

4 - 12 ،مقال متوفر عبر الموقع التالي: http://www.eastlaws.com

❖ **المجلات العلمية والقانونية.**

01- بن طالب ليندا ، "التفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، عدد 16 ، جوان 2017

02- أحمد الزاوي، الجزائر واتفاقية بودابست للجرائم الإلكترونية، مجلة العلاقات الدولية، جامعة الجزائر3 ، العدد 11، 2019.

03- العربي قاسمي، التحديات العملية لقبول الدليل الإلكتروني في المحاكم الجزائرية، مجلة البحوث القانونية، جامعة الجزائر 1، العدد 2، 2021.

قائمة المصادر و المراجع

04- بلقاسم بوعمرة، شروط قبول الدليل الإلكتروني في الإجتهاد القضائي الجزائري، مجلة القضاء والقانون، العدد 25، 2020.

05- حبت أمال، الجريمة المعلوماتية في التشريع الجزائري بين قانوني 15/05 و 04/09، مجلة هيرودورت للعلوم الإنسانية والاجتماعية، جامعة مولود معمري، الجزائر، المجلد 7، العدد 25، سنة 2023، ص 53-68.

06- خضراوي الهادي، تجربة الجزائر في مكافحة الجريمة الإلكترونية، بحوث المؤتمرات، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية المتحدة، الرياض 2016، ص 173-152.

07- رابح مقدم، تطور التشريع الجنائي في مجال الأدلة الإلكترونية، مجلة القانون المقارن، جامعة الجزائر 2، العدد 14، 2018.

08- ربح وهيبة، "الجريمة المعلوماتية في التشريع الاجرائي الجزائري "، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم-السياسية، جامعة الحاج لخظر، باتنة 1، العدد الرابع، ديسمبر

09- رضا هميسي، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، عدد 05، جوان 2012.

10- رشيد بوبكر، حماية الأدلة الرقمية في التشريع الجزائري، مجلة الباحث في الحقوق، جامعة تيزي وزو، الجزائر، العدد 5، 2020.

11- زكرياء قاسمي، طعن المتهم في سلامة الدليل الإلكتروني، مجلة الحقوق، جامعة الجزائر 1، العدد 22، 2019.

12- سمير بارة، الأمن السيبراني في الجزائر، السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، المجلد3، العدد2، 2017، ص 260-262.

قائمة المصادر و المراجع

13- شريف خالد، الجرائم المتصلة بتكنلوجيا الإعلام والإتصال في التشريع الجزائري، مجلة البيبان، جامعة محمد خيضر بسكرة، الجزائر، المجلد 10، العدد 01، جوان 2025، ص 119-140.

14- عبد الحميد شريفي، معوقات قبول الدليل الإلكتروني في القضاء الجزائري، مجلة الدراسات القضائية، المعهد الوطني للقضاء، الجزائر، العدد 12، 2020.

15- عبد المجيد شني، سبل تطوير حجية الدليل الإلكتروني في الجزائر، مجلة الإصلاح القانوني، جامعة قسنطينة 1، العدد 5، 2020.

16- فاطمة الزهراء بن ساسي، الإندثار الرقمي كعائق أمام الأدلة الإلكترونية، مجلة القانون والأعمال، جامعة قسنطينة، العدد15، 2019.

17- فتيحة زروقي، القرائن الإلكترونية في القانون الجزائي الجزائري، مجلة الحقوق، جامعة ورقلة، العدد9، 2019.

18- فوزية براهيمي، ارتباط الدليل الإلكتروني بالواقعة، مجلة الدراسات القانونية، جامعة البليدة، العدد 13، 2019.

19- مصطفى بلقاسم، التشفير التقني بين حرية التعبير ومتطلبات الأمن القومي، مجلة الحقوق والعلوم السياسية، جامعة الجزائر 1، العدد 15، 2020.

20- معاش سميرة، الجرائم المعلوماتية (دراسة تحليلة لمفهوم الجرائم المعلوماتية)، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة/ الجزائر، مجلة الفكر، العدد 17، رقم الإيداع 2006/1257.

21- منى غازي حسام إبراهيم، فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية (دراسة مقارنة في ضوء متطلبات الأمن السيبراني)، مجلة الشريعة والقانون، القسم الجنائي، كلية شريعة وأنظمة، جامعة الطائف، المملكة العربية السعودية، العدد 45 ، ماي 2025.

22- نادية عبد الحفيظ، توثيق الأدلة الرقمية في التشريع الجزائري، مجلة العلوم القانونية، جامعة باتنة، العدد 10، 2020.

قائمة المصادر و المراجع

23- نوال دراجي، إشكالية الجرائم المعلوماتية، مجلة الدراسات القانونية، جامعة وهران، العدد8، 2018.

24- وهيبة رابح، الجريمة المعلوماتية في التشريع الجزائري، مجلة الباحث للدراسات الأكاديمية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، ديسمبر 2014، ص 320-331.

25- يخلف عبد القادر، المكافحة الموضوعية للجرائم الإلكترونية في القانون الجزائري، مجلة البحوث القانونية والإقتصادية، المجلد8، العدد3، 2025، ص 512-513.

26- توصيات الندوة الوطنية حول الجرائم المعلوماتية المنعقدة بالمعهد الوطني للقضاء، الجزائر، سنة 2019، منشورات المعهد الوطني للقضاء 2020.

27المواقع:

1/ التقرير السنوي لنشاط الأنتربول لسنة 2012، الموقع الرسمي للأنتربول، نسخة عربية،

www.interpol.int/content/downlood/20552/185417/5/annual20%report%202012-ARi.pdf.

الفهرس

فهرس المحتويات

خطـة البحث: **الصفحة**

فهرس المحتويات

الملخص:

تعتبر الجريمة المعلوماتية من أخطر الجرائم التي شهدها العصر الحديث، وذلك لمواكبتها حركة التطور في شتى المجالات العلمية والتكنولوجية، وهذه الجريمة هي جريمة عابرة للحدود الوطنية أي أنها جريمة ذات طابع دولي لها انعكاسات سلبية على شتى المستويات.

و قد أدى ظهور هذا النوع من الجرائم إلى خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول وخاصة في مواجهة قانون العقوبات الأمر الذي أدى إلى البحث فيما إذا كانت النصوص القائمة كافية لمواجهة هذه الجرائم بشتى أنواعها أم أن الأمر يستدعي استحداث قوانين أو نصوص خاصة قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها.

لذلك كان لزاما أن تتصدى الجزائر و معظم دول العالم من خلال القوانين الداخلية وعلى رأسها قانون العقوبات، و من خلال الاتفاقيات الدولية والإقليمية والهيئات الخاصة لمكافحة هذه الظاهرة، وذلك من خلال وضع إستراتيجية شاملة لكبح هذه الجريمة.

الكلمات المفتاحية : الجريمة المعلوماتية الفضاء الإلكتروني، جرائم عابرة للحدود الأنظمة المعالجة الآلية للمعطيات العقوبة قانون جزائري.

Abstract:

Cyber crimes Is one of the mostdangerous crimes nowadays. This kind of crimes is beyond frontiers and has a lot of negative impacts on different fields.

This kind of crime pushed the legal system to create new challenges especially with penal.

Experts made deep researches on law texts to know if they are enough to face this kind of crimes, or if new and more specific law texts are needed to be created.

Therefore, Algeria must face these crimes, also as other countries, with creating a general strategy to brake these crimes.

Key words: cyber crime, internet network, trans-frontiers crimes automated data processing systems, punishment, Algerian law.