جامعة بلحاج بوشعيب عين تموشنت

كلية الحقوق

قسم: الحقوق

الجرائم السيبيرانية وآليات مكافحتها

مذكرة مكملة لنيل شهادة الماستر في الحقوق –تخصص: قانون عام

من إعداد الطالبتين:

- شيبان دعاء رابحة
- شيخي ابتسام

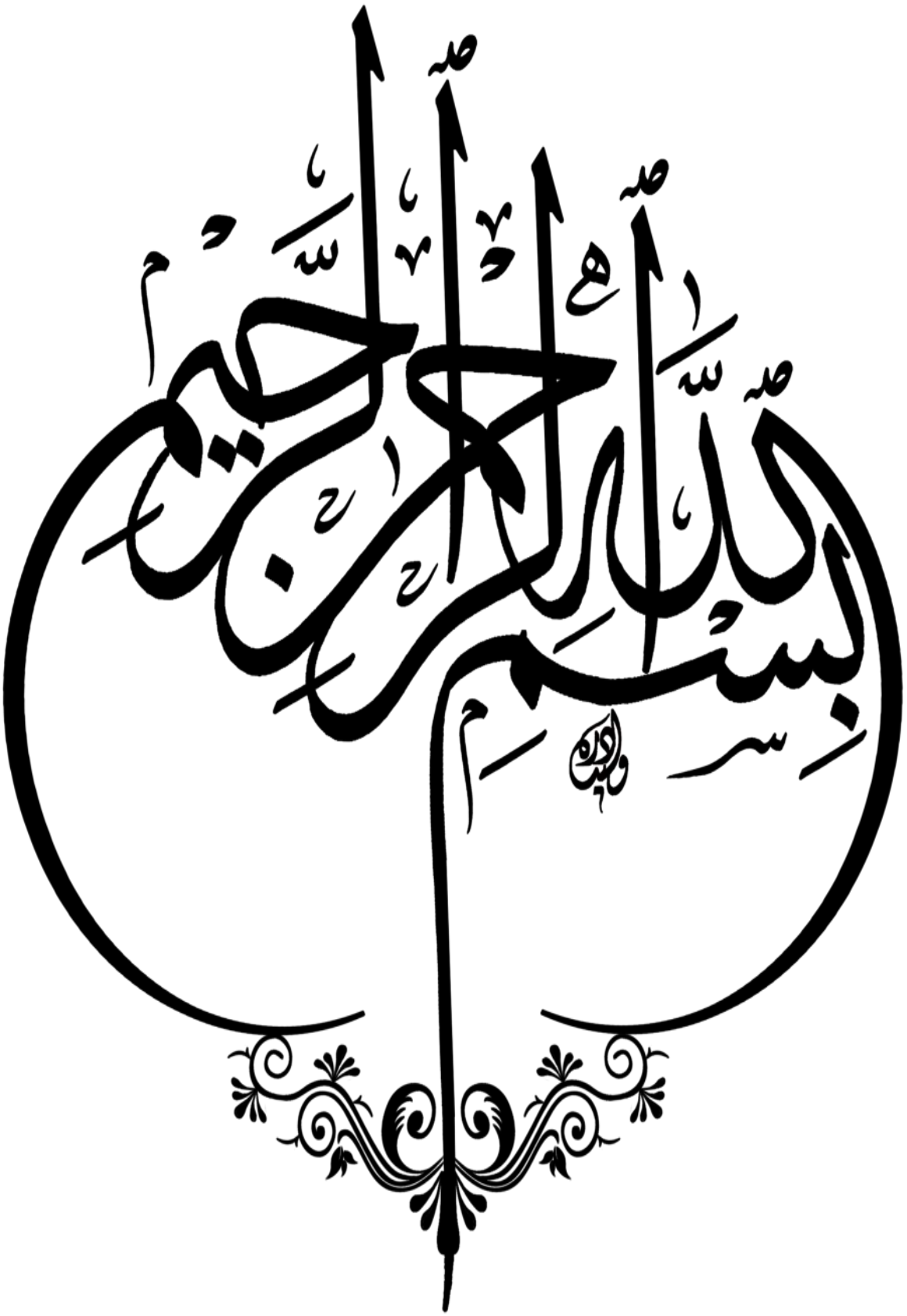
تحت إشراف الدكتور:

– فوحال رياض

لجنة المناقشة:

الرئيس	أ– جغدم بن ذهيبة	أستاذ محاضر –ب–	جامعة عين تموشنت
المشرف	أ–فوحال رياض	أستاذ محاضر – ب –	جامعة عين تموشنت
الممتحن	أ– بوعبسة محمد	أستاذ محاضر –ب–	جامعة عين تموشنت

السنة الجامعية: 2024–2025


بسم الله الرحمن الرحيم

شكر وعرفان

الحمد لله الذي بنعمته تتم الصالحات و بفضله تشرق شموس العلم و المعرفة ، و بتوفيقه تثمر الجهود و تتكلل المساعي بالنجاح ، الحمد لله عدد ما خط القلم ، و عدد ما جاد الفكر ، وعدد ما ترددت أصداء العلم في أروقة الزمن.

ونحمد الله عز وجل الذي اعاننا وثبتنا لإتمام هذا البحث المتواضع حمدا يليق بجلال وجهه وعظيم سلطانه والصلاة والسلام على اشرف المرسلين سيدنا محمد عليه افضل الصلاة و السلام.

ان هذا العمل بكل ما حواه من جهد ، و بكل ما تطلبه من صبر ، لم يكن ليرى النور لولا فضل الله وتوفيقه ، ثم عطاء نفوس كريمة بذلت و أعطت و امنت بان للعلم رسالة ، و للمعرفة قيمة لا تضاهيها كنوز الأرض

و ان اول ما يفرضه الوفاء " ان نجزي وافر الشكر والامتنان للأستاذ "**فوحال رياض**" الذي رافقنا طيلة انجازنا لهذا العمل وللرعاية الفائقة التي خصصها لنا و توجيهه العليم فضله كبير علينا نسال الله ان يحفظه بما يحفظ به عباده الصالحين.

و لا يفوتنا أن نتقدم باسمي آيات الشكر والاحترام الى اساتذتنا الاجلاء، أوليك الذين حملوا على عاتقهم مسؤولية العلم و زرعوا فينا شغف البحث و المعرفة.

وختاما نسال الله العظيم ان يجعل هذا العمل نافعا و ان يكون لبنة تضاف الى صرح العلم فأن اصبنا فذلك بفضل الله و منه و ان اخطانا فحسب الانسان انه سعى و اجتهد و الله ولي التوفيق و هو نعم المولى ونعم النصير.

إهـداء

بسم الله الرحمن الرحيم

قال تعالى (يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات)

الى الغائب و الحاضر في قلبي كل حين من حصد الأشواك عن طريقي ليمهد لي دروب العلم بكل حب ووفاء من علمني ان العلم لا يأتي إلا بالصبر والاصرار من مسك بيدي في أول الطريق وها أنا اليوم اصل الى نهايته دون يديه رحمك الله يا ابي لتنم قرير العين و تفاخر بابنتك عند أهل السماء كان شرفي الاول حمل اسمك ...

إلى من جعل الله الجنة تحت أقدامها إلى اليد الخفية و القلب الحنون من سهرت و ساندت وكافحت دوما إلى نبراس ايامي ووهج حياتي امي الغالية

إلى ضلعي الثابت و امان ايامي إلى من شددت عضدي بهم فكانوا ينابيع ارتوي منها اخوتي رفقاء حياتي

الى من كانوا لي عونا و سندا من امدوني بالقوة و آمنوا بي زوجي رفيق دربي و عائلتي الثانية

الى كل من سعى معي لاتمام هذه المسيرة لكل من كانت كلماتهم دافعا يمضي بي نحو الأمام ما كان لهذا الجهد أن يكتمل لولا توجيهكم و ارشادكم أساتذتي الكرام

فالحمد لله أولا وأخرا، ظاهرا وباطنا، على ما وهبني من صبر وقوة وتوفيق لإتمام هذا العمل. فلولاه ما كان للجهد تمرة، ولا للطريق نهاية. إليه وحده ترفع الأكف شكرا، وبه استعين في كل خطوة قادمة

.دعاء

إهـداء

إلى من كان لهم الفضل بعد الله تعالى في مسيرتي العلمية،

.إلى والديّ الكريمين، رمز التضحية والعطاء، لما قدّماه لي من دعم متواصل ودعاء صادق

إلى أساتذتي الأفاضل، الذين لم يبخلوا بعلمهم وتوجيهاتهم النيرة،

.إلى كل من ساندني خلال رحلتي العلمية، من أهل وأصدقاء وزملاء

أهدي هذا العمل المتواضع، تعبيرًا عن شكري وامتناني لكل من كان له دور في تحقيق هذا الإنجاز.

وإلى روح فقدتها ولا تزال ترافقني في كل خطواتي أخي فؤاد رحمه الله

ابتسام

قائمة المختصرات

ج: جزء

ط: طبعة

ع : عدد

د.د.ن : دون دار النشر

د.س.ن : دون سنة النشر

ج . ر : الجريدة الرسمية

مقدمة

مقدمة

شهد العالم في العقود الأخيرة تحولًا جذريًا غير مسبوق بفعل الثورة الرقمية، التي فرضت نفسها على مختلف جوانب الحياة الإنسانية، وأعادت تشكيل أساليب العيش والتفاعل على كافة المستويات. فقد أصبحت تكنولوجيا المعلومات والاتصالات في صميم المنظومات الاقتصادية والاجتماعية والسياسية والثقافية، محدثة بذلك نقلة نوعية في طرق التواصل، وإدارة المعلومات، وتنظيم العمل، وتقديم الخدمات، واتخاذ القرار، بل وحتى في طرق ارتكاب الجرائم ومكافحتها.

وقد فرض هذا التحول الرقمي واقعًا جديدًا، يتميز بالسرعة والتعقيد، وغيّر من طبيعة التحديات التي تواجهها المجتمعات الحديثة. فمن جهة، وفرت الرقمنة إمكانيات هائلة لتعزيز الكفاءة والشفافية والإنتاجية، ومن جهة أخرى فتحت المجال أمام بروز أشكال مستحدثة من التهديدات، كان من أبرزها تنامي الجرائم ذات الطابع السيبراني، والتي تختلف في طبيعتها وخصائصها عن الجرائم التقليدية.

وفي خضم هذا المشهد، يبرز موضوع الجريمة باعتباره أحد أكثر المواضيع إلحاحًا في السياق الرقمي، لما له من انعكاسات خطيرة على أمن الأفراد واستقرار المجتمعات وسلامة المؤسسات. فالجريمة، في جوهرها، تمثل سلوكًا اجتماعيًا منحرفًا ينطوي على خرق للقانون وانتهاك للحقوق، وهي قديمة قدم الوجود الإنساني، إلا أنها لم تكن يومًا ظاهرة جامدة، بل كانت دومًا في حالة تطور وتغير، بتغير المجتمعات والبيئات والوسائل والدوافع. ومع تطور المجتمعات الحديثة وتعقّد بنيتها، لم تعد الجرائم محصورة في الأشكال التقليدية مثل القتل والسرقة والاعتداء، بل ظهرت أنماط جديدة تعكس طبيعة العصر الرقمي، وفي مقدمتها الجرائم السيبرانية، التي تُعد من أخطر مظاهر الجريمة المعاصرة.

فهذه الجرائم لا تُرتكب في الواقع المادي المعروف، وإنما تتم في فضاء افتراضي غير مرئي، يتجاوز الحدود الجغرافية ويخضع لمنطق خاص به، مما يصعّب عمليات المتابعة والملاحقة، ويجعل الجريمة السيبرانية ذات طابع عالمي عابر للحدود. وتتسم هذه الجرائم بخصائص فريدة، تجعل منها تحديًا كبيرًا للأجهزة الأمنية والقانونية، فهي غالبًا ما تُدار عن بُعد، وتُستخدم فيها أدوات تكنولوجية متقدمة، وتستهدف قواعد البيانات، والحسابات البنكية، والمعلومات الحساسة، والبنى التحتية الرقمية للمؤسسات والدول.

كما أن مرتكبيها قد يكونون أفرادًا منفردين، أو مجموعات منظمة، أو حتى جهات ذات طابع استخباراتي، ما يزيد من تعقيد الظاهرة وخطورتها، وأمام هذا المشهد المعقّد وجدت الدول نفسها أمام واقع قانوني وأمني جديد، يفرض عليها ضرورة إعادة النظر في منظومتها القانونية، وتكييف قوانينها مع طبيعة هذه التهديدات الرقمية المستحدثة، إلى جانب تطوير قدراتها التقنية، وتعزيز الأمن السيبراني، وتكثيف التعاون الدولي في مجال تبادل المعلومات، والتنسيق الأمني، والتدريب، وتوحيد الجهود لمجابهة هذا التحدي المتنامي.

وفي هذا السياق، تُعد الجزائر من الدول التي بدأت تتلمس طريقها نحو مواجهة هذا النوع من الإجرام، سواء من خلال تطوير الإطار التشريعي الذي يجرم الاعتداءات على نظم المعلومات، أو عبر إنشاء خلايا أمنية مختصة بمكافحة الجرائم الإلكترونية، أو من خلال الانخراط في بعض المبادرات الدولية الرامية إلى التصدي للجرائم السيبرانية. غير أن هذه الجهود، وعلى أهميتها، تطرح تساؤلات حقيقية حول مدى فعاليتها، ودرجة جاهزية المنظومة الوطنية لمواجهة التحديات المتزايدة في هذا المجال.

ومن هذا المنطلق، جاءت هذه الدراسة لتحليل ظاهرة الجريمة السيبرانية من الزاوية القانونية والعملية، وتسليط الضوء على الإشكاليات المرتبطة بها، سواء من حيث مفهومها وخصائصها وتمظهراتها، أو من حيث سبل مواجهتها تشريعيًا ومؤسساتيًا. كما تهدف الدراسة إلى الوقوف على الجهود الجزائرية المبذولة في هذا المضمار، وتقييم مدى كفاءتها في ظل المعطيات الرقمية الراهنة، مع تقديم مجموعة من المقترحات التي من شأنها المساهمة في تعزيز الحماية القانونية والأمنية للفضاء السيبراني الوطني. وعليه، ومن خلال ما سبق، نطرح الإشكالية الآتية:

ما مدى فاعلية التشريعات الوطنية والدولية في مكافحة الجرائم السبيرانية ؟

و منه تتفرع الأسئلة الفرعية التالية:

1. ما هي الجريمة الالكترونية و ماهي اهم خصائصها؟
2. ما هي أنواعها الأساسية ؟ و ما هي أركانها؟
3. ماهي اهم القوانين الوطنية والدولية في مجال مكافحة الجرائم السيبيرانية ؟
4. ماهي اهم السبل لمكافحة هذا النوع من الجريمة؟

أهمية الدراسة:

تتمثل أهمية الدراسة في:

- **من الناحية النظرية:** تكتسي هذه الدراسة أهمية بالغة كونها تسهم في إثراء الأدبيات القانونية حول مفهوم الجريمة السيبرانية باعتبارها ظاهرة مستحدثة ومعقدة. كما تساهم في توضيح الإطار المفاهيمي والقانوني المرتبط بها، مما يفتح المجال أمام دراسات أكاديمية مستقبلية لفهم أعمق لأبعادها وتطوراتها في ظل البيئة الرقمية المتغيرة.
- **من الناحية العملية** : تنبع أهمية هذه الدراسة من التهديد المتزايد للجرائم الإلكترونية على الأمن القومي والمجتمعي والاقتصادي، وتبرز الحاجة إلى تقييم واقعي للجهود المبذولة على المستويين الوطني والدولي، مما يساهم في تعزيز آليات المواجهة القانونية والتقنية لهذا الخطر الرقمي المتنامي.

اهداف الدراسة:

أما في ما يخص أهداف الدراسة فهي كالتالي:

- تسليط الضوء على مفهوم الجريمة السبيرانية وخصائصها وأشكالها المختلفة.
- تحليل الإطار القانوني الوطني لمكافحة الجرائم الإلكترونية في الجزائر.
- تقييم الجهود والاتفاقيات الدولية الموجهة لمكافحة الإجرام السيبراني.
- إبراز النقائص والتحديات التي تواجه مكافحة الجريمة الإلكترونية واقتراح حلول عملية.

الدراسات السابقة:

و نظرا لحداثة الموضوع اعتمدنا على العديد من الدراسات الاكاديمية التي كانت لنا مرجعا و نذكر منا ما يلي:

- شنتير خضرة، "الآليات القانونية لمكافحة الجريمة الإلكترونية: دراسة مقارنة"، أطروحة دكتوراه، جامعة أحمد دراية – أدرار، 2021.
- براهيمي جمال، "التحقيق الجنائي في الجرائم الإلكترونية"، أطروحة دكتوراه، جامعة مولود معمري – تيزي وزو، 2018.

- مولاي ملياني دلال، "إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري"، أطروحة دكتوراه، جامعة أبي بكر بلقايد – تلمسان، 2018.

أسباب اختيار الموضوع :

ومن الأسباب التي دفعتنا الى اختيار هذا الموضوع في كالتالي:

- حداثة الموضوع وأهميته المتزايدة في ظل الاعتماد الواسع على التكنولوجيا.
- الحاجة الأكاديمية إلى إثراء البحث القانوني المتعلق بالجريمة الإلكترونية.
- رغبة الباحث في المساهمة في تطوير فهم أعمق لمجال الأمن السيبراني ومكافحة الجريمة الرقمية.

صعوبات الدراسة:

اما صعوبات التي واجهتنا خلال الدراسة:

- قلة المراجع والدراسات المتخصصة باللغة العربية حول الموضوع نظرا لحداثته.
- صعوبة الإحاطة بجميع الأطر القانونية الدولية المختلفة والمتغيرة باستمرار.
- الطبيعة التقنية للموضوع، والتي تفرض الحاجة لفهم جوانب معلوماتية وأمنية معقدة.

منهج الدراسة:

اما بالنسبة لمنهج الدراسة ونظرا للمعلومات اتبعنا الدراسة المنهج الوصفي التحليلي، من خلال استعراض وتحليل النصوص القانونية الوطنية والدولية المتعلقة بالجرائم الإلكترونية، بالإضافة إلى المنهج المقارن عند دراسة جهود الدول والمنظمات الدولية في التصدي لهذه الجرائم.

اما عن الخطة فهي كالتالي :

الفصل الأول : الاطار المفاهيمي للجرائم السيبيرانية

- المبحث الأول: ماهية الجرائم السيبرانية
- المبحث الثاني: مجال ونطاق الامن السيبيراني

الفصل الثاني : جهود القوانين المقارنة في مكافحة الجرائم السيبرانية

- المبحث الأول: آليات مكافحة الجرائم السيبرانية في التشريع الجزائري
- المبحث الثاني: جهود القوانين المقارنة في مكافحة الجرائم السيبرانية

الفصل الأول

الاطار المفاهيمي للجرائم السيبيرانية

الفصل الأول: الاطار المفاهيمي للجرائم السيبيرانية

أصبحت الجرائم السيبرانية تمثل أحد أخطر التحديات التي تواجه النظم القانونية الحديثة، خاصة مع التوسع الهائل في استخدام تكنولوجيا المعلومات والاتصال. فالتطور الرقمي، رغم ما يتيحه من مزايا وخدمات، أفرز أشكالًا جديدة من السلوك الإجرامي تختلف في طبيعتها ووسائل ارتكابها عن الجرائم التقليدية. هذا الواقع فرض على المشرع ضرورة التكيف مع هذا السلوك المستجدة، من خلال تبني مقاربة قانونية تواكب التحولات التكنولوجية المتسارعة. وفي الجزائر، برزت الحاجة الملحة إلى إيجاد إطار قانوني ينظم هذا النوع من الجرائم ويضبط آليات مكافحتها. وعليه، يهدف هذا الفصل إلى تقديم أرضية مفاهيمية أساسية تُمكن من فهم الجرائم السيبرانية من الزاوية القانونية، من خلال تسليط الضوء على خصائصها العامة، وتمييزها عن الجرائم التقليدية، واستعراض الأسس التي بني عليها التجريم في التشريع الجزائري.و عليه تم تقسيم هذا الفصل الى :

المبحث الأول: ماهية الجرائم السيبرانية

المبحث الثاني: مجال ونطاق الأمن السيبيراني

المبحث الأول:

ماهية الجرائم السيبرانية

أصبحت الجرائم السيبرانية من أبرز التحديات التي فرضها العصر الرقمي، نظراً لارتباطها الوثيق بالتطور التكنولوجي السريع وتأثيرها العميق على الأفراد والمؤسسات. وتتميز هذه الجرائم بطبيعة وأساليب تختلف عن الجرائم التقليدية، ما يستدعي فهماً قانونياً دقيقاً لها. وعليه، يتناول هذا المبحث الإطار العام للجرائم السيبرانية، من خلال المطلب الأول الذي يعرّف بها، والمطلب الثاني الذي يسلط الضوء على خصائصها وطبيعتها القانونية.

المطلب الاول:

مفهوم الجرائم السيبرانية

أدى الانتشار المتسارع للتكنولوجيا الرقمية إلى بروز أنماط جديدة من السلوك الإجرامي ترتبط بالفضاء السيبراني، ما استدعى إعادة النظر في المفاهيم التقليدية للجريمة. ويأتي هذا المطلب لتسليط الضوء على الإطار العام لمفهوم الجرائم السيبرانية، بما يعكس طبيعتها الخاصة والتطورات التي فرضتها على المنظومة القانونية. و عليه سوف نتطرق في هذا المطلب الى فرعين :

الفرع الأول :

تعريف الجرائم السيبرانية

تُعد الجريمة المعلوماتية من الظواهر الإجرامية التي شهدت تطورًا ملحوظًا في تسمياتها عبر مراحل ارتبطت بتطور تكنولوجيا المعلومات[1]. فقد أُطلق عليها في بداياتها مصطلحات متعددة تعكس طبيعة المرحلة التقنية، مثل: "إساءة استخدام الحاسوب"، و"احتيال الكمبيوتر"، ثم "الجريمة المعلوماتية"، و"جرائم الكمبيوتر"، و"جرائم التقنية العالية"، و"جرائم الهاكرز"، و"جرائم الإنترنت"، إلى أن استقرّت في الآونة الأخيرة على تسمية "الجرائم السيبرانية.(Cybercrime) "

وقد وُصفت هذه الجريمة بأنها عصية على التحديد، نظرًا لتعدد الزوايا التي تناولتها الدراسات والبحوث، فبعضها ركز على وسيلة ارتكابها، وبعضها الآخر على موضوعها، في حين اختارت فئة ثالثة الربط بينها وبين مستوى المعرفة بتقنية المعلومات.

[1]–عمر بن محمد العتيبي، الامن المعلوماتي في المواقع الالكترونية و مدى توافقه مع المعايير المحلية و الدولية، أطروحة دكتوراه ، جامعة نايف للعلوم الأمنية ، كلية الدراسات العليا، 2010،ص15.

وفي هذا الإطار، يُعرفها مكتب تقييم التقنية الأمريكي بأنها" :كل جريمة تلعب فيها البيانات الرقمية أو البرامج المعلوماتية دورًا رئيسيًا، أو كل فعل إجرامي متعمد له صلة مباشرة أو غير مباشرة بالمعلوماتية، يُلحق خسارة بالمجني عليه أو يُحقق كسبًا غير مشروع للجاني." [1]

وقد تبنى العديد من الفقهاء التعريف الصادر عن منظمة التعاون الاقتصادي والتنمية (OCDE) خلال اجتماعها في باريس عام 1983، والذي ينص على أن الجريمة المعلوماتية هي" :كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بمعالجة البيانات أو نقلها إلكترونيًا." [2]

أولا: الجريمة السيبرانية لغة :

سوف نتحدث عن الجريمة السيبيرانية لغة و اصطلاحا ث نتطرق الى مفهوم الجريمة السبيرانية في القانون.

السيبرانية كلمة إنجليزية مشتقة من كلمة (Cyber) وتعني : مرتبط بالحاسوب أو شبكات الحاسوب، وقيل تعني : قضاء الانترنت، وقيل : كلمة يونانية مشتقة من كلمة (Kybernetes)وتعني : الشخص الذي يدير دفة السفينة، مجازاً للمتحكم. [3]

كما يمكن أن نعرف الجريمة بأنها كل سلوك أو نشاط أو فعل مخالف للقيم والقواعد العامة السائدة ومعايير المجتمع والصادر من الإنسان مقصوداً أو تحت تأثير عامل معين والذي يحدث الضرر بالفرد ومؤسسات المجتمع والبناء الاجتماعي من جهة والذي يؤدي الى خلق نوع من الاضطرابات السلوكية ونشر الذعر والقلق والخوف بين أفراد المجتمع من جهة أخرى .[4]

ثانيا: تعريف الجريمة السيبرانية (الإلكترونية) فقها وقانوناً :

1-التعريف الفقهي : انقسم الفقه إلى عدة آراء منهم من ضيق من مفهوم الجريمة الإلكترونية ومنهم من وسع من مفهومها الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية، يذهب أنصار هذا الاتجاه إلى حصر

[1]-باخد نعيمة، الطيبي أمنة، دور العلام الرقمي في الحد من الجرائم السيبيرانية موقعي "الشروق" و "أخبار الوطن" اونلاين أنموذجا، مذكرة ماستر في علوم الاعلام و الاتصال تخصص صحافة مطبوعة الكترونية، جامعة احمد درايعية ، ادرار، الجزائر،2022-2023،ص36.

[2]-عائشة عبد الحميد، ملوك نوال الإجرام السيبراني وأثره على تهديد الأمن الثقافي في الجزائر" ، مجلة المفكر للدراسات القانونية والسياسية، المجلد 3، العدد 3، سبتمبر 2020 ، ص 216.

[3]-عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية : دراسة تأصيلية مقارنة ، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03،المملكة العربية السعودية، السعودية ،2020 ،ص 148.

[4]-نوري ياسين هرزاني، الإعلام والجريمة، مطبعة جامعة صلاح الدين، أربيل ، 2005، ص 29.

الجريمة الإلكترونية في الحالات التي تتطلب قدراً كبيرا من المعرفة التقنية في ارتكابها، ومن التعريفات إلى وضعها أنصار هذا الاتجاه أن الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى .

و يعتبر مصطلح الجرائم السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات .

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تتم الجريمة الإلكترونية وكما يقول فان دير هلست و ونيف هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف .

ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية كما تعرف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال . [1]

كما يعرف بعض الفقهاء مصطلح السيبرانية بأنها "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنى تحتية محمية الكترونيا لتعطيلها أو تدميرها أو الإضرار بها" ويعرفه آخرون بأنها "هجوم عبر الانترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها" كما تم تعريف مصطلح السيبرانية في ورشة عمل بعنوان "الأمن" الرقمي وحماية المستخدم من مخاطر الانترنت والذي نفذته هيئة الاتصالات وتقنية المعلومات المنعقد بتاريخ (26/04/2018) "بأنها مأخوذة من كلمة (سيبر)Cyber ، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي ، فالسيبرانية تعني : (فضاء الانترنت).

ويعرف أيضا بأنه "المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم ويشمل ذلك الأجهزة الالكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية الفضاء السيبراني ليس الإنترنت وإنما شبكات أخرى كثيرة متصلة مثل : gos/pstn/Gsm/Swift/Acars أما تعريف مصطلح الجريمة السيبرانية "هو السلوك غير المشروع أو المنافي للأخلاق أو غير المسموحبه المرتبط بالشبكات المعلوماتية العالمية .

[1]–راضية حميدة، الجريمة الإلكترونية غير مواقع التواصل الاجتماعي نحو تفعيل دور الأمن السيبراني المعلوماتي"، مجلة الإعلام والمجتمع، المجلد 05، العدد 02، ديسمبر 2021 ص 341.

ويعرف مايكل أرون دينس الجريمة السيبرانية بأنها هي جرائم سيبرانية، والتي أيضا جرائم الكمبيوتر ويتم استخدام الحاسب الآلي والانترنت فيها كأداة لتحقيق أهداف غير قانونية، مثل ارتكاب الاحتيال، والاتجار في المواد الإباحية للأطفال والملكية الفكرية، وسرقة الهويات، أو انتهاك الخصوصية .. " [1]

ويعرفها الفقيه (merwe) أنها كل فعل غير مشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية. [2]

لقد اختلفت تعريفات المصطلح الجريمة السيبرانية، مما يصعب معه تقرير بإمكان إيجاد تعريف موحد باعتبار أن هذه الظاهرة حديثة نسبياً مما يخشى حصرها في نطاق واحد وبالتالي يصعب وضع تعريف جامع مانع للجريمة السيبرانية إذ أنها كما قبل تقاوم التعريف ولا يوجد لديها تعريف متفق 3 عليه للدلالة عليها .[3]

كما أن تعدد المصطلحات المستخدمة للتعبير عن هذه الجرائم يعد دليلاً على مدى أهمية هذا الموضوع [4]، وعليه للجريمة السيبرانية مسميات عدة منها :

- جرائم الحاسوب والأنترنت .
- جرائم التقنية العالية .
- الجريمة الإلكترونية.
- جرائم أصحاب الياقات البيضاء.[5]

[1]–زياد بن محمد عادي العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدوافع من ارتكابها المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 3، العدد 1، 2020، ص 4

[2]– عبد العال الديربي، محمد صادق اسماعيل الجرائم الإلكترونية (دراسة قانونية قضائية مقارنة)، المركز القومي للإصدارات القانونية، ط 1 ، القاهرة ، 2012، ص 40.

[3]– محمد عبيد الكعبي الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية، القاهرة، 2009، ص 34

[4]– أيمن عبد الله فكري، الجرائم المعلوماتية (دراسة مقارنة في التشريعات العربية والاجنبية)، مكتبة القانون والاقتصاد، ط 1 ، الرياض، 2014، ص 84.

[5]– سراء جبريل رشاد مرعي،"الجرائم الإلكترونية(الأهداف– الأسباب–طرق الجريمة ومعالجتها)"،مجلة الدراسات الإعلامية، المركز الديمقراطي العربي،العدد،1يناير 2018 ،ص427.

ثالثا: التعريف القانوني للجرائم السيبرانية

أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة للتكنولوجيات الإعلام والاتصال فإنه يعرفها بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية... " [1]

وتعرف الجريمة عموماً في نطاق القانون الجنائي بأنها فعل غير مشروع صادر عن ارادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً . [2]

عند الرجوع إلى التشريع الجزائري، يُلاحظ أنه لم يعتمد مصطلحًا موحدًا ودائمًا للإشارة إلى هذا النوع من الجرائم، بل استخدم تسميات مختلفة عبر النصوص القانونية المتعاقبة. ففي القانون رقم 04-15 المعدل والمتمم لقانون العقوبات، أُشير إليها تحت تسمية "جرائم المساس بأنظمة المعالجة الآلية للمعطيات[3] ."ولاحقًا، بموجب القانون رقم 04-09 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، تم اعتماد مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[4]."

وقد عرّف هذا الأخير تلك الجرائم بأنها تشمل" :جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما هو محدد في قانون العقوبات، إضافة إلى كل جريمة يتم ارتكابها أو تسهيل ارتكابها بواسطة منظومة معلوماتية أو نظم الاتصالات الإلكترونية"، وذلك وفقًا لما ورد في المادة الأولى من القانون رقم 04-09 المتضمن الأحكام الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[5].

وخلافا للمشرع الفرنسي الذي لم يعط تعريفا للجريمة السيبرانية، فإن المشرع الجزائري قد اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب الفقرة (أ) المادة 02 من القانون

---

[1]– محمد بوعمرة، سيد على بينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية ، جامعة أكلى محمد أولحاج البويرة 2019/2020 ، ص 5-4.

[2]– الحمد نصر محمد الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، ط 1 ، مصر ، 2015، ص 15.

[3]القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 يعدل و يتمم الامر رقم 66-155 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، المؤرخة في 10 نوفمبر 2004.

[4]– مهدي رضا، الجرائم السيبيرانية و آاليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد 06، العدد 02، جامعة محمد بوضياف، المسيلة، الجزائر،2021،ص113.

[5]القانون رقم 04-09 المؤرخ في 05-08-2009، يتضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية ، العدد 47، الصادرة في 16-08-2009.

09/04 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ". [1]

الملاحظ على تعريف المشرع الجزائري أنه قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة السيبرانية، أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكتروني، وثانيها معيار موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار ا[2]لقانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات .

كما اعتمد المشرع على معيار رابع لتحديد نطاق الجريمة الإلكترونية، حيث نص على أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا من شأنه أن يوسع من دائرة التجريم في مجال الإجرام السيبراني في القانون الجزائري.[3]

الفرع الثاني:

الدوافع الإجرامية وسمات الجاني في الجرائم السيبرانية واصنافه

تُعدّ الجرائم السيبرانية من الظواهر الإجرامية الحديثة التي ارتبطت بتطور تكنولوجيا المعلومات والاتصال، ما يجعل فهم دوافع مرتكبيها وخصائصهم مسألة أساسية في مواجهتها. إذ تختلف دوافع الجناة في هذا النوع من الجرائم بين أغراض مالية، نفسية، أو حتى أيديولوجية. كما يتميّز المجرم السيبراني بخصائص سلوكية ومعرفية تجعله يختلف عن المجرم التقليدي، و هو ما سنوضحه في الاتي.

أولا : الدوافع الباعثة على ارتكاب الجريمة السيبرانية

يشير كلّ من "الدافع"، و"الباعث"، و"الغاية" إلى مفاهيم دقيقة في نطاق القانون الجنائي، ترتبط بما يُعرف بالقصد الخاص في الجريمة، أي النية المحددة التي تدفع الجاني إلى ارتكاب فعله الإجرامي. وتتميّز الجريمة السيبرانية بتعدد الدوافع التي تحرّك الجناة، والتي قد تكون شخصية، أو خارجية، أو مرتبطة ببيئة

[1] المادة 02 من القانون رقم 04-09، السالف الذكر.

[2]العيد شعثان، مسعود موفقي،الجرائم السيبيرانية في القانون الجزائري،مذكرة ماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية، جامعة زيان عاشور، الجلفة، الجزائر، 2021-2022،ص14.

[3]رحيمة نميلي، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مداخلة في المؤتمر الدولي ،14 طرابلس،عنوان الجرائم الالكترونية طرابلس، يومي 24و 25 مارس ،2017 ص05.

العمل. وتُظهر هذه الدوافع تداخلاً بين الرغبة الذاتية في الإضرار، والطموح لتحقيق مكاسب، أو حتى الرغبة في إثبات الذات[1].

1- الدوافع الشخصية

تنقسم الدوافع الشخصية إلى نوعين رئيسيين :دوافع مالية وأخرى ذهنية أو نمطية.

- أ. **الدوافع المالية:** يُعدّ السعي نحو تحقيق الكسب المادي من أقوى المحركات التي تدفع الأفراد لارتكاب الجرائم السيبرانية. وتُظهر خصائص هذه الجرائم إمكانية تحقيق أرباح ضخمة بوسائل غير تقليدية، كما هو الحال في عمليات الاحتيال أو غشّ المعالجة الآلية للمعلومات. ومثال ذلك ما حدث في فرنسا سنة 1986، حيث فاقت مكاسب جريمة غش إلكتروني واحد ما يربو عن 670,000 فرنك فرنسي، مقارنة بـ 70,000 فرنك فقط لجريمة سرقة تقليدية. وتشير تقارير المركز الوطني للاحتيال المعلوماتي بالولايات المتحدة (N.F.I.C) إلى أن الدافع المالي يظل الأكثر شيوعًا في هذا المجال[2].
- ب. **الدوافع الذهنية أو النمطية:** هناك فئة من الجناة يكون دافعها إثبات التفوّق على الأنظمة المعلوماتية، دون وجود نية صريحة للإضرار أو تحقيق ربح. هؤلاء يسعون لاختراق النظم من باب التحدّي الشخصي، وهو ما يتجسّد غالبًا في نشاطات قراصنة الأنظمة(Hackers) ، خاصة ما يُعرف بالمتطفلين الداخليين. ومع ذلك، تُظهر الإحصائيات أن الدافع المالي لا يزال يتفوّق من حيث الانتشار[3].

2- الدوافع الخارجية

تؤثر العوامل البيئية والاجتماعية والمهنية بشكل مباشر في تحفيز السلوك الإجرامي السيبراني، خاصة حين تتلاقى مع بيئة العمل الرقمي.

- أ. **دافع الانتقام:** يظهر هذا الدافع عندما يسعى الموظف أو العامل السابق إلى إلحاق الضرر برب العمل، كما حدث في إحدى الحالات حين قام محاسب بالتلاعب بالبرمجيات، لتدمير بيانات مؤسسة

[1]-بوديسة بجاد عبد الرؤوف ، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر في الحقوق تخصص قانون الاعلام الآلي والانترنيت، جامعة محمد البشير الابراهيمي، برج بوعريريج، الجزائر، 2021-2022،ص22.

[2]-داودي خالد ، الجريمة الالكترونية ، دار الاعصر للنشر والتوزيع، عمان، 2011، ص37-38.

[3]-احمد خليفة ملط، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص89-90.

بعد تركه العمل. وتُعتبر عمليات زرع الفيروسات أو حذف قواعد البيانات من أبرز صور هذه الجرائم[1].

- **ب. الرغبة في قهر النظام وإثبات التفوق:** يحاول بعض الأفراد، خصوصًا من فئة الشباب، إثبات قدراتهم التقنية عن طريق اختراق الأنظمة. وقد تستغل بعض الجماعات المنظمة هذا الميل لتجنيد هؤلاء الأفراد في عمليات إجرامية أكثر تعقيدًا، مثل التجسس السيبراني أو الإرهاب الإلكتروني.

ومن المهم الإشارة إلى أن الفعل الجرمي الواحد قد تندمج فيه عدة دوافع، مثل المزج بين الربح المالي والدوافع الأيديولوجية أو الانتقامية، كما في حالتي سرقة الأسرار التجارية أو الهجمات السيبرانية ذات الطابع السياسي[2].

ثانيا: خصائص المجرم السيبيراني

لا يوجد اتفاق شامل بين الباحثين حول صفات مرتكبي الجرائم السيبرانية، ولا يمكن حصرهم ضمن نموذج محدد أو قالب موحّد من الخصائص. ومع ذلك، تشير العديد من الدراسات، سواء العربية أو الأجنبية، إلى وجود سمات مشتركة برزت لدى الأشخاص الذين تم التحقيق معهم أو إدانتهم في هذا النوع من الجرائم. وتُظهر هذه الدراسات أن الفئة العمرية الأكثر تورطًا في الجرائم السيبرانية تتراوح بين 14 و38 سنة، وهو ما يدل على أن أغلب مرتكبي هذه الجرائم ينتمون إلى فئة الشباب[3].

ويتميّز المجرم السيبراني بجملة من الصفات والخصائص، أبرزها:

- **المهارة والذكاء التقني** :يتمتع المجرم السيبراني بدرجة عالية من الذكاء والمعرفة التكنولوجية، تُمكّنه من تجاوز العقبات التقنية التي قد تعترضه أثناء تنفيذ الجريمة.
- **السلطة على النظم السيبرانية** :غالبًا ما تكون لدى المجرم السيبراني سلطة أو امتيازات خاصة على النظام المستهدف، كامتلاكه لكلمات المرور أو الشفرات الأمنية التي تتيح له الدخول إلى البيانات، والتحكم في محتواها بالحذف أو التعديل أو النسخ.

[1]–بوديسة بجاد عبد الرؤوف، المرجع السابق، ص23.

[2]–خالد داودي، المرجع السابق، ص39.

[3]–امحمد مولاي، صعوبات تطبيق الإدارة الالكترونية بالجزائر : الجريمة الالكترونية نموذجا"، المؤتمر العالمي الأول للإدارة الالكترونية، مركز المدينة للوسائط المتعددة، طرابلس، ليبيا، 2010، ص23,

- **القدرات الفنية المتخصصة** :عادةً ما يكون الجاني السيبراني شخصًا متمكنًا من الأدوات الرقمية، لديه مهارات متقدمة في مجال الاختراق والتلاعب بالمعلومات، ويُتقن تقنيات التشفير، واستنساخ البرامج، وتحويل الأموال إلكترونيًا.
- **غياب النزعة للعنف** :على خلاف المجرم التقليدي، فإن المجرم السيبراني لا يعتمد على العنف الجسدي في ارتكاب فعله، إذ ترتكز الجريمة السيبرانية على الخداع والتقنيات الذكية دون إحداث أذى مباشر أو عنف مادي[1].

ثالثا: أصناف المجرم السيبيراني

استنادًا إلى ما توصلت إليه الدراسات المتخصصة في مجال الجريمة السيبرانية، يمكن تصنيف مرتكبي هذه الجرائم إلى سبع فئات رئيسية، مع الإشارة إلى أن الشخص الواحد قد يجمع بين خصائص أكثر من فئة في آنٍ واحد. وتتمثل هذه الأنماط الإجرامية فيما يأتي[2]:

1. **الفاعلون بدافع التسلية والمزاح** :هم أفراد يرتكبون أفعالا سيبرانية من باب المزاح أو التحدي دون نية إحداث أضرار مباشرة، ويغلب على هذه الفئة صغار السن أو المراهقون.
2. **المتسللون بدافع الفضول** :يسعى أفراد هذه الفئة إلى اختراق أنظمة الحواسيب المحمية دون ترخيص، بهدف تجربة قدراتهم، أو بدافع الفضول الشخصي، أو لاختبار مستوى الأمان، دون نية إجرامية واضحة لتحقيق مكاسب أو إلحاق ضرر.
3. **المخترقون الحاقدون** :وهم من يتعمدون إلحاق الأذى بالغير من خلال تدمير المعطيات أو نشر البرمجيات الخبيثة، دون أن يكون هدفهم تحقيق مصلحة مادية، بل بدافع الانتقام أو الإضرار فحسب.
4. **الحلول الفردية غير القانونية** :أفراد هذه الفئة يعمدون إلى ارتكاب أفعال سيبرانية للحصول على نتائج يعجزون عن تحقيقها عبر الوسائل القانونية أو التقليدية، كمن يلجأ إلى اختراق قاعدة بيانات لحل مشكلته الشخصية.

---

[1]–علي قابوسة، عبد السلام محمد الميل، عادل محمد الشربجي، الجريمة الالكترونية في الفضاء الالكترونية –المفهوم، الأسباب، سبل المكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات سداسية، دولية محكمة، العدد 04، المركز الجامعي ايليزي، 2019، ص247.

[2]–بوعرعارة إبراهيم زياد، خصوصية الجريمة الالكترونية، مذكرة ماستر في الحقوق تخصص قانون جنائي، جامعة غرداية، الجزائر، 2021–2022، ص47.

5. **المجرمون المحترفون** :يسعى هؤلاء إلى تحقيق أرباح غير مشروعة باستخدام وسائل تقنية، ويقومون بتنظيم عملياتهم بشكل ممنهج، وغالبًا ما ينتمون إلى شبكات إجرامية منظمة، ما يجعلهم أقرب إلى خصائص المجرم التقليدي[1].

6. **المتشددون والدوافع الإيديولوجية** :تضم هذه الفئة الجماعات التي تستخدم الفضاء السيبراني وسيلة لخدمة معتقدات متطرفة سياسية أو دينية أو اجتماعية، وقد يتجه نشاطهم نحو تعطيل أنظمة الدولة أو تخريب الممتلكات العامة لجذب الانتباه إلى قضاياهم، مثل ما قامت به جماعة "الألوية الحمراء" في أوروبا خلال الثمانينيات، حين دمّرت أكثر من 60 مركزًا للمعلومات.

7. **المهملون جنائيًا** :وهم أفراد يتسببون، نتيجة إهمالهم في استخدام الأنظمة الرقمية، في أضرار جسيمة قد تصل إلى إزهاق الأرواح، كما حدث في إحدى الحوادث بنيوزيلندا، حيث تسبب تعديل غير معلن على برنامج تحديد مسار طائرة في تحطمها ومقتل عشرات الركاب، ما أدى إلى محاكمة المتسببين بتهمة القتل غير العمد[2].

الفرع الثالث:

موقف المشرع الجزائري من الجريمة السيبرانية

أحدث المشرع الجزائري مؤخراً بعض التعديلات القانونية التي تهدف إلى سد الفراغ في مجال الجرائم المعلوماتية، حيث قام باستحداث نصوص تجريمية لقمع الاعتداءات على الأنظمة المعلوماتية بموجب القانون 04/15 المؤرخ في 10 نوفمبر 2004، والذي تضمن تعديل قانون العقوبات[3]. ومع ذلك، فقد تناول المشرع في النصوص المستحدثة الاعتداءات الموجهة ضد الأنظمة المعلوماتية، لكنه أغفل الاعتداءات التي تطال منتجات الإعلام الآلي. ويمكن تلخيص الأفعال التي جرمها المشرع الجزائري في هذا القانون كما يلي:

1. **جريمة التوصل أو الدخول غير المصرح به** :نصت المادة 394 مكرر من قانون العقوبات على معاقبة كل من يدخل أو يبقى في جزء من منظومة للمعالجة الآلية للبيانات بطريقة غير مشروعة،

[1]–قورة نائلة عادل محمد.، جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقية، ط1 دار النهضة العربية، القاهرة, 2021، ص65.

[2]–رستم هشام ، محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، ط1 ،مكتبة الآلات الحديثة، أسيوط، 1994 ، ص.69.

[3]– القانون 04-15، السالف الذكر.

أو يحاول ذلك. كما تضاعف العقوبة إذا ترتب على الدخول غير المشروع حذف أو تغيير المعطيات، أو إذا تسبب في تخريب نظام اشتغال المنظومة[1].

2. **جريمة التزوير المعلوماتي** :كما ورد في المادة 394 مكرر من قانون العقوبات، تعاقب كل من يدخل معطيات بطريق الغش في نظام المعالجة الآلية أو يعدل المعطيات الموجودة فيه بطريقة غير قانونية. [2]

3. **جريمة الاستيلاء على المعطيات** :طبقاً للمادة 394 مكرر 2، يعاقب كل من يقوم بتصميم أو تجميع أو نشر أو تجارة معطيات مخزنة أو معالجة أو مرسلة عبر منظومة معلوماتية، أو يقوم بحيازة أو نشر أو استخدام هذه المعطيات لغرض غير مشروع.

4. **جريمة إتلاف وتدمير المعطيات** :وفقاً للمادة 394 مكرر 3، يعاقب كل من يتلف أو يعدل أو يحذف معطيات من نظام المعالجة الآلية بطريقة غير قانونية، خاصة إذا تم ذلك باستخدام الفيروسات. [3]

5. **جريمة الاحتيال المعلوماتي** :نصت المادة 394 مكرر 2/1 على معاقبة كل من يقوم بتصميم أو تجميع أو نشر معطيات عبر منظومة معلوماتية بغرض جني فوائد مالية غير مشروعة.

6. **الجرائم المتعلقة بالإنترنت والمحتوى الضار** :تم تجريم أفعال الحيازة والنشر والاستخدام غير المشروع للمعطيات التي يتم الحصول عليها من الجرائم المنصوص عليها في القانون، مثل التلاعب بالمعلومات لغرض المنافسة غير المشروعة، التجسس، الإرهاب، والتحريض على الفسق. [4]

---

[1]– مال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة الجزائر ، د ت ، ص 99.

[2]– نص المادة 394من قانون العقوبات":مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق 1 المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها."

[3]– تنص المادة 394 مكرر 2 من قانون العقوبات " : يعاقب بالحبس والغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي :
–تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكبيها الجرائم المنصوص عليها في هذا القسم .
–حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم

[4]– العيد شعثان، مسعود موفقي، المرجع السابق، ص46.

أما الجزاءات التي تضمنها الفصل السابع مكرر من قانون العقوبات، فتتمثل في عقوبات حبسية وغرامات، بالإضافة إلى عقوبات تكميلية مثل مصادرة الأجهزة والبرامج المستخدمة في ارتكاب الجرائم، وإغلاق المواقع الإلكترونية التي ترتكب من خلالها الجرائم. كما تم تحديد حالات تشديد العقوبة مثل في حالة حذف أو تغيير المعطيات أو تخريب النظام. وأدرج المشرع الجزائري ضمن نصوصه تجريم الاشتراك في جرائم المعلوماتية سواء من قبل الأشخاص الطبيعيين أو المعنويين. [1]

كما أضاف المشرع الجزائري في الأمر 05/03 المؤرخ في 19 يوليو 2003، والذي يتعلق بحقوق المؤلف والحقوق المجاورة، حماية خاصة للبرمجيات الحاسوبية وأخضعها لقوانين الملكية الفكرية، حيث فرض عقوبات حبسية وغرامات على كل من يعتدي على هذه البرامج.

المطلب الثاني:

خصائص الجرائم السيبرانية وطبيعتها القانونية

تتميز الجرائم السيبرانية بخصوصيات قانونية وتقنية تجعلها تختلف عن الجرائم التقليدية، سواء من حيث الوسائل المستخدمة أو طبيعة الأفعال المرتكبة. ويناقش هذا المطلب أبرز السمات التي تنفرد بها هذه الجرائم، وطبيعة النظام القانوني الذي يحكمها في ظل التطورات الرقمية المتسارعة.و عليه سنتطرق في هذا المطلب الى خصائص الجريمة السيبيرانية (الفرع الأول) ثم الطبيعة القانونية للجرائم السيبيرانية (الفرع الثاني).

الفرع الأول:

خصائص الجريمة السيبيرانية

سيتم في هذا الفرع التطرق إلى أبرز السمات التي تنفرد بها الجريمة السيبرانية وتميزها عن باقي أنماط الجرائم التقليدية، وذلك من خلال عرض مجموعة من الخصائص النوعية التي تعكس طبيعتها المستحدثة وتعقيداتها التقنية، كما يلي:

أولا: الطابع "الناعم" للجريمة السيبرانية.

تُعد الجرائم الإلكترونية من الجرائم "الناعمة"، وذلك لكونها غالبًا ما تُرتكب بطريقة خفية وغير محسوسة، دون إثارة انتباه الضحية أو من حوله، وقد تتم في لحظة وجوده على الشبكة دون أن يلحظ شيئًا.

[1]– امال قارة، المرجع السابق، ص102.

هذه الخفة في التنفيذ راجعة إلى الطبيعة غير المادية للجريمة السيبرانية[1]، إضافة إلى تمتع مرتكبها بقدرات تقنية عالية تتيح له تنفيذ الاعتداء بدقة فائقة دون ترك أثر واضح. وتُعد جرائم مثل إرسال الفيروسات، وسرقة البيانات البنكية أو المعلومات الشخصية، أو عمليات التجسس الرقمي، من أبرز الأمثلة التي تعكس هذا الأسلوب المتخفي. [2]

وما يزيد من خطورة هذه الجرائم هو البيئة الرقمية التي تسمح للمجرمين حول العالم بالتواصل وتبادل المعارف والمهارات التقنية بسهولة عبر منتديات متخصصة ومواقع إلكترونية خفية، مثل تلك التي تُعرف بمنتديات "الهاكرز". حيث تُمثل هذه الفضاءات الإلكترونية منصات لتبادل الأساليب الحديثة في الاختراق والاحتيال الرقمي، ما يعزز من قدراتهم التخريبية ويُصعّب من مهام تعقبهم من قبل الجهات الأمنية، نظراً لاعتمادهم على أدوات التمويه والتشفير والبروكسيات متعددة الجنسيات[3].

ثانيا: اعتبارها أقل عنفا في التنفيذ.

تتميز جرائم الإنترنت بأنها أقل عنفاً في التنفيذ مقارنة بالجرائم التقليدية، حيث لا تتطلب جهدًا كبيرًا أو عنفًا ماديًا. على عكس الجرائم التقليدية التي قد تتطلب مجهودًا عضليًا، مثل الجرائم التي تشمل العنف الجسدي كجريمة القتل أو الاختطاف، أو تلك التي تنطوي على تكسير أو خلع في جريمة السرقة، فإن جرائم الإنترنت تُنفذ بأساليب غير عنيفة. فكل ما يحتاجه الجاني هو إلمام تقني بأساسيات التعامل مع أجهزة الحاسوب، واستخدام الشبكة العنكبوتية (الإنترنت) كأداة لارتكاب الأفعال غير المشروعة، مثل التجسس أو اختراق الخصوصيات أو استغلال الأطفال. بهذا الشكل، يمكن وصف الجرائم المرتكبة عبر الإنترنت بأنها جرائم "نظيفة"، حيث لا تترك وراءها أي أثر مادي ملموس، بل يتم التلاعب بالأرقام والبيانات داخل سجلات الحواسيب، دون أن يكون لها تأثير مرئي أو جسدي على الأشخاص[4].

---

[1]-امال قارة، المرجع السابق، ص102.

[2]– أسامة مهمل، الاجرام السيبيراني، مذكرة ماستر في الحقوق تخصص قانون جنائي، جامعة محمد بوضياف، المسيلة، الجزائر،2017–2018،ص12.

[3]– عبد المؤمن بن صغير " الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن ، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة الموسوم بعنوان الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و 17 نوفمبر 2015، ص 08

[4]–صالح بن محمد المسند وعبد الرحمان بن راشد المهيني " جرائم الحاسب الآلى الخطر الحقيقي في عصر المعلومات ". المجلة العربية للدراسات الأمنية والتدريب العدد 29 (المجلد (15) أفريل 2000، ص 20

هذا وقد لا يقتصر الضرر المترتب عن الجريمة على المجنى عليه وحده، وإنما قد يتعداه إلى متضررين آخرين في عدة دول، وهو الملاحظ من خلال جرائم نشر المواد ذات الخطر الديني والأخلاقي والأمني والسياسي والتربوي والثقافي والإقتصادي.[1]

تتم الجرائم السيبرانية في الغالب الأعم بواسطة أفعال ترتكب من قبل أشخاص من خارج الحدود، كما أنها تمر عبر شبكات وأنظمة المعلومات، الأمر الذي يثير التساؤل حول الإختصاص القضائي لهذه الجرائم، علاوة على أن إمتداد أنشطة الملاحقة والتحري والضبط والتفيش خارج الحدود، أمر يحتاج إلى تعاون دولي شامل يستهدف تحقيق مكافحة هذه الجرائم، مع إحترام السيادة الوطنية للدول المعنية .[2]

رابعا: عدم قيام ضحايا الإجرام السيبراني بتقديم الشكوى أو التبليغ.

من بين خصائص الجريمة السيبرانية، أنه لا يتم في غالب الأحيان تقديم شكوى أو الإبلاغ عند إرتكابها، إما لعدم إكتشاف الضحية لها وإما خوفا من التشهير [3]، لذا نجد أن معظم جرائم الأنترنت تكتشف بالمصادفة، وأحيانا بعد وقت طويل من إرتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد الجرائم المرتكبة والعدد الذي تم إكتشافه هو رقم خطير .[4]

وتبدو هذه الظاهرة أكثر وضوحا في المؤسسات المالية، كالبنوك والمؤسسات الإدخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها عادة من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو إتخاذ الإجراءات القضائية بشأنها إلى نقص ثقة عملائها فيها وإنصرافهم عنها.[5]

خامسا: صعوبة الوصول إلى الدليل.

تكون البيانات والمعلومات المتداولة عبر شبكة الأنترنت على هيئة رموز مخزنة في وسائط تخزين ممغنطة بلغة الصفر والواحد لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه

---

[1]– عبد المومن بن صغير المرجع السابق، ص 09

[2]–المرجع نفسه، ص 11

[3]– أمير فرج يوسف الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص 157.

[4]– عبد الرحمان جميل محمود حسين الحماية القانونية لبرامج الحاسب الآلي، مذكرة ماجيستير جامعة النجاح الوطنية نابلس فلسطين، كلية الدراسات العلياء 2008، ص 09

[5]– محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر،2009،ص37.

بالقراءة والتوصل عن طريقه إلى الجاني يبدوا أمرا صعبا، خاصة وأن الجاني يسعى إلى عدم ترك أثر لجريمته، ضف إلى ذلك ما يتطلبه من فحص دقيق الموقع الجريمة من قبل المتخصصين في هذا المجال، للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة.[1]

وتتم الجريمة المرتكبة عبر الأنترنت خارج إطار الواقع المادي الملموس، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق، فداخل هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة ،كما يسعى مرتكب الجريمة السيبرانية إلى إعاقة سلطات التحقيق في الوصول إلى الدليل بشتى الوسائل الممكنة، كحذف البرامج أو وضع رموز سرية وكلمات للمرور، وقد يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه.[2]

إنه من السهل مسح الدليل من الكمبيوتر في زمن قياسي بإستخدام البرامج المخصصة لذلك، إذ يتم بمجرد لمسة خاطفة على لوحة المفاتيح، على إعتبار أن الجريمة تتم بأوامر وتعليمات تصدر إلى الجهاز ، ومن بين صعوبات الوصول إلى الدليل أيضا، قيام كبرى المواقع العالمية بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية، لمنع التسلل والوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها ونسخها.[3]

سادساً: صعوبة ضبط وتكييف الجرائم السيبرانية.

من الواضح أن رجال الشرطة القضائية والمحققين والقضاة يواجهون تحديات كبيرة في عمليات ضبط الجرائم المعلوماتية وتحديد الوصف القانوني المناسب لها. يرجع السبب في ذلك إلى الطبيعة المميزة لهذه الجرائم التي تحدث في بيئة إلكترونية تتسم بالتغير السريع والديناميكية، فضلاً عن انتشارها عبر الحدود الجغرافية، مما يجعل من الصعب تحديد نطاق القضية وملاءمة القوانين المتاحة لها. [4]

سابعا: تصادم التفتيش عن الأدلة مع الحق في الخصوصية المعلوماتية.

---

[1]– موسى مسعود أرحومة " الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، مداخلة مقدمة ضمن فعاليات المؤتمر المغاربي الأول الذي نظمته أكاديمية الدراسات العليا بطرابلس الموسوم بعنوان: المعلوماتية والقانون، يومي 28 –29 أكتوبر، 2010،ص03.

[2]–محمد عبيد الكعبي، نفس المرجع، ص 38

[3]–عبد المؤمن بن صغير المرجع السابق، ص 11.

[4]–أسامة مهمل، المرجع السابق،ص16.

يتم التفتيش في الجرائم السيبرانية بشكل أساسي على نظم الكمبيوتر، قواعد البيانات، وشبكات المعلومات، وقد يتطلب الأمر التوسع في التفتيش ليشمل أنظمة أخرى مرتبطة بالنظام المشتبه فيه، وذلك بسبب الانتشار الواسع للتشبيك بين الحواسيب وتوزع الشبكات الداخلية على مستوى المؤسسات والشبكات المحلية والدولية. لا شك أن هذا التوسع في التفتيش يمكن أن يتداخل مع الحق في الخصوصية المعلوماتية للأفراد الذين يمتد التفتيش إلى أنظمتهم، مما يثير تساؤلات قانونية حول التوازن بين حقوق الخصوصية وضرورة جمع الأدلة في التحقيقات. [1]

الفرع الثاني:

الطبيعة القانونية للجرائم السيبيرانية

تُعد الطبيعة القانونية للجريمة السيبرانية من أبرز الإشكالات المطروحة في ظل التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصال، فهي تمثل نقلة نوعية في مفهوم الجريمة من الشكل التقليدي إلى النمط الرقمي المعقد.[2]

ويكمن جوهر هذا الطرح في ضرورة تحديد الوضع القانوني للبيانات والمعلومات والبرمجيات، وما إذا كانت تُشكل قيمة قانونية قائمة بذاتها، أم أنها مجرد عناصر مستحدثة تنضوي ضمن القيم القابلة للحماية.

فخلافًا للجرائم التقليدية التي تُمارس في بيئات مادية واضحة، ترتبط الجرائم السيبرانية بفضاءات رقمية تعتمد على نظم المعالجة الإلكترونية للبيانات، حيث يتم الاعتداء من خلال التلاعب بالبرمجيات أو البيانات المخزنة أو المتبادلة إلكترونيًا. وتتضمن هذه الجرائم سلوكيات مثل تجميع البيانات أو معالجتها أو إدخالها أو استخراجها بطرق غير قانونية، ما يجعل محل الجريمة إما البيانات والمعلومات أو البرامج ذاتها، أو حتى البنية التحتية الرقمية التي تُستخدم كوسيلة للاعتداء. وتظهر أهمية هذا النقاش بشكل خاص عند الحديث عن ما يُعرف بالمال المعلوماتي، الذي يُقسم إلى نوعين: مال معلوماتي ذو طبيعة معنوية يتعلق بالمحتوى الرقمي غير الملموس، ومال معلوماتي ذو طبيعة مادية يمس البنية التقنية والأجهزة المادية الحاملة للمعلومة. [3]

---

[1]– موسى مسعود أرحومة المرجع السابق، ،ص03.

[2]–نورهان محمد الربيعي، الجريمة السيبيرانية و آليات مكافحتها (دراسة مقارنة)، مجلة الفارابي للعلوم الإنسانية ، المجلد 03، العدد 01، كلية الحقوق، جامعة عجمان، الامارات العربية المتحدة، 2024،ص81.

[3]– فريد روايح، محاضرات في القانون الجنائي العام، مطبوعة دروس للسنة الثانية ليسانس، قسم الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر،2018–2019، ص87.

وقد طرحت شبكة الإنترنت تحديات قانونية معقدة تتعلق بمدى خضوع خدمات النشر الإلكتروني وتبادل المعلومات لأطر قانونية واضحة، الأمر الذي يثير تساؤلات حول تحديد النظام القانوني الواجب التطبيق على هذه الخدمات، خاصة في ظل صعوبات إثبات الجريمة، ووجود تقنيات تشفير متقدمة، وصعوبة تحديد الفاعل الحقيقي أو مكان ارتكاب الجريمة، نظرًا للطبيعة العابرة للحدود للفضاء السيبراني.

كما أن غموض الاختصاص القضائي الدولي في الكثير من الحالات يعيق تطبيق العقوبات أو محاكمة الجناة. وبناءً على ما سبق، فإن تحديد الطبيعة القانونية للجريمة السيبرانية يُعد خطوة أساسية لفهم هذا النوع من الجرائم ووضع أسس قانونية مناسبة لمكافحتها، سواء من خلال تحديد المجال الذي تقع فيه الجريمة (الفضاء الرقمي)، أو محل الاعتداء (البيانات أو البرمجيات)، بما يضمن مواءمة النصوص القانونية مع واقع الجريمة المعلوماتية المعاصرة وتطوراتها التقنية المتسارعة. [1]

[1]–نورهان محمد الربيعي، المرجع السابق ،ص81.

المبحث الثاني:

مجال ونطاق الامن السيبيراني

يعد تصنيف الجرائم السيبرانية أمرًا أساسيًا لضبط هذا النوع من الإجرام وتحديد آليات التجريم والعقاب بفعالية.[1] يساعد التصنيف في تنظيم الأفعال الجرمية وفق معايير واضحة، مما يعزز من تماسك السياسة الجنائية. يتناول هذا المبحث أنواع الجرائم السيبرانية (المطلب الأول) وأركان الجرائم السيبرانية (الفرع الثاني).

المطلب الاول:

انواع الجرائم السيبرانية

يصعب تعداد جميع أصناف الجرائم الإلكترونية باعتبارها تستند إلى تقنيات حديثة، غير أنه يمكن تقسيمه إلى نوعين الجرائم الإلكترونية المرتكبة بواسطة النظام المعلوماتي (الفرع الأول) وتلك المرتكبة على النظام المعلوماتي(الفرع الثاني).

الفرع الأول :

الجرائم الإلكترونية المرتكبة بواسطة النظام المعلوماتي

ونفرق في هذا المجال بين الجرائم الإلكترونية المرتكبة ضد الأشخاص الطبيعية، وتلك المرتكبة ضد الأشخاص المعنوية، حيث سنتناول:

أولا – الجرائم الإلكترونية المرتكبة ضد الأشخاص الطبيعية :

وتسمى كذلك بجرائم الإنترنيت الشخصية كونها تمس بالأفراد من خلال الوصول إلى هويتهم الشخصية عن طريق قرصنة حساباتهم الشخصية وانتحال شخصيتهم أو الإطلاع على صورهم الشخصية لاستعمال غير مشروع كابتزازهم بها بهدف كسب المال . [2]

وعليه، يعد استخدام النظام المعلوماتي في الاعتداء على حرمة الأفراد جريمة يعاقب عليها القانون وتتمثل الجرائم الإلكترونية ضد الأفراد الأكثر شيوعا في انتحال شخصيات فنية أو سياسية والتشهير بها عبر

[1]–فريد روايح، المرجع السابق، ص87.

[2]لاكلي نادية، الجريمة السيبيرانية في الجزائر والعقوبات المقررة لها، مجلة الاجتهاد القضائي ، المجلد 15، العدد 01، جامعة بلحاج بوشعيب، عين تموشنت، الجزائر، 2023،ص263.

المواقع الإلكترونية من خلال الولوج إلى النظام المعلوماتي الخاص بالضحايا واستخدام معلوماتهم وصورهم الشخصية التي تم سرقتها من حساباتهم الخاصة، وتهديدهم بها مقابل الحصول على المال .

كما يمكن للمجرم اختراق النظام المعلوماتي للشخص للإعتداء على حقوقه الفكرية والأدبية والفنية من خلال سرقة بعض المعلومات العلمية مثلا ونسبها إليه، أو الإعتداء على براءة الاختراع إذ تعتبر كلها حقوقا معنوية شخصية محمية قانونا وغالبا ما تتم الجرائم الإلكترونية ضد الأفراد من خلال الولوج إلى بريدهم الإلكتروني للحصول على هويتهم الشخصية . [1]

ونشير إلى أن المشرع الجزائري قد كرس مجموعة من الآليات الحماية الأشخاص في العالم الافتراضي لاسيما مع تعدد مواقع التواصل الاجتماعي وخطورتها وذلك بموجب القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث أكدت المادة الثانية منه على ضرورة معالجة المعطيات ذات الطابع الشخصي في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة كم استحدث هذا القانون سلطة وطنية لحماية المعطيات ذات الطابع الشخصي والتي تتخذ إجراءات ادارية في حالة خرق أحكام هذا القانون من طرف المسؤول عن المعالجة، كما يمكنها القيام بالتحريات اللازمة ومعاينة المحلات التي تتم فيها المعالجة ماعدا محلات السكن، كما يمكنها الولوج على المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها. [2]

ونظرا للتطور التكنولوجي في المجال التجاري والذي أدى إلى ظهور التجارة الالكترونية كرس المشرع الجزائري حماية للمستهلك الالكتروني من خلال حماية بياناته الالكترونية لاسيما تلك المتعلقة ببطاقة الدفع في حالة استعمالها لاقتناء منتوجاته، فنجد أن القانون رقم 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين خصص إجراءات تقنية معينة لحماية وسائل الدفع الالكتروني من الهجمات السيبرانية تتمثل في التوقيع والتصديق، إذ يخضع التوقيع الالكتروني إلى تقنية التشفير والمتمثلة في تحويل البيانات المتعلقة ببطاقة الدفع الإلكتروني إلى رموز مبهمة لا يمكن للغير الاطلاع عليه أو فهمها إلا من خلال استخدام المفتاح السري لها لفك هذه الشفرة فنظرا لحساسية التوقيع الإلكتروني والمعاملات الإلكترونية يشترط ان تصدر تقنية التشفير من جهة مختصة بذلك.

ولقد خول المشرع الجزائري بموجب المادة 14 من القانون رقم 15-04 هذا الاختصاص إلى الهيئة الوطنية المكلفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منه، فلا يحق حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الكتروني من طرف الغير ويعتبر هذا التصرف غير مشروع ومعاقب عليه بمقتضى

[1] بن يونس علي، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، مصر،2004،ص21.

[2] -لاكلي نادية ، المرجع السابق، ص264.

المادة 68 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، إذ تتمثل العقوبة بالنسبة للشخص الطبيعي في الحبس من 03 أشهر إلى 03 سنوات وغرامة مالية من 1000.000 دج إلى 5000.000 دج أو بإحدى هاتين العقوبتين . [1]

أما بالنسبة للتصديق الالكتروني فلقد أنشأ المشرع الجزائري بموجب القانون رقم 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين في الباب الثالث منه ثلاث سلطات للتصديق الإلكتروني :

-**السلطة الوطنية:** تهتم بإعداد سياسة التصديق الإلكتروني والسهر على تطبيقها والموافقة على سياسات التصديق الصادرة عن السلطتين الحكومية والاقتصادية .

-**السلطة الحكومية** :والتي يكمن دورها في متابعة ومراقبة التصديق الإلكتروني بالإضافة إلى إعداد القواعد والإجراءات التنظيمية والتقنية الخاصة بالتوقيع والتصديق الإلكترونيين والسهر على تطبيقهما بعد الحصول على موافقة السلطة الوطنية وهذا ما أقرته المادة 28 من القانون رقم 15-04 .

-**السلطة الاقتصادية** والتي حولها المشرع بموجب المادة 30 من القانون رقم 15-04 مجموعة من السلطات منها سلطة منح التراخيص المؤدي خدمات التصديق الإلكتروني والموافقة على سياسات التصديق الصادرة عنهم والسهر على تطبيقها واتخاذ التدابير اللازمة لضمان استمرارية هذه الخدمات في حالة عجز مؤدي خدمات التصديق الإلكتروني عن تقديمها. كما يمكن أن تلعب السلطة الاقتصادية دور التحكيم في النزاعات القائمة بين مؤديي خدمات التصديق الإلكتروني فيما بينهم أو مع المستعملين .

وتسند المؤدي خدمات التصديق الالكتروني عملية التصديق لضمان صحة البيانات الالكترونية، ثم يقوم مؤدي خدمات التصديق الإلكتروني بإصدار شهادة تثبت بأن التوقيع الإلكتروني صحيحا وصادرا عن صاحبه الحقيقي وأن البيانات كلها صحيحة لا احتيال فيها. وأنه يستوفي جميع الشروط القانونية المطلوبة وتسمى هذه الشهادة بشهادة التصديق الإلكتروني." [2]

كما أكد المشرع على ضرورة إنشاء واستغلال منصات الدفع الإلكتروني حصريا من طرف البنوك المعتمدة من قبل بنك الجزائر وبريد الجزائر وهذا ما نصت عليه المادة 27 من القانون رقم 18-05 المتعلق بالتجارة الالكترونية في فقرتها الثانية، وتخضع منصات الدفع الإلكتروني الرقابة بنك الجزائر لضمان

[1]- العزيز سميرحامد، التعاقد عبر تقنيات الاتصال الحديثة -دراسة مقارنة)، دار النهضة العربية،2001،ص62.

[2]-العزيز سميرحامد، المرجع السابق،ص62.

استجابتها السرية البيانات وسلامتها وأمن ،تبادلها، وهذا ما جاء في نص المادة 29 من القانون رقم 18-05 المتعلق بالتجارة الإلكترونية . [1]

ثانيا – الجرائم الإلكترونية ضد الأشخاص المعنوية :

هي جرائم تستهدف المؤسسات بشتى أنواعها، يقوم الجاني من خلالها بإتلاف الوثائق المهمة للمؤسسة أو برامجها الخاصة، أو استعمال بيانات غير مسموح بها من أجل اختلاس المال من المؤسسات المالية . [2]

ومن بين الجرائم الإلكترونية الشائعة في هذا المجال السرقة الواقعة على المؤسسات المالية لاسيما في المجتمعات المتقدمة، إذ يقوم الجاني باختلاس البيانات الخاصة بزبائن البنك والمحفوظة في برنامج خاص ويستخدم شخصية الضحية لتحويل المال لحسابه الخاص أو يقوم الجاني بإنشاء صفحة انترنيت مطابقة لصفحة أحد البنوك الكبرى ويطلب من العميل إدخال بياناته الخاصة من أجل استخدامها في سرقة المال، ولا يقتصر الأمر على الأشخاص الطبيعية والمعنوية فحسب بل قد تمتد الجريمة الإلكترونية إلى المساس بأمن الدولة من خلال اختراق الجاني للمواقع الخاصة بالدولة كالمواقع العسكرية، ونشر المعلومات السرية بهدف المساس بأمن الدولة بواسطة برامج متخصصة في فك أو سرقة كلمة السر .

الفرع الثاني:

الجرائم الإلكترونية المرتكبة داخل النظام المعلوماتي

بالإضافة إلى الجريمة الإلكترونية التي ترتكب بواسطة النظام المعلوماتي توجد جرائم الكترونية يكون النظام المعلوماتي في حد ذاته محل الجريمة، وتستهدف هذه الجرائم إما المكونات المادية أو المنطقية (برامج للنظام المعلوماتي أو المعلومات المدرجة في النظام المعلوماتي .

أولا – الجرائم الواقعة على المكونات المادية للنظام المعلوماتي :

ويقصد بها تلك الجرائم التي تستهدف الأجهزة والمعدات الملحقة التي تستخدم في تشغيل النظام المعلوماتي كالأسطوانات مثلا وذلك من خلال سرقتها أو إتلافها عمدا، إذ تكمن القيمة الحقيقية للمعدات فيما تحتويه من معلومات .

[1]–جمال ابراهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية ، المجلد 11،العدد 02، جامعة مولود معمري، تيزي وزو، الجزائر، دت ،ص120.

[2]– امال قارة ، المرجع السابق، ص102.

ثانيا – الجرائم الواقعة على برامج النظام المعلوماتي :

يتميز مرتكب هذه الجريمة بمعرفة تقنية عالية في المجال المعلوماتي وتتمثل هذه الجرائم في الدخول إلى النظام المعلوماتي للشخص والبقاء فيه لتعديل أو حذف بياناته أو الاستيلاء على البيانات الشخصية لاستعمالها لأغراض غير مشروعة كسرقة المال وغالبا ما تكون في مجال المؤسسات المالية كما تتجلى هذه الجريمة من خلال التلاعب في البرامج بزرع برنامج فرعي في البرنامج الأصلي يسمح بالولوج في أي نظام معلوماتي وتعد جريمة البقاء في النظام المعلوماتي جريمة مستمرة لأنها مقترنة بفترة زمنية تستمر فيها الجريمة .[1]

كما يمكن تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي وتعتبر المعلومة المعاجة آليا أساس عمل النظام المعلوماتي لذلك قد تكون محل الجريمة الإلكترونية من خلال تعديل المعلومات الموجودة داخل النظام أو إتلافها من خلال الإستعانة ببعض البرامج الفيروسية، ويعد برنامج حصان طراودة Le cheval de (troie)من أشهر هذه البرامج وهو نوع من الفيروسات الضارة يظهر في شكل برنامج مفيد لخداع الضحية لكنه يحتوي على فيروس يسمح للشخص بالتجسس على الآخرين وسرقة بياناتهم بكل سهولة .

كما توجد انواع أخرى من الفيروسات الضارة كفيروس "الدودة (Le vers) "وهو عبارة عن برنامج ينتشر في شبكات المعلوماتية بصورة أوتوماتيكية، وتتمثل وظيفته في التكاثر بشكل يؤدي إلى تعطيل الشبكات المعلوامتية لتسهيل تسرب مختلف الفيروسات[2] ."

ويوجد أيضا فيروس القنبلة المنطقية (La bombe logique) وهو عبارة عن برنامج يتم تنفيذه في فترة زمنية معينة، ويقوم هذا الفيروس بتسهيل تنفيذ العمليات غير المشروعة من قبل الجاني وتدمير النظام المعلوماتي .[3]

ونشير إلى أنه مجرد استعمال الفيروس المعلوماتي يدل على وجود فعل مجرم قانونا، وقد اعتبر القضاء الفرنسي في إحدى القضايا المعروضة أمامه في هذا المجال بأنه تعتبر شركة الصيانة في مجال

---

[1]–محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، مصر، 1993،ص189.

[2]–مغنية تشتاش، مداخلة حول الركن المفترض في الجريمة المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، 2015–2016،ص05.

[3]–قطاف سليمان، بوقرين عبد الحليم، الاليات الموضوعية والاجرائية المتبعة لتحقيق الامن السيبيراني (الجزائر نموذجا)، مجلة الحوكمة والقانون الاقتصادي، جامعة عمار ثليجي ، الاغواط، الجزائر، 2023، ص86.

المعلوماتية مسؤولة عن الضرر اللاحق بالنظام المعلوماتي المملوك للغير نظرا للإستعمال غير المشروع الفيروس القنبلة الذي أدى إلى تدمير النظام المعلوماتي، واعتبر القاضي في هذه القضية مسير الشركة فاعلا أصليا للجريمة بينما اعتبر باقي العمال شركاء له فيها . لذلك ينصح دائما بتحميل البرامج المضادة للفيروسات المعلوماتية بهدف حماية النظام المعلوماتي منها. [1]

وعليه، يمكن أن تتجلى جريمة الاعتداء على النظام المعلوماتي من خلال الدخول والبقاء فيه بشكل غير مشروع، أي استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه ، ولا يشكل الدخول في النظام المعلوماتي تصرف محظور في حد ذاته وإنما عدم الترخيص بهذا الدخول يشكل جريمة. ويعتبر الدخول في النظام المعلوماتي جريمة شكلية لا تتطلب الركن المادي لتحقق نتيجتها الإجرامية، إذ يشكل تصرفا محظورا مجرد الدخول في كل او جزء من النظام المعلواتي دون علم أو إذن صاحبه وهذا ما يفهم من نص المادة 394 مكرر من قانون العقوبات ... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..... وجاءت صيغة المادة بشكل عام إذ لم يشترط أن يكون النظام المعلوماتي محمي فنيا لحظر الدخول بل يجرم الدخول في النظام المعلوماتي حتى في حالة عدم حمايته شريطة عدم الحصول على ترخيص . [2]

وبالتالي تعتبر جريمة الدخول الإحتيالي إلى النظام المعلوماتي إذ لا يشكل الدخول الخطأ تصرفا يعاقب عليه القانون نظرا لحسن النية، ولكن يصعب إثبات نية الجاني في هذا النوع من الجرائم .

ويعاقب القانون جريمة الدخول إلى النظام المعلوماتي مهما كانت الوسيلة المستعملة وتفرق في هذا المجال بين الإتصال المادي المباشر بالنظام المعلوماتي وبين الإتصال المعنوي عن بعد بالنظام المعلوماتي

ويقصد بالإتصال المادي المباشر بالنظام المعلوماتي الدخول عليه دون الحاجة إلى وسيلة الكترونية كشبكة الأنترنت، إذ يكون الجاني في نفس مكان تواجد النظام المعلوماتي ويقوم بعمليات مادية كالتلاعب بمعطيات النظام وتعديلها أو نقلها إلى قرص مضغوط مثلا من أجل استخدامها لأغراض شخصية، كالجرائم التي يقوم بها موظفو الشركات الكبرى أو البنوك، أو تلك التي يقوم بها الشخص المكلف بصيانة الجهاز . [3]

---

[1]–مروة خنتي، الملتقة الدولي بعنوان الجرائم السيبيرانية الظاهرة المستجدة الأسباب وسبل المعالجة ، مداخلة بعنوان الجريمة السيبيرانية نقطة تهديد للمحتوي الرقمي ، جامعة خميس مليانة، 24–25 نوفمبر 2024، الجزائر، ص15.

[2]–بدر عدنان ، احمد سعيد الخبيزي، تحديات و تهديدات الأمن السيبراني و طرق التغلب عليها، حوليات آداب عين الشمس، جامعة عين الشمس، المجلد 51 ،العدد سبتمبر ،2023 مصر، ص230

[3]–راوية بنت عطية هلا الصحفي، الجرائم السيبرانية، مجلة الإلكترونية الشاملة متعددة التخصصات ، العدد 24، 2020،ص53.

أما الإتصال المعنوي عن بعد بالنظام المعلوماتي فيقصد به الدخول إلى النظام المعلوماتي عن بعد من خلال استعمال شبكة الانترنت إذ يمكن للجاني في هذه الحالة ارتكاب الجريمة وهو في مكانه دون الحاجة إلى التنقل إلى المكان المعني .

وفي كلتا الحالتين يجب توافر العنصر المعنوي للجريمة أي يجب أن يقوم الجاني بالدخول إلى النظام المعلوماتي بإرادته وليس عن طريق الصدفة أو الخطأ، فلا يعاقب القانون الدخول غير المقصود إلى النظام المعلوماتي. [1]

كما تتجلى الجريمة المعلوماتية من خلال البقاء في النظام المعلوماتي أي الاستمرار في التواجد فيه دون ترخيص من صاحبه، إذ يكمن الركن المادي لهذه الجريمة في البقاء في المنظومة دون إذن صاحبها. وقد يحدث ان يدخل شخص في نظام معلوماتي بالخطأ دون قصد الإضرار بصاحبه فيجيب عليه في هذه الحالة الخروج فورا من النظام وعدم البقاء فيه .

يعتبر البقاء الإحتيالي في النظام المعلوماتي المرحلة الموالية للدخول فيه، وقد يكون هذا البقاء ناتجا عن دخول مشروع أي عن طريق الخطأ أو الصدفة، كما قد يكون ناتجا عن دخول احتيالي بهدف الإضرار بالنظام المعلوماتي ويعرف البعض البقاء الإحتيالي في النظام المعلوماتي بانه اتصال غير عادي بالنظام المعلوماتي عن طريق الشبكة المعلوماتية والنظر في المعطيات التي يتضمنها هذا النظام دون علم صاحبها.

المطلب الثاني:

اركان الجرائم السيبرانية

تستند الجريمة الإلكترونية إلى ثلاثة أركان أساسية: الركن المادي، الركن الشرعي، والركن المعنوي. ولها خصائص مميزة تفرقها عن الجرائم التقليدية. من أبرز هذه الخصائص أن الجرائم الإلكترونية تستلزم وجود جهاز إلكتروني واستخدامه بمهارة، حيث أن الهدف منها غالبًا ما يكون المساس بالكيانات المعنوية المرتبطة بتلك الأجهزة. كما تتميز الجريمة الإلكترونية بأنها بلا حدود جغرافية، مما يجعلها تنتشر عبر الفضاء الإلكتروني العالمي. ومن الصعب إثبات هذه الجرائم واكتشاف مرتكبيها بسبب الطبيعة التقنية التي تميزها. وسوف نتطرق في المطلب الى (الركن الشرعي للجريمة الالكترونية في الفرع الأول) ثم (الركن المادي والركن المعنوي للجريمة الإلكترونية في الفرع الثاني)

[1]–ينو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون و التنمية، المجلد 4، العدد 1، 2022،ص61.

الفرع الاول:

الركن الشرعي

ان الركن الشرعي للجريمة يُقصد به وجود نص قانوني يجرم الفعل ويحدد العقوبة المقررة له في وقت ارتكاب هذا الفعل. وبناءً على هذا الركن، لا يجوز محاكمة الشخص عن فعل ارتكبه قبل صدور النص الذي يجرمه، أو بعد إلغاء هذا النص. كما أنه لا يجوز القياس على أفعال لم ينص المشرع على تجريمها، أو مقارنة أفعال أخرى ورد نص التجريم عليها، بغض النظر عن التشابه بينها من حيث الدوافع أو الفاعلية أو النتائج أو العناصر. وهذا يشير إلى أنه لا يجوز التوسع في تفسير النصوص الجزائية، ويتعين على القضاة الالتزام الصارم بمضامين النصوص القانونية ومدلولها عند تطبيقها. [1]

تعتبر الجريمة نتيجة للأفعال المادية الصادرة عن الإنسان، وهذه الأفعال تتنوع حسب أنشطة الفرد، وهو ما دفع المشرع إلى التدخل بتحديد الأفعال الضارة وتجريمها وفق نص قانوني يحدد الفعل المجرم والعقوبة المقررة له. ويُعد هذا المبدأ أساسًا لفهم كيفية تفسير القاضي للنصوص القانونية، حيث يجب عليه أن يتبع تفسيرًا ضيقًا للنصوص، ويمنع عليه اللجوء إلى القياس أو التوسع في تفسير النصوص الجزائية. وهذا يعني أنه لا يمكن للقاضي أن يقيس فعلًا ورد نص بتجريمه على فعل آخر لم يُنص عليه، بل يجب أن يلتزم بالعقوبات المنصوص عليها للأفعال المحددة فقط. [2]

مع ظهور شبكة الإنترنت، تطورت ظاهرة الجريمة بشكل كبير، مما أدى إلى تفشي الجريمة الإلكترونية. وقد زادت خطورة هذا الوضع خاصة بعد أن أصدر المجلس الأوروبي في سنة 1989 توصية لتشجيع الدول الأعضاء على تبني نصوص عقابية خاصة بالمساس بأنظمة المعالجة الآلية للبيانات. وقد اختلفت الدول في اختيار الطريقة التشريعية الأنسب للتعامل مع الجرائم الإلكترونية، حيث قامت بعض الدول بإدراج النصوص العقابية المتعلقة بالإجرام المعلوماتي ضمن قانون العقوبات التقليدي، في حين قامت دول أخرى بسن قوانين جنائية مستقلة تتعلق بالمعلوماتية، تُعرف بالقانون الجنائي التقني. [3]

تستمد الجرائم الإلكترونية شرعيتها من التشريعات الوطنية التي تركز على هذا النوع من الجرائم، حيث بذلت الأمم المتحدة والمجلس الأوروبي جهودًا كبيرة لإقناع الدول بتطوير تشريعات لمكافحة الجرائم الإلكترونية وتعزيز التعاون الدولي في هذا المجال. من الأمثلة على ذلك، التوصية رقم R89 9 الصادرة عن

---

[1]–سعيد علي نعيم اليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج الخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012، ص 33

[2]–القطاونة مصعب، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني، 2010، الأردن ،ص27

[3]–القطاونة مصعب، المرجع السابق، ص 28

المجلس الأوروبي بشأن الجرائم المرتبطة بالحاسب الآلي، بالإضافة إلى الاتفاقية الخاصة بالإجرام المعلوماتي أو السيبيري، والتي تم توقيعها في نوفمبر 2001 في بودابست ودخلت حيز التنفيذ في يوليو 2004. وقد صادقت بعض الدول على هذه الاتفاقية مثل كندا واليابان والولايات المتحدة الأمريكية وجنوب أفريقيا، مما جعل منها وثيقة دولية ملزمة للدول الأطراف. [1]

ومع ذلك، واجه المشرع العديد من التحديات عند محاولة تنظيم مجال الحماية الجنائية ضد جرائم الإنترنت. من أبرز هذه التحديات كان التساؤل حول إمكانية تطبيق النصوص التقليدية على هذا النوع الجديد من الجرائم، وما إذا كان ذلك يشكل انتهاكًا لمبدأ الشرعية الجنائية. ففي حال تم تطبيق النصوص القديمة على الجرائم الإلكترونية، قد يؤدي ذلك إلى تفسير خاطئ وغير ملائم لهذه الجرائم وفقًا لمبادئ القانون الجنائي، مما قد يؤدي إلى تداخل أو تعارض في تفسير النصوص وتطبيقها بشكل غير دقيق.

وللاجابة على هذا الاشكال ظهر اختلاف المشرعين بين ضرورة وضع نصوص جديدة خاصة بالجرائم الالكترونية وبين تكييف النصوص القديمة مع هذه الجرائم الحديثة بتقنية متطورة، والبعض الآخر يقول أن في ذلك اخلالا بالبنيان القانوني، حيث ان المشرع يتطلب في الجرائم التقليدية سلوكا محددا وتتحقق مع الركن المادي للجريمة تختلف عن سلوكات المطلوبة في الجرائم الالكترونية . [2]

وهناك من يقول ان الجرائم الالكترونية ما هي الا جرائم عادية ترتكب بواسطة الحاسب الآلي، فالمطلوب من المشرع توقيع العقاب على ارتكاب هذه الجرائم بنصوص تقليدية، وعلى المشرع فقط الالمام بمصطلحات تقنية حتى لا يتم المساس بجريمة تبادل المعارف والحفاظ على الحق في احترام الحياة الخاصة .

مما يطرح اشكاليتين هما :

أولا: إشكالية الموقع.

اين يمكن ادماج النصوص القانونية الجديدة في قانون العقوبات التقليدي؟ ام في قانون خاص هناك من يقول بإمكانية ادماجها في جرائم الأموال باعتبار انه يمكن إضفاء صفة المال على الكيانات المادية والمعنوية للحاسوب، والبعض الآخر يفضل ادماجها في اطار الجزء الخاص بالجرائم ضد الملكية باعتبار الكيان المادي للحاسوب عناصر مادية قابلة للتملك، كما ان الكيان المعنوي يدخل في اطار الملكية الفكرية،

[1] إبراهيم خالد ممدوح الجرائم المعلوماتية، دار الفكر الجامعي، طاء الإسكندرية، 2009، ص 77.

[2] قورة نائلة عادل ، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط1، بيروت، 2012، ص 178

وهناك من يرى إضافة جزء اخر خاص بالجرائم الالكترونية مستقل عن الأجزاء التقليدية باعتبار ان هذه الجرائم تتعلق بقيمة اقتصادية جديدة لها طابع خاص. [1]

هناك اتجاه ثالث يرى ان الحاق كل جريمة الكترونية بما يقابلها في قانون العقوبات التقليدي مثلا: وضع جريمة التزوير المعلوماتي في باب المحررات الاعتداء على المعطيات يلحق بالاتلاف... الخ. [2]

ثانيا : إشكالية المصطلحات.

نظرا لما تتميز به الجريمة الالكترونية من طابع تقني، فانها تطرح إشكالية المصطلحات التقنية نظرا لغموض مفهومها باعتبارها مصطلح غريب عن لغة القانون بالنسبة للاشكالية التي يطرحها الركن الشرعي للجريمة الالكترونية يختلف موقف التشريعات في تحديد تعريف المصطلحات التقنية في الدول الانجلوسكسونية التي تعتمد على طريقة إعطاء التعريفات في صلب القانون، اما الطريقة الفرنسية توكل مهمة تحديد المعاني المصطلحات التقنية للقضاء وهي الطريقة المفضلة نظرا لسرعة تطور تقنيات الاعلام الآلي وإمكانية مواكبة القانون الجنائي لهذا التطور. [3]

بدأت المحاولة في فرنسا سنة 1985 حين تقدم وزير العدل بمشروع قانون العقوبات الجديد أضاف الى الكتاب الثالث منه بابا رابعا بعنوان " الجرائم الالكترونية مكونا من ثماني مواد 01 /307الى 307/08 والتي كانت تجرم التقاط البرامج أو المعطيات أو أي عنصر من النظام المعلوماتي عمدا واستخدام او انتاج برنامج او معطيات او أي عنصر من النظام الالكتروني وبدون موافقة من لهم الحق عليه، وتخريب أو تعييب كل جزء من نظام المعالجة الآلية للمعطيات، وكذلك عرقلته لأدائه كوظيفة المشروع لنظام المعالجة الآلية للمعطيات ولكن هذا المشروع ظل حبيس الادراج ولم يرى النور .[4]

وفي 05 أوت 1986 تقدم الى الجمعية الوطنية الفرنسية النائب مع بعض النواب من أعضاء حزب التجمع من أجل الجمهورية باقتراح مشروع قانون الغش المعلوماتي، وكان هذا الإقتراح مجرد تعديل وتطويع

[1]–مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات –ماهيتها، صورها، الجهود الدولية لمكافحتها– –دراسة مقارنة–، ط1، دار الخلدونية، الجزائر، 2018،ص151.

[2]–عقيقي كامل عفيفي، جرائم الكمبيوتر، دار النهضة العربية، القاهرة، 2010، ص 76

[3]–الجبور محمد الوسيط في قانون العقوبات القسم العام، دار وائل، ط1، عمان، 2012، ص 159.

[4]–معاشي سميرة، ماهية الجريمة الالكترونية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة الجزائر 2011، ص 280.

بعض الجرائم التقليدية مثل السرقة والنصب والاحتيال وخيانة الأمانة والاخفاء والتخريب والاتلاف والتزوير واستعمال المحررات المزورة . [1]

ولكن عندما نظر البرلمان الفرنسي لهذا الإقتراح، دارت حوله مناقشات طويلة ومعمقة وأدخلت عليه تعديلات جوهرية وتم اقراره في شكل جديد يختلف عن شكله الأول الذي قدم به، بحيث اقترب من الاقتراح الذي سبق الإشارة اليه في مشروع قانون العقوبات السنة 1985، وكان ذلك في 22/12/1987 وأصبح قانونا منذ 05/01/1988 بشأن الغش المعلوماتي .

وأدمج هذا القانون في قانون العقوبات الفرنسي، وأصبح يشكل بابا جديدا هو الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات والمتعلق بالجنايات والجنح المتعلقة بالاشخاص والجرائم الالكترونية، حيث يعالج الباب الأول الجنايات والجنح ضد الأشخاص، ويعالج الباب الثاني الجرائم الالكترونية . [2]

يحتوي هذا الباب على المواد من 462/2 الى 462/9 ويجرم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه، وشدد عقوبة تلك الجريمة في حالة محو او تعديل المعطيات الموجودة فيه أو طرق معالجتها أو نقلها سواء تم ذلك بطريقة مباشرة أو غير مباشرة، ويجرم كل من عرقل أو افسد عمدا او بدون مراعاة لحقوق الغير أداء النظام لوظيفته، كما يجرم تزوير المستندات المعالجة آليا أيا كان شكلها، وكذلك استعمال تلك المستندات ويجرم أخيرا الشروع في ارتكاب الجرائم السابقة، وكذلك الاتفاق الجنائي على ارتكابها . [3]

والمشرع الفرنسي قد فصل بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات وبين جريمتي تزوير المستندات المعالجة اليا واستعمالها، ويلاحظ على نصوص السابقة كذلك تجريم كل الاعتداءات على نظام المعالجة اليا واستعمالها .

ففي الكتاب الثالث من هذا القانون الجنايات والجنح ضد الأموال، وفي القسم الثاني من هذا الكتاب وفي الاعتداءات الأخرى على الأموال يعالج الباب الأول منه الاخفاء والجرائم الأخرى المشابهة أو القريبة منه، ويخصص الباب الثاني للإتلاف والتخريب، أما الباب الثالث، فقد كرسه المشرع للإعتداءات على الأنظمة المعالجة للمعطيات .

---

[1]–الزيدي وليد، القرصنة على الانترنت والحاسوب، دار أسامة للنشر، ط3، عمان، 2009، ص 54 .

[2]–هادي زيادة، آليات التعاون الدولي في مكافحة الجريمة السيبيرانية، مذكرة ماستر في القانون العام تخصص قانون جنائي و علوم جنائية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2022–2023،ص30.

[3]–الزبيدي وليد، المرجع السابق،ص55.

أما جريمتا تزوير المستندات المعالجة آليا واستعمالها فقد اختفوا من الباب الثالث المذكور لأن المشرع رأى أن المصلحة المحمية فيهما الثقة العامة، وليس نظام المعالجة الآلية للمعطيات، وأضافهما الى جريمة التزوير العادية بعد تطويع نصوصها بما يتلاءم وتلك المستندات، حيث نصت المادة 441/1 قانون العقوبات الفرنسي الجديد في باب التزوير على تجريم كل تغيير للحقيقة مكتوب في محرر أو أي دعامة أخرى تحتوي على الأفكار . [1]

وخصص المشرع الجزائري قسما خاصا للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهو القسم السابع مكرر بمحتوى المادة 394 مكرر الى 394 مكرر 7 بمقتضى القانون رقم 04-15 المؤرخ في 10/11/2004 ولم يكتف المشرع المذكور بذلك بل فرض حماية جنائية للحياة الخاصة للأفراد من خلال القانون 06 /23 المؤرخ في 2006/12/20حيث جاء بالمواد 303 و 303 مكرر إلى 303 مكرر 03، وهذا تصديا للاستخدام السيء لوسائل التكنولوجيا الحديثة. [2]

الفرع الثاني:

الركن المادي للجريمة الإلكترونية

حيث نتناول في الفرع أولا الركن المادي ثم تناول الركن المعنوي .

أولا: الركن المادي للجريمة الإلكترونية.

لابد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما في داخل الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما ملا يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طريق جهاز الكمبيوتر، وهذا لا يسبب إشكال، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها ، وهذا ما يدعو للتدخل التشريعي . [3]

---

[1] قاسم محمد عبد الله، الحماية الجنائية للمعلومات الالكترونية، ط1، دار الكتب القانونية، مصر،2010،ص148.

[2] القرانون رقم 06/23 المؤرخ في 20/12/2006 والذي من المادة 303 واقراره بالمادة 303 مكرر إلى 303 مكرر 03، وهذا تصديا للاستخدام السيء لوسائل التكنولوجيا الحديثة.

[3] –محمد حزيط مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة للنشر، ط3، الجزائر، 2008، ص 44

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها، مثال: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل.

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب مثال : جريمة الغش المعلوماتي الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية . [1]

ثانيا : الركن المعنوي للجريمة الإلكترونية.

يقوم الركن المعنوي للجريمة الإلكترونية على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجريمة المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة الجرمية من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالآثار الضارة الناشئة عنه .

يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به بعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي .

وفي جريمة الإحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع.[2]

يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين هما العلم والإرادة .

-**العلم** : هو إدراك الفاعل الأمور .

[1]-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، 2006،ص53.

[2]-خالد ممدوح الجريمة الالكترونية، الدار الجامعية الجديدة، الإسكندرية، 2008، ص 41.

-أما **الإرادة** : فهي اتجاه السلوك الإجرامي لتحقيق النتيجة، وطبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخاصا القصد الجنائي العام هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود ارتكاب الفعل، أما القصد الجنائي الخاص فهو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة، بل يذهب إلى التأكد من تحقق النتيجة مثال في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه، وعليه ما هو القصد الجنائي الذي يجب توافره في الجريمة الإلكترونية الأصل إن الفاعل في الجريمة الإلكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتقاء علمه كركن للقصد الجنائي العام[1] .

إذا فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص مثال: جرائم تشويه السمعة عبر الإنترنت، وجرائم نشر الفيروسات عبر الشبكة .

وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي ويرى الباحث أن القصد العام والخاص في الجريمة الإلكترونية هو أساسي لتحديد المسؤولية الجزائية، والذي يحدد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونية الإضرار أو النية الخاصة للجاني والتي يمكن استشفائها من مكونات كل جريمة على حدا وبشكل مستقل، وبالتالي فإن الجريمة الإلكترونية وكجريمة مستحدثة هي كغيرها من الجرائم التقليدية يشترط فيها وجود الركن المعنوي لقيام الجريمة ولا يتصور قيام أي نوع من أنواع الجرائم المعلوماتية دون وجود الركن المعنوي ، أما عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات وتمحيصها بما لها من صلاحية ، باعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها .[2]

[1]-شمسان ناجي، صالح، الجرائم المستخدمة بطريقة غير مشروعة لشبكة الإنترنت، دار النهضة العربية، القاهرة، مصر ،2009،ص44.

[2]-المرجع نفسه، ص45.

خلاصة الفصل:

تناولنا في هذا الفصل الإطار المفاهيمي للجرائم السيبرانية، كما بينا في تعريف الجريمة السبيرانية لغويا و قانونيا ثم ادرجنا اهم الخصائص العامة التي تميزها عن غيرها من الجرائم، كطابعها غير المادي، وامتدادها عبر الحدود، وصعوبة كشفها وإثباتها. كما أبرز التحديات القانونية التي فرضتها هذه الجرائم على المنظومة التشريعية، خاصة ما يتعلق بمبدأ الشرعية الجنائية، والتكييف القانوني الدقيق لأفعال إجرامية تتم في الفضاء الرقمي. وأخيرًا، ألقى الفصل الضوء على كيفية تعامل المشرع الجزائري مع هذه الظاهرة من خلال استحداث نصوص قانونية خاصة تضمن الحد الأدنى من الحماية القانونية في مواجهة الجرائم السيبرانية.

الفصل الثاني:

جهود القوانين المقارنة في مكافحة الجرائم السيبرانية

الفصل الثاني: جهود القوانين المقارنة في مكافحة الجرائم السيبيرانية

أضحت الجريمة السيبرانية من أخطر التهديدات العابرة للحدود في العصر الرقمي، نتيجة للاعتماد المتزايد على تكنولوجيا المعلومات في كافة مجالات الحياة. فقد أتاحت البيئة الرقمية للمجرمين إمكانيات هائلة لتنفيذ أفعال إجرامية معقدة، وبأدوات يصعب تتبعها أو ضبطها بالوسائل التقليدية. وفي ظل هذا الواقع المتغير، وجدت الدول نفسها مضطرة لتطوير آليات قانونية ومؤسساتية تواكب طبيعة هذه التهديدات الجديدة.

ولم تعد الاستجابات الوطنية كافية لوحدها، بل أصبح التعاون الدولي ضرورة ملحة من أجل تبادل المعلومات، وتوحيد الجهود التقنية والقانونية، وتعزيز القدرات البشرية لمواجهة هذه الظاهرة، وفي هذا الفصل نتناول بعمق مختلف الجهود الوطنية والدولية المبذولة لمكافحة الجرائم السيبرانية، مركّزًا على الأطر القانونية والأدوات الإجرائية، وأوجه التعاون الفني بين الدول، مع إبراز حالة الجزائر كنموذج في هذا السياق.و عليه تم تقسيم هذا الفصل إلى :

- **المبحث الأول: آليات مكافحة الجرائم السيبرانية في التشريع الجزائري**
- **المبحث الثاني: جهود القوانين المقارنة في مكافحة الجرائم السيبرانية**

المبحث الأول:

آليات مكافحة الجرائم السيبرانية في التشريع الجزائري

شهد العالم تطورًا متسارعًا في استخدام تكنولوجيا المعلومات، مما أفرز أنماطًا جديدة من الجرائم عُرفت بالجرائم السيبرانية، هذا الواقع فرض على المشرّع الجزائري ضرورة الإستجابة بتشريعات وآليات فعالة لمكافحة هذه الظاهرة المستحدثة، وفي هذا الإطار، جاء هذا المبحث لتسليط الضوء على الإطار القانوني والتنظيمي الذي اعتمده المشرّع لمواجهة هذه الجرائم. وذلك من خلال استعراض أهم الآليات التي أقرها القانون الوطني في هذا المجال، من خلال المطلب الأول التدابير الوقائية من الجرائم السيبيرانية في ظل القانون 09-04 ثم المطلب الثاني العقوبات المقررة للجرائم السيبرانية.

المطلب الاول:

التدابير الإجرائية من الجرائم السيبرانية في ظل قانون 09-04

كخطوة تنظيمية جديدة، بادر المشرع الجزائري إلى إصدار القانون رقم 09-04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها. ورغم صدور هذا الإطار القانوني، إلا أن تجسيد مضامينه على أرض الواقع لا يزال محدودًا، ويرجع ذلك بالأساس إلى ضعف الإهتمام بالجوانب التقنية الضرورية لتصنيف هذا النوع من الجرائم، وتحديد العقوبات المناسبة لمرتكبيها، إذ غالبًا ما تقتصر العقوبات المقررة على الغرامات المالية فقط .[1]

غير أن القانون وضع مجموعة من التدابير الوقائية والإجرائية لمواجهة هذه الجرائم والحد من انتشارها، حيث تناول هذا المطلب في فرعين الفرع الأول التدابير الوقائية، أما في الفرع الثاني تناول فيه أهم الهيئات التي تقوم بمتابعة هذا النوع من الجرائم.

الفرع الأول:

التدابير الوقائية

تعتبر التدابير الوقائية والإجرائية من الركائز الأساسية في مكافحة الجرائم السيبرانية، حيث تهدف إلى الحد من وقوع هذه الجرائم والتعامل معها بفعالية عند حدوثها، وتتضمن هذه التدابير استراتيجيات وقائية تمنع الهجمات السيبرانية قبل وقوعها، بالإضافة إلى إجراءات قانونية تتخذ لملاحقة مرتكبي هذه الجرائم، كما

[1]-القانون رقم 09-04، السالف الذكر.

يكتسب هذا المجال أهمية متزايدة في ظل التوسع الرقمي، مما يفرض على الأنظمة القانونية تكثيف الجهود لمواكبة التحديات المستمرة في هذا المجال، بحيث تناول الفرع في مجمله العناصر التالية:

أولا : التدابير الوقائية : وتتمثل في:

وتتمثل في :

1 .المراقبة الإلكترونية.

تُعدّ المراقبة الإلكترونية أحد التدابير الإستباقية الجوهرية التي تستهدف رصد التهديدات الرقمية قبل وقوع الجرائم السيبرانية، مما يعزز قدرة الدولة على التدخل السريع والفعّال. وقد منح المشرع الجزائري هذا الإجراء مكانة خاصة في القانون رقم 09-04، نظرًا لدوره الحيوي في تتبع النشاطات الإجرامية داخل الفضاء السيبراني، وفقًا للمادة 04 من القانون، لا يمكن اللجوء إلى المراقبة الإلكترونية إلا في حالات محددة وحرجة، كالأفعال ذات الطابع الإرهابي، التخريبي، أو ما يمس بأمن الدولة وسلامة مؤسساتها الحيوية، أو في حالة وجود تهديد وشيك لمنظومات معلوماتية حساسة كالمؤسسات المالية، الدفاعية، أو الصحية. [1]

وتُمارس هذه المراقبة بإذن مكتوب وصريح من السلطة القضائية المختصة، مما يضمن احترام مبدأ الشرعية وحماية الحقوق الدستورية للمواطنين، لا سيما الحق في الخصوصية. وتشمل آليات المراقبة تتبع البريد الإلكتروني، رسائل المحادثة، زيارات المواقع، تحميل الملفات، تحديد المواقع الجغرافية عبر IP ، وتحليل أنماط التصفح، وتعتمد الجهات الأمنية في ذلك على تقنيات متطورة منها برمجيات التحليل الجنائي الرقمي وأنظمة مراقبة الشبكات(IDS/IPS) ، مما يسمح بتتبع المشتبه فيهم، واكتشاف سلوكيات مشبوهة، وجمع الأدلة الرقمية القابلة للإستغلال القضائي.

كما يمكن توسيع نطاق المراقبة الإلكترونية في إطار إتفاقيات التعاون القضائي الدولي (مثل اتفاقية بودابست حول الجرائم السيبرانية)، ما يسمح بتبادل المعلومات الاستخباراتية بشأن أنشطة إلكترونية مشتبه بها عبر الحدود، خاصة وأن الفضاء السيبراني لا يعترف بالحدود الجغرافية. يُعزز ذلك من قدرة الجزائر على مجابهة التهديدات الخارجية التي تستهدف بنيتها الرقمية الوطنية. [2]

[1]-مهدي رضا، الجرائم السيبيرانية وآليات مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث والدراسات، المجلد 06، العدد 02، جامعة محمد بوضياف ، المسيلة ، الجزائر، 2021، ص118.

[2]-حسين ربيعي ، اليات البحث والتحقيق في الجرائم المعلوماتية ، أطروحة دكتوراه في العلوم تخصص قانون العقوبات ، جامعة باتنة 1، الجزائر ، 2015-2016، ص62.

2 .إشراك مزودي الخدمات في الوقاية من الجريمة السيبرانية.

جاء القانون رقم 09-04 بمقاربة حديثة تؤسس لتعاون وثيق بين الدولة والقطاع الخاص، لا سيما مزودي خدمات الإنترنت والاتصالات، باعتبارهم طرفًا أساسيًا في ضبط وتنظيم حركة البيانات الرقمية. وقد ورد هذا الدور بوضوح في المادتين 11 و12 من القانون، حيث فُرضت على هؤلاء المزودين مجموعة من الالتزامات الجوهرية التي تهدف إلى تيسير عمل الأجهزة الأمنية والقضائية في التحقيق والوقاية. [1]

يُلزم القانون المزودين بتسجيل بيانات التعريف التقني للمستخدمين، وتشمل: عنوان الـIP ، توقيت الاتصال، مدة الجلسة، نوعية الجهاز المستخدم، ونوعية الخدمة. وتحتفظ هذه البيانات في سجلات محمية لفترة زمنية محددة، مع إمكانية تقديمها للسلطات عند الطلب، بعد الحصول على إذن قضائي، كما يُمنع عليهم حذف أو تعديل هذه البيانات دون ترخيص قانوني، ضمانًا لسلامة الأدلة الرقمية.

ومن جهة أخرى، يُفرض على المزودين التدخل الفوري لحذف أو حجب المحتويات الرقمية غير المشروعة، مثل: منشورات العنف، الدعوات الإرهابية، التحريض على الكراهية العرقية أو الدينية، والاستغلال الجنسي للأطفال. ويحدث ذلك عبر بلاغات ترسلها الهيئات الأمنية المختصة إلى المزودين، وهم مطالبون بالتنفيذ في آجال قصيرة لتفادي انتشار المحتوى أو تكراره عبر منصات أخرى. [2]

ويمثل هذا التعاون أحد مظاهر "الأمن السيبراني التشاركي"، الذي يعزز مناعة الفضاء الرقمي الجزائري، ويجعل من القطاع الخاص شريكًا فعّالًا في محاربة التهديدات الإلكترونية، لا مجرد فاعل اقتصادي محايد.

3 .حماية بيانات حركة السير المعلوماتية.

تمثل بيانات حركة السير المعلوماتية قاعدة بيانات تقنية بالغة الأهمية في إطار مكافحة الجرائم السيبرانية، وهي تتعلق بجميع المعطيات التي تولدها الاتصالات الرقمية خلال نشاط المستخدم على الإنترنت، وتشمل هذه البيانات، مصدر الاتصال، وجهته، توقيته، مساره، مدة الجلسة، حجم البيانات، ونوع الخدمة المستعملة (تحميل، بث، تصفح، إلخ).

وقد نصت المادة الأولى من القانون 09-04 على أهمية هذه البيانات بوصفها أدلة رقمية قابلة للاستغلال في سياق التحقيقات الإلكترونية. وتكمن القيمة القانونية لهذه البيانات في كونها تمثل "بصمة

[1]-المادة 11و 12 من القانون 09-04 المؤرخ في 05 اوت 2099 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا المعلومات.

[2]-مهدي رضا، المرجع السابق ، ص119.

رقمية" يمكن من خلالها إعادة بناء التسلسل الزمني والمنطقي للأحداث التي سبقت أو رافقت الجريمة. على سبيل المثال، يمكن عبر تحليل إثبات دخول غير شرعي إلى نظام معلوماتي، أو تحديد الجهة التي أرسلت رسائل خبيثة أو برمجيات تجسسية. [1]

بموجب هذا القانون، يُلزم مقدمو خدمات الإنترنت بجمع هذه البيانات فور حدوث الاتصال، وتخزينها بطريقة محمية ضد الفقدان أو التعديل، كما يجب أن تتوفر شروط الأمن المعلوماتي المناسبة لتفادي تسرب البيانات أو اختراقها. يُمنع أيضًا محو هذه المعطيات قبل انتهاء المدة القانونية للاحتفاظ بها، والتي تحددها السلطات التنظيمية المختصة.

وتُستخدم بيانات حركة السير أيضًا في إطار التعاون مع أجهزة إنفاذ القانون الدولية، لتحديد مواقع الجناة الذين يستخدمون VPN أو خوادم بروكسي لإخفاء هويتهم، مما يُمكّن من تتبع مسار الجريمة حتى وإن تم تنفيذها عبر دول متعددة.[2]

ثانيا: التدابير الإجرائية لمكافحة الجريمة السيبرانية في القانون الجزائري

تُعد التدابير الإجرائية من الأدوات الجوهرية التي يستعين بها القضاء والسلطات المختصة لضمان التحقيق الفعال في الجرائم السيبرانية، وتمثل هذه التدابير مجموعة من الإجراءات القانونية والتقنية التي تهدف إلى جمع الأدلة الرقمية، حماية النظم المعلوماتية، وتأمين سلاسة التعاون القضائي الوطني والدولي، وقد خصص المشرع الجزائري ضمن القانون 09-04 عدة مواد قانونية تُنظم هذه التدابير وتحدد آليات تنفيذها. وفيما يلي أهمها:

أ- تفتيش وحجز المنظومات المعلوماتية.

يشكل تفتيش المنظومة المعلوماتية وحجز المعطيات الرقمية أحد أبرز الإجراءات الإجرائية في مجال مكافحة الجريمة السيبرانية، حيث يسمح للسلطات القضائية بالوصول إلى الأدلة الإلكترونية التي غالبًا ما تكون مخزنة ضمن أجهزة الحواسيب أو الخوادم أو في البيئات السحابية.

[1]-المادة 01 من القانون 09-04 ، السابق الذكر.

[2]-معاشي سميرة، ماهية الجريمة الالكترونية، بحث منشور في مجلة المنتدى القانوني، العدد الاسبع، دامعة محمد خيضر، بسكرة، الجزائر، ، ص280.

نصت المادة 3 من القانون 09-04 على إمكانية القيام بالتفتيش وحجز نظم المعلومات عندما تقتضي ضرورة حماية النظام العام أو في إطار التحقيقات القضائية، ويشمل ذلك مراقبة الاتصالات الإلكترونية، تجميع وتسجيل محتواها في الزمن الحقيقي.[1]

كما أجاز المشرع وفق المادة 6 اللجوء إلى التفتيش عن بُعد، سواء كان ذلك لمنظومة معلوماتية كاملة أو لجزء منها، بما في ذلك المعطيات المخزنة في خدمات التخزين السحابي أو خوادم موجودة خارج النطاق الجغرافي للدولة، شريطة أن تكون هذه المعطيات مرتبطة بجريمة تمس الأمن الوطني أو المصالح العليا للدولة[2].

وتنص المادة 7 من نفس القانون على أن عملية الحجز قد تواجه تحديات تقنية، لا سيما في حالة أنظمة محمية أو موزعة، ما يستوجب على السلطات المختصة استخدام تقنيات رقمية متقدمة لمنع الوصول غير المصرح به إلى المعطيات أو نسخها. وتُخوّل الجهات المخولة أن تستعين بأشخاص ذوي خبرة تقنية في مجال نظم المعلومات، لتقديم الدعم الفني وتوفير المعلومات الضرورية لإنجاح عملية التفتيش وضمان سلامة الدليل الرقمي. [3]

ب- تمديد الاختصاص القضائي.

استجابةً لطبيعة الجريمة السيبرانية التي لا تعترف بالحدود الجغرافية، منح المشرع الجزائري اختصاصًا موسعًا للمحاكم الوطنية في النظر في الجرائم الإلكترونية المرتكبة خارج التراب الوطني، متى ما استهدفت هذه الأفعال مؤسسات الدولة الجزائرية أو مصالحها الاقتصادية أو دفاعها الوطني. [4]

ويستند هذا التمديد إلى مبدأ حماية المصلحة الوطنية العليا، إذ تُخوّل المحاكم الجزائرية صلاحية المتابعة والمتابعة القضائية ضد أي أجنبي ارتكب فعلاً مجرّمًا بموجب القانون الجزائري، طالما أن الفعل له آثار ضارة على الأمن القومي أو الاقتصاد الوطني، حتى وإن كان موقع الجريمة خارج الجزائر.

---

[1]-المادة 03 من القانون 09-04 ، السابق الذكر.

[2]المادة 06 من القانون 09-04 ، السابق الذكر.

[3]-سعيداني نعيم، اليات البحث و التحري عن الجريمة المعلوماتية ، مذكرة ماجستير في العلوم القانونية ، جامعة الحاج لخصر، باتنة، الجزائر، 2012-2013، 43.

[4]-عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، مجلة معالم للدراسات القانونية و السياسية ، المجلد 04، العدد01، جامعة يحي فارس، المدية، الجزائر، 2020، ص200.

ج- التعاون القضائي الدولي

نظراً للطبيعة العابرة للحدود للجرائم السيبرانية، أتاح القانون إمكانية تبادل المساعدة القضائية الدولية في مجالات التحري، التحقيق، وتحصيل الأدلة الإلكترونية.

كما يمكن للجزائر، بموجب الاتفاقيات الثنائية أو المتعددة الأطراف، أو حتى على أساس مبدأ المعاملة بالمثل، أن تطلب أو تستجيب لطلبات المساعدة القضائية التي تتعلق بجمع الأدلة الرقمية أو اتخاذ إجراءات تحفظية، مثل تجميد الحسابات الإلكترونية، حجز الخوادم، أو حجب محتويات رقمية ذات طابع إجرامي، ويشمل هذا التعاون تبادل المعلومات الاستخباراتية، التنسيق بشأن توقيت تنفيذ العمليات الإلكترونية، وتوفير الأدلة الرقمية بصيغ معترف بها قضائيًا وفقًا للمعايير الدولية. [1]

د- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

كجزء من الهيكل المؤسساتي لمكافحة الجريمة السيبرانية، تم استحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بموجب القانون 09-04، وهي تمثل هيئة إدارية ذات طابع مستقل، بحيث أعيد تنظيم هذه الهيئة بموجب المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، حيث تم تحديد مقرها في العاصمة الجزائرية مع إمكانية نقله بموجب مرسوم رئاسي. [2]

كما تتمتع الهيئة بالشخصية المعنوية والاستقلال المالي، وتخضع مباشرة لسلطة رئيس الجمهورية، وتتكون من مجلس توجيه ومديرية عامة، وهي مكلفة باقتراح السياسات الوطنية في مجال الوقاية من الجرائم الإلكترونية، التنسيق مع مختلف الجهات الأمنية، التقنية، والقضائية، ومتابعة التقدم التكنولوجي لضمان جاهزية الدولة لمواجهة أي تهديد رقمي.

كما تقدم الهيئة تقارير دورية عن نشاطاتها إلى رئيس الجمهورية، وتعمل على رصد ومتابعة تطور الجريمة السيبرانية محليًا ودوليًا، وإعداد الدراسات المتعلقة بالجرائم المستجدة وتقديم التوصيات للتعديل التشريعي عند الضرورة.[3]

---

[1]-مهدي رضا، المرجع السابق ، ص119.

[2]-مرسوم رئاسي رقم 20-183 مؤرخ في 13 يوليو 2020 (21 ذي القعدة 1441 هـ) يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد نُشر هذا المرسوم في الجريدة الرسمية للجمهورية الجزائرية بتاريخ 11 يوليو 2020، ص 12.

[3]-عبد الصديق شيخ، المرجع السابق، ص200.

الفرع الثاني:

الهيئات المتخصصة في البحث والتحري عن الجرائم السيبيرانية

يتزايد التهديد السيبراني تزامنًا مع التطور المتسارع في التكنولوجيا واعتماد المجتمعات الحديثة بشكل واسع على الأنظمة الرقمية في مختلف القطاعات. وقد أدى هذا الاعتماد المتزايد إلى بروز الجرائم السيبرانية كأحد أبرز التحديات التي تهدد الأمن الوطني للدول، مما فرض ضرورة استحداث هيئات متخصصة في البحث والتحري لمواجهة هذا النوع من الجرائم.

تلعب هذه الهيئات دورًا محوريًا في كشف وتتبع الأنشطة غير القانونية التي تستهدف الأفراد، المؤسسات، والبنى التحتية الحيوية، من خلال الاستفادة من أحدث التقنيات وتسخير كفاءات بشرية مؤهلة. وتسعى الدول عبر هذه الهيئات إلى تعزيز قدراتها الدفاعية في الفضاء السيبراني، بما يضمن حماية الأمن القومي واستقرار الفضاء الرقمي[1]. في هذا الفرع، سيتم التطرق إلى أهمية ودور الهيئات المتخصصة في مكافحة الجرائم السيبرانية، مع التركيز على الإطار القانوني والتنظيمي الذي يضبط عمل هذه الهيئات.

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

قام المشرّع الجزائري بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك بموجب القانون رقم 09-04 المؤرخ في 14 أغسطس 2004، والمتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد نصت المادة 13 من هذا القانون على استحداث هذه الهيئة باعتبارها أداة مركزية في جهود الدولة للتصدي للجرائم السيبرانية. [2]

أُنشئت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب القانون رقم 09-04، الذي خوّل التنظيم مهمة تحديد تشكيلتها، تنظيمها، وكيفية سير عملها، وذلك حسب ما نصّت عليه المادة 13 من نفس القانون.

وفي هذا الإطار، صدر المرسوم الرئاسي رقم 19-172، الذي ألغى المرسوم الرئاسي السابق رقم 15-261،[3] حيث نصّ على أن الهيئة تُعدّ مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية

[1]-عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري، ،دار بلقيس ، 2015 ص 91.

[2]-المادة 13 من القانون 09-04 السابق الذكر.

[3]-مرسوم رئاسي رقم 15-261 مؤرخ في 2015/10/08، تعدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم. المتصلة بتكنولوجيات الاعلام والاتصال والمكافحة الجريدة الرسمية، العدد 53 الصادرة بتاريخ 2015/10/08.

والاستقلالية المالية، وتخضع لوصاية وزارة الدفاع الوطني. ويُعد هذا التنظيم تجسيدًا لرؤية المشرع في إضفاء الطابع المؤسساتي على مكافحة الجرائم السيبرانية، ضمن هيكل إداري واضح وفعال. [1]

من حيث التشكيلة والتنظيم، نصّت المادة 4 من المرسوم الرئاسي 19-172 على أن الهيئة تتكوّن من هيئتين أساسيتين :مجلس التوجيه والمديرية العامة .يترأس مجلس التوجيه وزير الدفاع الوطني أو من يمثله. ويضم ممثلين عن عدة وزارات استراتيجية هي: [2]

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

أما بخصوص سير عمل الهيئة، فقد حدّدت المادة 7 من نفس المرسوم آلية انعقاد مجلس التوجيه، حيث يجتمع في دورتين عاديتين سنويًا بناءً على استدعاء من رئيسه، كما يمكنه الانعقاد في دورات غير عادية كلما اقتضت الحاجة، إما بمبادرة من رئيس المجلس أو بطلب من أحد أعضائه أو المدير العام للهيئة. [3]

وفيما يتعلق بمهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإنها تمارس صلاحياتها المنصوص عليها في المادة 14 من القانون رقم 09-04، وذلك تحت إشراف ورقابة السلطة القضائية، ووفقًا لأحكام قانون الإجراءات الجزائية. وتتمثل أبرز مهام الهيئة في الآتي: [4]

1. تقديم الدعم والمساعدة للسلطات القضائية ومصالح الشرطة القضائية، لا سيما في إطار التحريات المتعلقة بالجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، بما يشمل جمع المعلومات وإجراء الخبرات القضائية ذات الصلة.
2. التعاون الدولي، من خلال تبادل المعلومات مع الهيئات النظيرة في الخارج، بهدف جمع المعطيات التي من شأنها المساعدة في التعرف على مرتكبي الجرائم السيبرانية وتحديد أماكن تواجدهم.

---

[1]-مرسوم رئاسي رقم 19-172 مؤرخ في 06-06-2019 يجدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها و تنظيمها وكيفيات سيرها جريدة رسمية رقم 37 لسنة 2019.

[2]-المادة 4 من المرسوم الرئاسي 19-172، المرجع السابق .

[3]-المادة 7 من المرسوم الرئاسي 19-172، المرجع السابق.

[4]-المادة 14 من القانون رقم 04-09، المرجع السابق.

ولتحديد مهام الهيئة بشكل أكثر تفصيلًا، نص المرسوم الرئاسي رقم 19-172 على توزيع هذه المهام بين مجلس التوجيه والمديرية العامة للهيئة، وذلك من خلال المواد6، 9، 11، 13و14 من المرسوم، التي توضح بدقة صلاحيات كل جهاز داخلي. [1]

ثانيا: الوحدات التابعة لسلك الأمن الوطني والقيادة العامة للدرك الوطني.

تجسيدًا لالتزام الدولة الجزائرية بمكافحة الجريمة الإلكترونية، عمد المشرع إلى إصدار حزمة من النصوص القانونية التي أسندت مهمة الوقاية والمكافحة إلى عدد من الهياكل الأمنية المتخصصة. وفي هذا السياق، ظهرت وحدات تابعة لكل من سلك الأمن الوطني والقيادة العامة للدرك الوطني، تضطلع بدور محوري في التصدي للجرائم السيبرانية، سواء من حيث التحري أو التحقيق أو التحليل الفني.

1- مركز الوقاية من الجرائم في الإعلام الآلي والجرائم المعلوماتية التابع للدرك الوطني.

تم إنشاء مركز الوقاية من الجرائم في الإعلام الآلي والجرائم المعلوماتية سنة 2008، ويُعد الجهة الوحيدة المتخصصة على المستوى الوطني في تأمين منظومة المعلومات. يضطلع المركز بمهمة أساسية تتمثل في حماية الأنظمة المعلوماتية بما يخدم الأمن العام، كما يقوم بدور مركز توثيق وتحليل، ويتخذ من بئر مراد رايس مقرًا له ، يعمل المركز على تحليل البيانات والمعطيات المتعلقة بالجرائم المعلوماتية، بهدف تحديد هوية مرتكبي هذه الأفعال سواء كانوا أفرادًا أم جماعات منظمة، ويأتي هذا في إطار تعزيز أمن وسلامة الأنظمة المعلوماتية، لا سيما تلك المستخدمة في المؤسسات الرسمية، والقطاعات الحساسة مثل البنوك والمرافق الحيوية وحتى المنازل، كما يسهم المركز في دعم وتنسيق جهود باقي الأجهزة الأمنية، من خلال تقديم الدعم الفني والتحليلي اللازم، مما يعزز فعالية التصدي للجريمة المعلوماتية. [2]

وقد نجحت قيادة الدرك الوطني، عبر برامج التكوين المستمر والمشاركة في ملتقيات وطنية ودولية، إضافة إلى تبادل الخبرات مع دول أخرى، في تكوين نخبة من الكفاءات تجمع بين الاختصاص القانوني والتقني، على غرار مهندسي الإعلام الآلي وخبراء في القانون، بهدف الإلمام العميق بخصوصيات الجرائم المعلوماتية وأساليب مكافحتها.

وفي هذا السياق، تمكن المركز من معالجة عدد كبير من القضايا المرتبطة بالجرائم الإلكترونية والرقمية، بما في ذلك تلك المرتكبة عبر وسائل التواصل الاجتماعي، أو المرتبطة باختراق المواقع الإلكترونية

[1]-المواد6، 9، 11، 13و14 من المرسوم الرئاسي رقم 19-172 ، المرجع السابق.

[2]-عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، قيادة الدرك الوطني، مداخلة بالملتقى الوطني حول : الجريمة المعلوماتية بين الوقاية والمكافحة جامعة محمد خيضر بسكرة 16 نوفمبر 1015 ، ص 30.

الرسمية للمؤسسات العمومية والخاصة. وتُبرز هذه المعالجة المستمرة أهمية الدور الذي يضطلع به المركز في حماية البنية التحتية المعلوماتية الوطنية، والتصدي لأي محاولات تستهدف أنظمة المعالجة الآلية للمعطيات. [1]

2- المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع للدرك الوطني.

يُعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، أنشئ بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004 [2].ويُعد هذا المعهد هيئة علمية وتقنية تُسند إليها مهام ذات طابع تحليلي وتطبيقي، مدعومة بأحدث التقنيات والتكنولوجيات، ويُشكّل أداة فعّالة في خدمة العدالة ودعم وحدات التحري التابعة للشرطة القضائية، ويُكلف المعهد بعدة مهام رئيسية، من بينها:

- إجراء الخبرات العلمية والتقنية، التي تُستخدم كأدلة في توجيه التحقيقات القضائية بطلب من القضاة، بهدف كشف الحقيقة وتحديد هوية مرتكبي الجنايات والجنح اعتمادًا على الأدلة العلمية.
- مساعدة المحققين خلال عمليات المعاينة والتحقيق، عبر وضع مختصين مؤهلين تحت تصرف الجهات المعنية عند الضرورة.
- المبادرة بإجراء بحوث علمية متعلقة بالإجرام، من خلال الاعتماد على التكنولوجيات الدقيقة والمتقدمة.
- المساهمة في تطوير البحوث التطبيقية، وتحسين أساليب التحري التي أثبتت فعاليتها في مجال علم الإجرام والأدلة الجنائية، سواء على المستوى الوطني أو الدولي. [3]

3- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني.

تُعد المصلحة المركزية لمكافحة الجريمة المعلوماتية إحدى أهم الهياكل المستحدثة في إطار تطوير آليات مواجهة الجرائم الإلكترونية، وقد جاءت استجابة لتزايد التهديدات المرتبطة بالأمن السيبراني وضرورة توفير حماية فعالة للفضاء الرقمي. بدأت هذه الجهود من خلال تكوين فصيلة متخصصة داخل المديرية الشرطية القضائية، والتي شكلت اللبنة الأولى لبناء قدرات وطنية في مجال مكافحة الجريمة الإلكترونية. ومع

[1]-عز الدين عز الدين ، المرجع نفسه ، ص .30.

[2]-مرسوم رئاسي رقم 04-183 ، المؤرخ في 26 يونيو سنة 2004 بتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية 41 ، الصادرة في 27/06/2004.

[3]-امام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، 2026،ص44.

تطور الحاجة إلى التكيف مع التهديدات المتزايدة، تم في سنة 2011 تعزيز هذا التوجه ضمن الهيكل التنظيمي للمديرية العامة للأمن الوطني. [1]

وفي جانفي 2015، صدر قرار من المدير العام للأمن الوطني بإنشاء المصلحة المركزية لمحاربة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ضمن الهيكل التنظيمي للمديرية الشرطية القضائية. ويُعبر هذا القرار عن التزام الدولة بتعزيز منظومة الأمن السيبراني، وتوفير الوسائل البشرية والتقنية الضرورية لمواجهة هذا النوع من الجرائم المستجدة.

ثالثا: الهيئات القضائية المختصة بالفصل في الجرائم الإلكترونية.

لقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000، والذي ارتكز على ثلاثة محاور رئيسية :تعزيز حقوق الإنسان، تسهيل الولوج إلى القضاء، وإعادة الاعتبار لمنظومة التكوين والتأهيل القضائي، في إحداث تحولات عميقة على مستوى المنظومة القضائية الوطنية. وقد تجلت هذه الإصلاحات من خلال تعديل واستحداث تشريعات جديدة تتماشى مع التزامات الجزائر الدولية، وتستجيب لمتطلبات العصر وتحدياته، لاسيما في ظل تصاعد التهديدات الإجرامية العابرة للحدود. [2]

ومن أبرز ما خلصت إليه توصيات لجنة إصلاح العدالة، ضرورة تعديل قانون العقوبات وقانون الإجراءات الجزائية، من أجل مواجهة الأنماط الجديدة من الإجرام، وفي مقدمتها الجرائم التقنية والمعلوماتية، التي باتت تُهدد خصوصية الأفراد وأمن المجتمعات واقتصادات الدول، خصوصًا مع لجوء الجماعات الإرهابية والمنظمات الإجرامية إلى استغلال الفضاء السيبراني في تنفيذ مخططاتها، مستفيدة من طبيعة الجريمة الإلكترونية وصعوبة تعقب مرتكبيها.

واستجابة لهذا التحدي، اتجه المشرع الجزائري، على غرار بعض التشريعات المقارنة وعلى رأسها المشرع الفرنسي، إلى استحداث أقطاب جزائية متخصصة، وهي محاكم ذات اختصاص إقليمي موسع، وذلك بموجب القانون رقم 14-04 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون الإجراءات الجزائية. ويهدف هذا القانون إلى تمكين بعض المحاكم، ووكلاء الجمهورية، وقضاة التحقيق، من اختصاص نوعي في معالجة جرائم محددة بدقة، تُصنّف على أنها جرائم خطيرة ومعقدة ومنظمة، مثل: [3]

[1]-عز الدين عز الدين ، المرجع السابق ، ص41.

[2]-كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الاكاديمية للبحث القانوني، المجلد 11، العدد 01، 2015، ص17.

[3]-القانون رقم 04 - 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 - 155 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004.

- جرائم المخدرات.
- الجريمة المنظمة العابرة للحدود الوطنية.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (الجرائم الإلكترونية).
- جرائم تبييض الأموال.
- الجرائم الإرهابية والتخريبية.
- جرائم مخالفة التشريع والتنظيم الخاص بالصرف.

وفي هذا السياق، صدر المرسوم التنفيذي رقم 16-280 المؤرخ في 02 نوفمبر 2016، المعدل والمكمل للمرسوم التنفيذي رقم 08-04 المؤرخ في 19 جانفي 2008، والمتعلق بالقانون الأساسي الخاص بالموظفين المنتمين للأسلاك المشتركة في المؤسسات والإدارات العمومية[1]. وقد تم بموجب هذا المرسوم توسيع الاختصاص الإقليمي للأقطاب الجزائية المتخصصة عبر التراب الوطني، لتشمل أربع محاكم رئيسية:

1. محكمة سيدي أمحمد (الجزائر العاصمة)، وتضم ضمن اختصاصها الإقليمي المجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة، وبومرداس.
2. محكمة قسنطينة، ويشمل اختصاصها: قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، خنشلة، سوق أهراس، وميلة.
3. محكمة ورقلة، ويمتد نطاقها إلى: ورقلة، أدرار، تمنراست، إيليزي، بسكرة، الوادي، وغرداية.
4. محكمة وهران، وتشمل المجالس القضائية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تموشنت، وغليزان.

وبذلك، يغطي كل قطب جزائي مجموعة من المجالس القضائية ضمن منطقة جهوية محددة (شمال، جنوب، شرق، غرب)، حيث تتمركز الخبرات البشرية والتقنية اللازمة لمواجهة الجرائم المعقدة، كما

[1]-المرسوم التنفيذي رقم 16-280 المؤرخ في 02-11-2016 المعدل والمتمم للمرسوم التنفيذي رقم 08-04 المؤرخ في 19-01-2008المتضمن القانون الاساسي الخاص بالموظفين المنتمين للأسلاك المشتركة في المؤسسات والإدارات العمومية الجريد الرسمية العدد 66، الصادر بتاريخ 09/11/2016.

تم دعم هذه الأقطاب بآليات التحري الخاصة لمواجهة الجريمة المنظمة، بما في ذلك الجريمة المعلوماتية، عبر اعتماد الوسائل العلمية والتقنية التي تتيح ملاحقة هذه الجرائم وتقديم مرتكبيها للعدالة. [1]

المطلب الثاني:

العقوبات المقررة للجرائم السيبرانية

بالرجوع إلى المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري، يتضح أن المشرع قد شدد على تجريم كافة صور الاعتداء على الأنظمة المعلوماتية، سواء تم ذلك من خلال الدخول أو البقاء غير المشروع في هذه الأنظمة، أو عن طريق التعديل أو الحذف أو الإدخال الاحتيالي للبيانات

وتتمثل هذه الأفعال في حذف المعطيات المعلوماتية أو تغييرها عن حالتها الأصلية، دون اعتبار لطبيعتها أو قيمتها الاقتصادية أو التقنية، مما يدل على حرص المشرع على حماية البنية الرقمية ذاتها، لا فقط مضمونها. وتشمل الأفعال المعاقب عليها كذلك إدخال فيروسات أو برمجيات خبيثة أو بيانات غير مصرح بها بهدف الإضرار بالنظام أو إفشاء أسرار الغير أو عرقلة العمل.

كما يعاقب القانون على تصميم أو تطوير أدوات وبيانات أو برامج مخصصة للقرصنة، حتى وإن لم تُستعمل فعليًا، مما يعكس توجهًا احترازيًا في مواجهة التهديدات السيبرانية. وتزداد العقوبات شدةً في حال استهداف أنظمة حساسة كأنظمة الدفاع الوطني أو المؤسسات العمومية، غير أن الملاحظ أن هذه العقوبات، رغم تعددها وتنوعها بين عقوبات أصلية وأخرى تكميلية، لا تزال في نظر العديد من المختصين تفتقر إلى الطابع الردعي الكافي، نظرًا لعدم تناسبها أحيانًا مع الضرر المادي والمعنوي الجسيم الذي قد تتسبب فيه مثل هذه الجرائم، سواء للأفراد أو للهيئات العامة، وعليه سنتطرق في هذا المطلب الى العقوبات الاصلية للجرائم السيبيرانية في الفرع الأول ثم العقوبات التكميلية للجرائم السيبيرانية في الفرع الثاني .

الفرع الأول :

العقوبات الاصلية للجرائم السيبيرانية

أدرك المشرع الجزائري منذ العقدين الأخيرين خطورة الجرائم المعلوماتية التي أصبحت تشكل تهديدًا مباشرًا لأمن الأفراد والمؤسسات والدولة ككل، لذلك سعى إلى تقنين نصوص جزائية واضحة ضمن قانون العقوبات لمعالجة هذا النوع المستحدث من الإجرام.

[1]–امام غازي، المرجع السابق،ص44.

أولًا: معاقبة الدخول الاحتيالي إلى المنظومات المعلوماتية.

تنص المادة 394 مكرر من قانون العقوبات الجزائري (المعدّلة بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004) على ما يلي[1]: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من خمسين ألف (50.000 دج) إلى مائتي ألف (200.000 دج) دج، كل من يدخل أو يبقى، عن طريق الغش، في كل أو جزء من نظام المعالجة الآلية للمعطيات، أو يحاول ذلك".

هذا النص يكرّس الطابع الردعي تجاه من يحاول اختراق الأنظمة الإلكترونية بطرق غير مشروعة، حتى في حال عدم إحداث أي ضرر مادي، إذ يكفي مجرد الدخول أو محاولة الدخول "بطريقة احتيالية" لقيام الجريمة/ ويُفهم من ذلك أن الجريمة تتحقق بمجرد : [2]

- الدخول غير المشروع إلى النظام المعلوماتي (سواء من داخل المؤسسة أو من خارجها).
- أو البقاء فيه دون وجه حق (حتى لو دخل بدايةً بتصريح مشروع).
- أو محاولة ذلك، وهو ما يشكل سابقة قانونية لأن المشرّع هنا يعاقب على مجرد "المحاولة" دون وقوع النتيجة.

ثانيًا: تشديد العقوبة عند إقتران الفعل بضرر فعلي.

تضمنت الفقرتان الثانية والأخيرة من المادة نفسها حالات مشددة ترتفع فيها العقوبة تلقائيًا إلى الضعف، وذلك في الحالات التالية: [3]

- إذا أدى الدخول غير المشروع إلى حذف أو تغيير المعطيات المخزنة داخل النظام.
- إذا نجم عن الفعل تخريب أو تعطيل جزئي أو كلي لنظام التشغيل أو وظائف النظام المعلوماتي.

في هذه الحالة، تصبح العقوبة:

- الحبس من ستة أشهر إلى سنتين.

---

[1]-القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات. جريدة الرسمية رقم 71 المؤرخة سنة 2004.

[2]-لاكلي نادية، المرجع السابق، ص268.

[3]-أحمد حليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، مصر، 2006، ص14.

- وغرامة تتراوح بين 200.000دج إلى 500.000 دج.

ويُفهم من هذا التشديد أن المشرع الجزائري يراعي جسامة الأثر المترتب على الجريمة، إذ لا يعامل من دخل فقط مثل من قام بتغيير أو تخريب البيانات.

ثالثًا: العقوبات المقررة على الشخص المعنوي.

في خطوة مواكبة للتطورات التشريعية الدولية، أخذ المشرع الجزائري بمبدأ المسؤولية الجنائية للشخص المعنوي، حيث نصت المادة 394 مكرر 4 على ما يلي: [1]

"يعاقب الشخص المعنوي، عندما تثبت مسؤوليته عن الجرائم المنصوص عليها في هذا القسم، بغرامة مالية تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة على الشخص الطبيعي". [2]

وهذا يعني أن:

- الغرامة المفروضة على الشخص المعنوي يمكن أن تصل إلى مليون دينار جزائري (1.000.000 دج).
- وتطبق عليه أيضًا العقوبات التكميلية الواردة في المواد الخاصة بالأشخاص المعنويين (وسنفصلها في الفرع التالي).

ويهدف هذا التوجه إلى تجريم الأفعال المرتكبة باسم الشركات أو المؤسسات الخاصة أو العامة، لا سيما إذا استُخدمت بنيتها التحتية لارتكاب الجريمة، أو كانت هي المستفيدة من نتائجها.

رابعًا: العقوبات الواردة في القانون 18-07 المتعلق بحماية المعطيات الشخصية.

يُعد قانون 18-07 المؤرخ في 10 جوان 2018 من أبرز القوانين التي تسير جنبًا إلى جنب مع قانون العقوبات لمواجهة الجريمة المعلوماتية، وقد خصص مواد لحماية المعطيات ذات الطابع الشخصي. تنص المادة 46 من القانون على ما يلي: [3]

---

[1]-جمال براهيمي، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون و العلوم السياسية kالمجلد 11k العدد02، جامعة مولود معمري، تيزي وزو، الجزائر، دت ،ص128.

[2]-امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، 102.

[3]-القانون 18/07 المؤرخ في 10/05/2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34 المؤرخة في 10/05/2018

"يعاقب كل من يخالف أحكام المادة 2 من هذا القانون، المتعلقة بضرورة التصريح المسبق أو الحصول على ترخيص من السلطة المختصة قبل معالجة المعطيات الشخصية، بالحبس من سنتين (2) إلى خمس سنوات (5)، وبغرامة من 200.000دج إلى 500.000 دج".

وتعتبر هذه العقوبة من العقوبات الأصلية المشددة نظرًا لحساسية المعلومات الشخصية، مثل:

- البيانات الصحية.
- السجلات البنكية.
- المواقع الجغرافية للأفراد.
- المعطيات البيومترية.

وفي حال ارتكاب هذه الجريمة من قبل شخص معنوي (مثل شركة أو مؤسسة مالية)، فيُطبق عليه نفس الغرامات مضاعفة، مع إمكانية تطبيق العقوبات التكميلية كحل الشركة أو تعليق نشاطها[1].

الفرع الثاني:
العقوبات التكميلية للجرائم السيبيرانية

إلى جانب العقوبات الأصلية التي ينص عليها قانون العقوبات الجزائري لمعاقبة مرتكبي الجرائم المعلوماتية، أفرد المشرّع جملة من العقوبات التكميلية التي تهدف إلى تعزيز الردع العام والخاص، ومضاعفة آثار العقوبة بغرض منع تكرار مثل هذه الجرائم، لا سيما وأن الجرائم الإلكترونية تتسم بالمرونة التقنية وسرعة الانتشار وصعوبة التتبع.

أولًا: العقوبات التكميلية في حق الأشخاص الطبيعيين.

تتضمن العقوبات التكميلية المنصوص عليها في المادة 394 مكرر 6 من قانون العقوبات الجزائري[2] عددًا من التدابير الخاصة بالأشخاص الطبيعيين، وتتمثل في:

- **مصادرة الأدوات والوسائل المستعملة** في ارتكاب الجريمة المعلوماتية، وتشمل:

[1]–تومي يحي الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18/07، دراسة تحليلية مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2019، ص114.

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

- الحواسيب.
- البرمجيات.
- وسائط التخزين.
- أي أجهزة تقنية أخرى وظّفها الجاني لتنفيذ الجريمة.

- **غلق المواقع الإلكترونية** أو التطبيقات أو المنصات التي كانت محلًّا للجريمة أو وسيلةً في ارتكابها، إذا ثبت استخدامها في تنفيذ أفعال إجرامية مثل الاختراق أو نشر بيانات محمية أو محتويات غير قانونية.

- **غلق الأماكن التي تم فيها ارتكاب الجريمة بعلم مالكها**، كغلق مقهى إنترنت ارتُكبت فيه الجريمة مع علم صاحبه، ويهدف هذا الإجراء إلى تحميل أصحاب الأماكن مسؤولية الرقابة والتأمين، ومنعهم من التهاون في مواجهة الجرائم المعلوماتية. [1]

ثانيًا: العقوبات التكميلية في حق الأشخاص المعنويين.

يولي القانون الجزائري اهتمامًا خاصًا بمسؤولية الأشخاص المعنويين (الشركات، المؤسسات، الجمعيات...)، إذ خصهم المشرّع بجملة من العقوبات التكميلية التي نصت عليها المادة 18 مكرر من قانون العقوبات، وتتمثل في[2]:

1. حلّ الشخص المعنوي :أي إنهاء وجوده القانوني في حال ثبوت تورطه في جريمة معلوماتية.
2. غلق المؤسسة أو فرع منها لمدة لا تتجاوز خمس سنوات.
3. الإقصاء من الصفقات العمومية لمدة أقصاها خمس سنوات.
4. المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية، سواء بشكل مباشر أو غير مباشر، نهائيًا أو مؤقتًا، بحد أقصى خمس سنوات.
5. مصادرة الوسائل المستعملة أو الناتجة عن الجريمة.

[1]–طباش عز الدين، "حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي"، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 56، العدد 1، 2019،ص213.

[2]–لاكلي نادية، المرجع السابق ،ص 269

6. نشر وتعليق حكم الإدانة في أماكن علنية، وذلك لردع المؤسسة وجعلها عبرة.

7. الوضع تحت الحراسة القضائية، والتي قد تمتد إلى خمس سنوات، وتشمل تقييد النشاط الذي أدّى إلى ارتكاب الجريمة.

هذه التدابير تهدف إلى منع المؤسسات المتورطة من الاستمرار في أنشطة قد تسهّل وقوع الجرائم الإلكترونية، وضمان الرقابة على نشاطها مستقبلاً.

وفضلاً عن العقوبات، اهتم المشرع الجزائري بـ الإجراءات الوقائية الاستباقية، والتي نص عليها القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ومن أبرز هذه التدابير: [1]

1. **مراقبة الاتصالات الإلكترونية** :حيث نصّت المادة 3 على إمكانية مراقبة وتسجيل محتوى الاتصالات الإلكترونية "حال وقوعها"، وذلك لحماية النظام العام أو لأغراض التحقيقات القضائية، كما يجب أن تتم هذه المراقبة بإذن كتابي من السلطة القضائية المختصة من خلال المادة 4.

2. **دخول الأجهزة الأمنية إلى المنظومات المعلوماتية** من خلال المادة 5 خولت لضباط الشرطة القضائية والسلطات القضائية المختصة الدخول إلى منظومات معلوماتية لأغراض التفتيش، كما أجازت المادة 6 حجز البيانات المخزنة التي تساعد في الوصول إلى هوية الجاني أو تفاصيل الجريمة.

3. **إشراك مزوّدي خدمات الإنترنت في الوقاية** حيث أوجب القانون على مزودي الخدمات الإلكترونية التعاون مع السلطات الأمنية، وذلك من خلال:

- حفظ البيانات والمعطيات الإلكترونية.
- السحب الفوري للمحتويات غير القانونية.
- وضع ترتيبات تقنية لمنع الوصول إلى المحتوى المخالف للنظام العام أو الآداب العامة. [2]

[1]-المادة 05 و 06 من القانون رقم 09-04 السابق الذكر .

[2]-لاكلي نادية ، المرجع السابق،ص270.

المبحث الثاني:

جهود القوانين المقارنة في مكافحة الجرائم السيبرانية

تعد الجرائم السيبرانية من التحديات العالمية التي تتطلب تنسيقاً دولياً لمواجهتها بفعالية، نظراً لطابعها العابِر للحدود. وقد عملت العديد من المنظمات الدولية والدول على وضع أطر قانونية وتعاونية لمكافحة هذه الجرائم وحماية الأمن السيبراني،يشمل هذا المبحث استعراضاً للجهود الدولية التي تهدف إلى تعزيز التعاون بين الدول لمكافحة هذه الجرائم وضمان الأمن الرقمي على مستوى العالم، وتضمن هذا المبحث مواجهة الجريمة السيبيرانية على المستوى الدولي كمطلب أول ثم مجالات التعاون لمكافحة الجريمة السيبيرانية كمطلب ثاني .

المطلب الأول:

مواجهة الجريمة السيبيرانية على المستوى الدولي

لقد أدى التسارع المتزايد في وتيرة التقدم التكنولوجي، إلى جانب بروز الفضاء الإلكتروني، إلى إحداث ثورة رقمية شاملة مست جميع مناحي الحياة، وأصبح من الصعب، إن لم يكن من المستحيل الاستغناء عن الخدمات التي توفرها هذه التكنولوجيا المتطورة. إلا أن هذه التقنيات، على الرغم من مزاياها العديدة، قد فتحت المجال لاستغلالها في أنشطة غير مشروعة من قبل بعض الأفراد والجماعات. [1]

وإذ يتميز الفضاء السيبراني بغياب الحدود الجغرافية وعدم خضوعه لمبدأ السيادة التقليدية للدول، فقد أصبح من العسير إخضاعه لمنظومة قانونية واحدة تتكفل بها دولة بمفردها، لمواجهة هذا النمط الجديد من الجرائم. وهو ما يجعل من الضروري تطوير الإطار التشريعي الدولي بما يتماشى مع طبيعة هذه الظواهر الإجرامية الحديثة، والتي تتسم بالتعقيد والتطور المستمر.

وفي هذا السياق، تبرز الحاجة الملحة إلى استحداث آليات فعالة للتعاون الدولي، سواء من خلال ترقية وتحديث الأدوات التقليدية القائمة أو إنشاء أطر جديدة أكثر كفاءة، بما يسمح بمواكبة التطور السريع الذي تعرفه الجرائم الإلكترونية، وتعزيز قدرات الدول والمجتمع الدولي على التصدي لها ومكافحتها بشكل مشترك وفعّال[2]. وهذا ما سنعالجه من خلال الفرعين التاليين.

---

[1]-قرران مصطفى، زرقين عبد القادر الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن العدد 02 جامعة خميس مليانة الجزائر ، 2022، ص 125.

[2]–قرران مصطفى، زرقين عبد القادر ، المرجع السابق، ص 125.

الفرع الأول:

دور الأمم المتحدة في مواجهة الجريمة الإلكترونية

منظمة الأمم المتحدة منذ وقت مبكر إلى معالجة آثار التقدم التكنولوجي على الحقوق والحريات الأساسية، وخاصة في مجال حماية الحياة الخاصة .وقد تُوجت هذه الجهود في المؤتمر الدولي الأول لحقوق الإنسان المنعقد بطهران عام 1968، والذي ركّز على العلاقة بين التكنولوجيا الحديثة وحقوق الإنسان. وقد اعتمدت الجمعية العامة للأمم المتحدة توصيات المؤتمر، والتي اعتبرت أن الحواسيب الإلكترونية تُعد من أخطر أدوات المراقبة والتجسس، خصوصًا عند استخدامها في تخزين وتحليل البيانات الشخصية، لما تشكله من تهديد مباشر للخصوصية والحرية الفردية من خلال الكشف عن أنماط التعامل والعلاقات الخاصة بالأفراد.

وفي هذا السياق، تبذل الأمم المتحدة جهودًا كبيرة في مواجهة الجرائم المعلوماتية، مؤكدة على ضرورة تعزيز التعاون الدولي بين الدول الأعضاء لمواجهة هذه الظاهرة المتنامية. وقد تناولت عدة مؤتمرات أممية هذه القضية بشكل خاص، من أبرزها: [1]

- المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية المنعقد في الدوحة (قطر) من 12 إلى 19 أبريل 2015، والذي ركّز على إدماج العدالة الجنائية في السياسات العامة وتعزيز سيادة القانون على الصعيدين الوطني والدولي. وقد تبنّت الجمعية العامة في قرارها رقم 67/184، ضرورة عقد ورشات عمل تعالج الأنماط الجديدة من الجريمة، بما في ذلك الجريمة السيبرانية.
- المؤتمر الثاني عشر الذي انعقد بالبرازيل في الفترة من 12 إلى 19 أبريل 2010، تحت شعار : "استراتيجيات شاملة لتحديات عالمية: نظم منع الجريمة والعدالة الجنائية في عالم متغير"، وقد خُصص جزء من جدول أعماله لموضوع جرائم الإنترنت .ودعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع مفتوح للخبراء الحكوميين لدراسة الجريمة الإلكترونية وتدابير مواجهتها.

أولاً: أبرز قرارات وتوصيات الجمعية العامة للأمم المتحدة.

1. القرار رقم 121/45 لسنة 1990، تلاه إصدار دليل منع الجرائم المعلوماتية ومكافحتها عام 1994.[2]

---

[1]–محمد امين شوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية ، ط01، دار الثقافة للنشر والتوزيع، الأردن، 2009،ص73.

[2]–فاروق خلف، الاليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات ، العدد02، كلية الحقوق ، جامعة ، جامعة حمه لخضر ، الوادي ، الجزائر، 2015، ص08.

2. القرار رقم 63/55) 2000 (والقرار (2001) 56/121حول مكافحة إساءة استخدام تكنولوجيا المعلومات، حيث دعَت الجمعية العامة الدول الأعضاء إلى الاسترشاد بأعمال لجنة منع الجريمة عند صياغة تشريعاتها الوطنية ذات الصلة.

3. القرار 239/57 (2003)و والقرار 199/58 (2004)، اللذان أكدا على ضرورة بناء ثقافة عالمية للأمن السيبراني، ودعوة الدول لتعزيز التعاون في هذا المجال.

4. قرار لجنة مكافحة المخدرات 5/48 بشأن تعزيز التعاون الدولي لمنع استغلال الإنترنت في ارتكاب الجرائم المرتبطة بالمخدرات.

5. توصيات الهيئة الدولية لمراقبة المخدرات (INCB) لسنة 2005، التي دعت للحد من بيع الأدوية الخاضعة للرقابة بطريقة غير مشروعة عبر الإنترنت.

6. القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين (هافانا، 1990) [1]بشأن الجرائم المتصلة بالحاسوب، والذي شدد على ضرورة قيام الدول الأعضاء بـ:

   - ضمان فعالية تطبيق التشريعات القائمة على سلطات التحقيق والإثبات.
   - إدخال تعديلات تشريعية عند الضرورة لتغطية الأفعال الإجرامية المستجدة.
   - تجريم إساءة استخدام الحاسوب والمعاقبة عليها.
   - تعزيز التعاون الدولي، خاصة في مجالات تسليم المجرمين والمساعدة القضائية.

كما أوصى المؤتمر بضرورة ملاءمة التشريعات الوطنية مع التطورات التقنية، بحيث تشمل الأشكال المستجدة من الإجرام السيبراني، واتخاذ تدابير فعّالة على المستويين الوطني والدولي.

ثانيًا: رؤية الأمم المتحدة المستقبلية لمكافحة الجريمة الإلكترونية: [2]

- وضع معايير دولية لحماية أمن المعالجة الآلية للبيانات.
- معالجة إشكالية الاختصاص القضائي في الجرائم العابرة للحدود.[3]

[1]–فاروق خلف، المرجع نفسه ، ص12.

[2]–ليندة شرابسة، السياسة الدولية و الإقليمية في مجال الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة الدراسات والأبحاث ، العدد 01، جامعة عاشور زيان، الجلفة ، الجزائر، 2009،ص244.

[3]–طرشي نورة، المرجع السابق، ص69.

- إبرام اتفاقيات دولية تنظم إجراءات التفتيش والضبط المعلوماتي، مع ضمان حماية الحقوق والحريات الفردية، واحترام سيادة الدول.

الفرع الثاني:

دور المجلس الأوروبي وجامعة الدول العربية في مواجهة الجريمة الإلكترونية

سنتناول هذا الفرع في قسمين كما يلي:

أولا: دور المجلس الأوروبي في مواجهة الجريمة الإلكترونية.

لعب المجلس الأوروبي دورًا محوريًا في التصدي للجريمة الإلكترونية، لا سيما في مجال حماية المعطيات الشخصية وصون الحياة الخاصة، وذلك نظرًا لكون الدول الأعضاء فيه من بين أكثر الدول تقدمًا في المجالين العلمي والتقني. هذا التقدم جعلها تدرك التهديدات الناشئة عن إساءة استخدام تكنولوجيا المعلومات، ومن ثم بادرت بوضع مجموعة من التوصيات وصياغة اتفاقيات دولية تهدف إلى حماية بنيتها الرقمية من أي انتهاكات.

تُعد اتفاقية بودابست (المعروفة أيضًا باتفاقية الجريمة السيبرانية) أبرز مساهمة للمجلس الأوروبي في هذا المجال، غير أن هذه الاتفاقية لم تكن نقطة البداية في الاهتمام بموضوع الجريمة الإلكترونية، بل جاءت تتويجًا لجهود سابقة تعود إلى منتصف السبعينات.

ففي عام 1976، نُوقش لأول مرة موضوع ارتباط الحاسوب بالجريمة خلال المؤتمر الثاني عشر لمديري معاهد البحث في علم الإجرام، المنعقد تحت إشراف المجلس الأوروبي. وفي عام 1983، نظّمت منظمة التعاون الاقتصادي والتنمية (OECD) اجتماعًا لدراسة سبل تطبيق قوانين الجريمة على المستوى الدولي فيما يخص الجرائم المعلوماتية. تلت ذلك جهود اللجنة الأوروبية المكلفة بدراسة هذه الجرائم بين 1985و1989، والتي انتهت بإصدار التوصية رقم 89، متضمنة توجيهات تشريعية للدول الأعضاء بشأن تجريم الأفعال المرتبطة بالجريمة المعلوماتية. [1]

وقد صنّفت هذه التوصية الأفعال الجرمية إلى مجموعتين:

- المجموعة الأولى (إلزامية) :وهي تشمل:
  - الاحتيال المعلوماتي؛

[1]–ليندة شرا بشة السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية – الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة الدراسات والأبحاث العدد 01، جامعة عاشور زبان الجلفة الجزائر ، 2009 ، ص 244.

- التزوير المعلوماتي؛
- الإتلاف العمدي للبيانات أو الأنظمة؛
- الاعتراض غير المشروع للأنظمة؛
- تعطيل وظائف النظم المعلوماتية؛
- الدخول غير المشروع للبرامج؛
- النسخ غير المصرّح به لتصاميم الرقائق الإلكترونية. [1]

- المجموعة الثانية (اختيارية) :وتضم:
  - التلاعب أو تعديل البيانات المخزنة؛
  - التجسس الإلكتروني؛
  - الاستخدام غير المصرح به للأنظمة أو البرامج؛
  - انتهاك الحقوق المرتبطة بالبرمجيات المحمية قانونًا.

وفي سياق تعزيز التنسيق الأوروبي لمواجهة هذه التهديدات، عقد المجلس الأوروبي في 11سبتمبر 1995 مؤتمرًا وزاريًا خصصه لمناقشة مسألة صياغة اتفاقية دولية لمكافحة الجرائم الإلكترونية، وهو ما أثمر لاحقًا عن إقرار اتفاقية بودابست في 23 نوفمبر 2001، والتي تبنتها لجنة وزراء المجلس الأوروبي في دورتها 109.

ثانيا: دور جامعة الدول العربية في مواجهة الجريمة الإلكترونية.

لم تكن المجتمعات العربية بمعزل عن التهديدات المتصاعدة للجريمة الإلكترونية، التي تتصف بطبيعتها العابرة للحدود الجغرافية والسيادية، بل باتت هذه الظاهرة تمثل تحديًا مشتركًا يفرض على الدول العربية تنسيق جهودها واتخاذ تدابير تشريعية وتنظيمية متكاملة لمواجهتها. ومن هذا المنطلق، عملت جامعة الدول العربية على تطوير منظومة قانونية مشتركة، تمثلت في إصدار القانون العربي النموذجي الاسترشادي

[1]–طرشي نورة مكافحة الجريمة المعلوماتية، رسالة ماجستير تخصص قانون جنائي، جامعة الجزائر 01 الجزائر 2011 – 2012، ص69.

لمكافحة الجرائم الإلكترونية، المعروف أيضًا بجرائم الحاسوب والإنترنت، والذي جاء نتيجة تعاون بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في إطار الأمانة العامة للجامعة. [1]

وقد سعت الجامعة منذ تأسيسها إلى تعزيز التعاون الأمني والقضائي بين الدول الأعضاء، خصوصًا في مجالات مكافحة الجريمة وتحقيق العدالة الجنائية، من خلال تنسيق السياسات الجنائية ووضع آليات قانونية فعالة لتنظيم هذا التعاون. كما كانت لجامعة الدول العربية مساهمة فاعلة في الجهود الدولية لمكافحة الجريمة المنظمة، حيث شاركت في صياغة اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (اتفاقية باليرمو)، من خلال تقديم مقترحات عملية في اجتماعات الخبراء الحكوميين. [2]

وفي خطوة مهمة، تم اعتماد مشروع قانون إماراتي كمصدر مرجعي لتطوير الإطار القانوني العربي الموحد لمكافحة الجرائم الإلكترونية، ليُعرف لاحقًا باسم "القانون العربي الاسترشادي". وقد تم إقرار هذا القانون النموذجي من قبل مجلس وزراء العدل العرب في دورته التاسعة عشرة بموجب القرار رقم 495 بتاريخ 8 أكتوبر 2003، ومن طرف مجلس وزراء الداخلية العرب في دورته الحادية والعشرين.

هذا القانون – الذي اقتُبس من التشريع الإماراتي – يحظر نسخ برامج الكمبيوتر دون إذن مسبق، ويعاقب مرتكبي قرصنة البرمجيات بموجب أحكام القانون المدني والجنائي، حيث تشمل العقوبات غرامات مالية، ومصادرة البرمجيات المخالفة، إضافة إلى عقوبة الحبس التي قد تصل إلى ثلاث سنوات[3].

كما نصت إحدى مواد القانون العربي الموحد على تجريم تزوير المستندات الإلكترونية أو البيانات المخزنة في وسائط إلكترونية مثل أقراص الحاسوب أو الأشرطة الممغنطة أو غيرها، معتبرًا ذلك من أشكال إساءة استخدام تكنولوجيا المعلومات[4].

ومن الجهود التشريعية الأخرى التي تبنتها جامعة الدول العربية، يبرز "القانون الجزائي العربي الموحد"، الذي أقره مجلس وزراء العدل العرب، حيث تضمن هذا القانون في الباب السابع (الجرائم ضد الأشخاص) فصلًا خاصًا حول الاعتداء على حقوق الأفراد الناتجة عن المعالجات المعلوماتية. وقد أشارت

---

[1]–برقوق يوسف، المساعدة القضائية المتبادلة لمواجهة الجرائم الالكترونية، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 01، العدد01،2021،ص100.

[2]–ليندة شرا بشة المرجع السابق، ، ص 244.

[3]–فريد ناشف اليات التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، جامعة بليدة 02 الجزائر2022، ص 445.

[4]–يوهرين فتيحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، مجلد 14، العدد 04، جامعة قسنطينة 02 الجزائر، 2021، ص 56.

المواد من 461 إلى 464 إلى ضرورة حماية الحياة الخاصة وسرية البيانات الشخصية، ونظّمت كيفية جمع البيانات الاسمية والاطلاع عليها، بالإضافة إلى تحديد العقوبات المقررة في حال ارتكاب تلك الجرائم.

أما في مجال حماية الملكية الفكرية، فقد تم إبرام الاتفاقية العربية لحماية حقوق المؤلف، والتي نصت صراحة على توفير الحماية القانونية لبرامج الحاسوب، كما دعت الدول الأعضاء إلى تطوير تشريعاتها العقابية لمواكبة تطور الجريمة الإلكترونية.

ورغم هذه المبادرات المهمة، إلا أن الملاحظ على الجهود العربية في هذا المجال أنها لا تزال تركز على معالجة الفراغ التشريعي العام، من خلال وضع أطر إرشادية ومبادئ توجيهية تتعلق بضوابط استخدام الإنترنت وأمن النظم المعلوماتية. وتضمنت هذه الجهود تحديد أنواع السلوكيات الإجرامية المحتملة عبر الشبكة، إضافة إلى مجموعة من تعليمات حماية المنشآت المعلوماتية، والبرمجيات، والإجراءات التنظيمية الخاصة بربط الإدارات الحكومية بالإنترنت.[1]

المطلب الثاني:

مجالات التعاون لمكافحة الجريمة السيبيرانية

تبذل الدول جهودًا متزايدة في شتى الميادين من أجل تكريس التعاون الدولي بشكل فعّال للحد من هذا النوع الخطير من الإجرام المستحدث. وفي هذا السياق، يندرج تعزيز التعاون الدولي لمكافحة الجريمة الإلكترونية ضمن بعدين أساسيين الأول يتمثل في التعاون القضائي والإجرائي الدولي، بالنظر إلى الطابع العابر للحدود الذي يميز هذا النوع من الجرائم، والثاني يتمثل في التعاون الفني الدولي، وذلك بالنظر إلى الطبيعة التقنية والفنية البالغة التعقيد للجريمة الإلكترونية، كما سنتناول في فرع ثالث موقف المشرّع الجزائري من آليات التعاون الدولي في هذا المجال، حيث سنتناول :

الفرع الأول :

مظاهر التعاون القضائي والإجرائي الدولي لمكافحة الجريمة الإلكترونية

أمام التحديات التقنية والطبيعة العابرة للحدود التي تميز الجريمة الإلكترونية، بات التعاون القضائي والإجرائي الدولي من الأسس الجوهرية التي لا غنى عنها لمواجهتها. وتجلّت مظاهر هذا التعاون في عدة أوجه رئيسية تمّ التأكيد عليها ضمن أبرز الاتفاقيات الدولية، لاسيما اتفاقية بودابست لمكافحة الجريمة

[1]–لصغير يوسف الجريمة المرتكبة عبر الأنترنت مذكرة لنيل شهادة ماجستير تخصص قانون دولي للأعمال، كلية الحقوق والعلوم سياسية، تيزي وزو الجزائر 2013، ص 101.

المعلوماتية (2001)، وكذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010)، ونبرز في هذا السياق ثلاث آليات رئيسية: [1]

1 .تبادل المعلومات.

يُعد تبادل المعلومات بين الدول عنصرًا وقائيًا محوريًا في جهود مكافحة الجريمة الإلكترونية. فوفقًا لاتفاقية بودابست، يُمكن للدول الأطراف إرسال المعلومات المرتبطة بالجرائم المعلوماتية دون طلب مسبق، وذلك إذا ما تبين أن لهذه المعلومات فائدة مباشرة في تسهيل التحقيقات أو الإجراءات القضائية في دولة أخرى طرف في الاتفاقية. ويُسمح للدولة الطرف أن تطلب من نظيرتها الكشف عن بيانات إلكترونية مخزنة على أنظمة معلوماتية واقعة ضمن إقليمها. كما أجازت الاتفاقية، دون الحاجة إلى إذن مسبق، الوصول إلى المعلومات الإلكترونية المتاحة للعموم والمخزنة في الفضاء الرقمي للدولة الأخرى. [2]

2 .المساعدة القضائية المتبادلة.

تعتبر المساعدة القانونية المتبادلة من أهم صور التعاون الدولي في المجال الجنائي، وقد أكّدت عليها الاتفاقيات الدولية بوضوح. فنصّت الاتفاقية العربية لعام 2010 على ضرورة أن تقدم الدول الأعضاء أقصى درجات التعاون والمساعدة المتبادلة فيما بينها في إطار التحقيقات والإجراءات ذات الصلة بالجرائم المعلوماتية. [3]

أما اتفاقية بودابست، فقد خصصت الفصل الثالث كاملاً لتحديد مبادئ المساعدة المتبادلة، مؤكدة على ضرورة إصدار الدول الأطراف تشريعات داخلية تمكّنها من تطبيق أحكام المواد من 27 إلى 35، التي تشمل كيفية طلب المساعدة، شروط الاستجابة، وآليات تسريع التعاون، خاصةً في الحالات العاجلة التي تتطلب تدخلاً فوريًا. ومن ثم، يصبح التعاون القضائي مسنودًا بتدابير قانونية وإجرائية على المستوى الوطني، ما يمنح فعالية أكبر في مكافحة هذه الجرائم المعقدة.

3 .تسليم المجرمين.

يُعرّف تسليم المجرمين بأنه إجراء قانوني يتم بموجبه نقل شخص محل متابعة أو محكوم عليه من دولة إلى أخرى، بناءً على طلب رسمي، وذلك لمحاكمته أو تنفيذ العقوبة. وقد أكد المؤتمر الدولي العاشر للقانون الجنائي المنعقد في روما سنة 1969 على أن هذا الإجراء يشكّل شكلًا من أشكال التعاون القضائي

[1]-يوهرين فتيحة ، المرجع السابق ، ص 56.

[2]–محمد أحمد سليمان عيسى التعاون الدولي المواجهة الجرائم الإلكترونية المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016، ص 50.

[3]–يوسف صغير، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، جامعة مولود معمري تيزي وزو، 2013، ص 133.

بين الدول. وفيما يتعلق بالجرائم الإلكترونية، فقد نصّت الاتفاقية العربية لعام 2010 على إمكانية تسليم المجرمين، شرط توفر مبدأ التجريم المزدوج (أي أن تكون الأفعال مجرّمة في كلا الدولتين). كما تناولت اتفاقية بودابست (المادة 24) تفاصيل التعاون في مجال تسليم الأشخاص المرتكبين لجرائم إلكترونية، وأكدت على أهمية توحيد القواعد المنظمة لعملية التسليم لضمان فعاليتها في ظل التطور التقني المتسارع لهذه الجرائم. [1]

أما فيما يخص التعاون الفني الدولي في مجال مكافحة الجريمة الإلكترونية لا يقتصر التعاون الدولي في مجال مكافحة الجريمة الإلكترونية على الجوانب القضائية والإجرائية البحتة، بل يتجاوزها ليشمل جانبًا بالغ الأهمية يتمثل في التعاون الفني والتقني، والذي يُعد ركيزة أساسية في دعم القدرات الوطنية للدول لمواجهة التحديات التقنية المتنامية لهذا النوع من الجرائم.

تتميز الجرائم الإلكترونية بكونها جرائم تقنية عالية التعقيد، تتطلب مستوىً متقدمًا من الكفاءة والمعرفة في مجالات التكنولوجيا الحديثة، وهو ما يجعل من الضروري تعزيز القدرات المؤسسية والبشرية للدول، خاصة تلك التي لا تمتلك البنى التحتية التقنية أو الخبرات البشرية المؤهلة بشكل كافٍ لمواكبة تطور أساليب ووسائل المجرمين السيبرانيين. [2]

من هذا المنطلق، أولت الاتفاقيات الدولية أهمية بالغة للتعاون الفني، حيث تضمنت العديد من النصوص التي تحث الدول على تبادل الخبرات، ونقل المعرفة التقنية، وتنمية المهارات ذات الصلة بإنفاذ القانون في المجال السيبراني. ففي اتفاقية بودابست لعام 2001، وهي الاتفاقية المرجعية الدولية في هذا المجال، نصت المادة 35 على ضرورة قيام الدول بإنشاء "نقطة اتصال وطنية" تعمل 24ساعة في اليوم و7 أيام في الأسبوع، لتوفير الاستجابة العاجلة والدعم الفني في حالات الجرائم الإلكترونية، سواء من حيث تقديم المشورة التقنية، أو التنسيق بين السلطات الوطنية والأجنبية المعنية بإنفاذ القانون.

وبالمثل، نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 في مادتها 43 على التزام الدول الأطراف بتعزيز التعاون الفني من خلال التدريب والتكوين المستمر، وتبادل التجارب والخبرات، بما يُسهم في تطوير كفاءات الموارد البشرية العاملة في المجال الأمني والقضائي، ورفع جاهزيتها في التعامل مع الجرائم المعلوماتية.

[1]–عادل عبد العال، إبراهيم الخراشي، مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة للنشر، 2015، ص 237.

[2]–عبد العال الدريبي، محمد صادق اسماعيل الجرائم الإلكترونية، دراسة قضائية قانونية مقارنة مع أحدث التشريعات العربية في مجال مكافحة الجريمة المعلوماتية والإنترنت المركز القومي للإصدارات القانونية، 2012، ص 155.

وتتجلى أهمية هذا التعاون الفني في عدة صور عملية، أبرزها:

1. تنظيم دورات تدريبية وورش عمل تقنية موجهة للقضاة وأعوان الضبطية القضائية، تهدف إلى تمكينهم من فهم الجوانب الفنية المعقدة للجرائم الإلكترونية، كتحليل الأدلة الرقمية، أو تعقب مصادر الهجمات السيبرانية، أو استرداد البيانات المحذوفة من الأجهزة الإلكترونية.
2. تبادل الخبرات بين الدول، من خلال إرسال بعثات تدريبية أو استقبال خبراء دوليين في الأمن السيبراني للمساعدة في تطوير المنظومات الوطنية، مما يسهم في سد فجوة التفاوت بين الدول من حيث القدرات الفنية.
3. تعزيز التعليم الأكاديمي والتقني المتخصص، سواء من خلال إدراج وحدات دراسية تتعلق بالأمن السيبراني في مناهج كليات الحقوق والشرطة، أو من خلال دعم الجامعات ومراكز البحث لتطوير برامج متخصصة في مكافحة الجرائم الإلكترونية.
4. إنشاء شبكات مهنية دولية تُسهّل تبادل المعلومات والممارسات الفضلى، مما يخلق منظومة استجابة جماعية فاعلة ومنسقة على المستوى الدولي .[1]

وعلاوة على ذلك، فإن الاستثمار في العنصر البشري يعتبر محورًا رئيسيًا في التعاون الفني، ذلك أن بناء قدرات الأفراد – خصوصًا القضاة، المحققين، ومهندسي الأدلة الجنائية الرقمية – يتطلب الاهتمام بمجموعة من العوامل، منها: المؤهلات الأكاديمية، الاستعداد الذهني والنفسي للتعامل مع الضغوط والسرعة التي تميز بيئة الجريمة الإلكترونية، فضلاً عن توفر الإمكانيات التقنية اللازمة للتدريب.

وليس من المبالغة القول إن التعاون الفني الدولي أصبح اليوم شرطًا لا غنى عنه في أي استراتيجية وطنية لمكافحة الجرائم الإلكترونية، حيث لم تعد المواجهة ممكنة بشكل فردي، بل تستلزم تكاملًا عالميًا وجهودًا منسقة مبنية على الثقة المتبادلة، وتبادل الدعم الفني والمعرفي المستمر[2].

الفرع الثاني:

موقف المشرّع الجزائري من التعاون الدولي في مكافحة الجريمة الإلكترونية.

أدرك المشرّع الجزائري في وقت مبكر التحديات التي تفرضها الجريمة الإلكترونية، ليس فقط من حيث آثارها على الأمن الداخلي والمجتمعي، بل أيضًا من حيث الطابع العابر للحدود الوطنية الذي يُميز هذا

[1]–ميرفت محمد جباية، مكافحة الجريمة الإلكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري العلمية، ص 315.

[2]–ميرفت محمد جباية، المرجع السابق، ص 315.

النوع من الجرائم، والذي يفرض ضرورة التعاون بين الدول لمواجهتها بفعالية. ويُعد القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أبرز تجليات هذا الوعي التشريعي، حيث تناوله في عدة عناصر .

أولاً: الإقرار بأهمية التعاون الدولي في المجال القضائي.

نص القانون 09-04 بوضوح على أهمية المساعدة القضائية الدولية في مجال التحقيقات المتعلقة بالجرائم الإلكترونية، وذلك بما يتماشى مع الاتفاقيات الدولية المصادق عليها من طرف الجزائر. وقد جاء هذا الإقرار في إطار احترام الجزائر لالتزاماتها الدولية، خاصةً بعد توقيعها على اتفاقية بودابست حول الجريمة السيبرانية سنة 2001، وإن لم تصادق عليها بعد، فإن روح الاتفاقية تتجلى في التشريع الوطني، لا سيما في ما يتعلق بـ: [1]

- تبادل المعلومات الجنائية.
- تسليم المجرمين الأجانب (وفق ضوابط).
- التعاون في جمع الأدلة الرقمية.
- تنفيذ الإنابات القضائية في الجرائم العابرة للحدود.

ثانيًا: المرونة الإجرائية لمواكبة الطبيعة التقنية للجرائم الإلكترونية.

نظرًا للطابع الفوري والدينامي لهذه الجرائم، فإن الأدلة الرقمية قد تُمحى أو تُعدل في ثوانٍ، ما يتطلب تدخلًا عاجلًا وفوريًا. ولهذا السبب، أجاز المشرّع الجزائري استخدام وسائل الاتصال الحديثة (كالبريد الإلكتروني والفاكس) في استقبال أو تنفيذ طلبات التعاون الدولي، دون اشتراط المرور بالطرق الدبلوماسية التقليدية، التي قد تكون غير ملائمة لطبيعة هذه الجرائم.

وتُعد هذه النقطة من مظاهر تطور الرؤية التشريعية الجزائرية، التي تهدف إلى التوفيق بين السرعة الإجرائية واحترام الضمانات القانونية، مما يساهم في تعزيز فعالية التعاون الدولي. [2]

[1]-مجاهدي خديجة صافية، اليات التعاون الدولي لمكافحة الجريمة المنظمة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري،تيزي وزو، 2018،ص240.

[2]-شنتير خضرة الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية .، ادرار، الجزائر، 2020-2021،ص210.

ثالثًا: القيود السيادية على التعاون الدولي.

رغم الانفتاح الواضح في النصوص على التعاون مع الدول الأجنبية، إلا أن المشرع الجزائري فرض مجموعة من القيود السيادية التي تُراعي خصوصية الدولة الجزائرية، والمبادئ الدستورية العليا، من بينها:

- مبدأ المعاملة بالمثل أي لا يتم تقديم المساعدة إلا إذا كانت الدولة الطالبة تقدم نفس مستوى التعاون.
- عدم المساس بالسيادة الوطنية أو النظام العام أو الأمن القومي :وهذه قيود تقليدية معمول بها في معظم النظم القانونية.
- سرية المعلومات بحيث لا يجوز استخدام المعلومات أو البيانات التي يتم تبادلها دوليًا إلا في إطار الغرض الذي طُلبت لأجله.

وتُظهر هذه القيود سعي الجزائر إلى التوفيق بين الانخراط في منظومة التعاون الدولي، وبين حماية مصالحها الحيوية وسيادتها الوطنية.

رابعًا: الاختصاص القضائي الموسّع.

من المسائل المهمة التي عالجها القانون رقم 09-04 أيضًا هي مسألة الاختصاص القضائي في الجرائم الإلكترونية، حيث منح للقضاء الوطني صلاحيات موسعة، من خلال تمكين المحاكم الجزائرية من النظر في الجرائم الإلكترونية التي تمس: [1]

- المؤسسات السيادية للدولة 5مثل رئاسة الجمهورية، الجيش، وزارة الداخلية)...
- البنى التحتية الإستراتيجية (مثل شبكات الطاقة، المياه، الاتصالات)...

وذلك حتى لو كان مرتكبو هذه الجرائم من الأجانب أو يقيمون خارج الجزائر، ما ينسجم مع مبدأ "الاختصاص العالمي الجزئي" الذي يُقرّه القانون الدولي في حالات معينة[2] .

خامسًا: موقف المشرع من تسليم المجرمين.

وفقًا لأحكام قانون الإجراءات الجزائية الجزائري، وخاصة المادة 699 منه، فإن الجزائر لا تُسلّم مواطنيها إلى أية دولة أجنبية، بصرف النظر عن طبيعة الجريمة، ويشمل ذلك الجرائم الإلكترونية. ومع ذلك، فإن تسليم الأجانب مسموح به، شريطة توافر الشروط التالية:

[1]-أيمن بن ناصر بن جماد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، دراسة مقارنة مكتبة القانون والاقتصاد، الرياض ،2015 ، ص201 .

[2]-مجاهدي خديجة صافية، المرجع السابق،ص240.

- أن تكون الجريمة معاقبًا عليها في القانون الجزائري (مبدأ التجريم المزدوج).
- ألا تكون الجريمة سياسية أو عسكرية.
- ألا يكون هناك خطر على حقوق الشخص المطلوب تسليمه.

ويمثل هذا الموقف توازنًا بين احترام السيادة الوطنية من جهة، والانخراط في التعاون الدولي من جهة أخرى، وهو نفس النهج الذي تتبناه دول أخرى عديدة مثل ألمانيا وفرنسا.

سادسًا: ملاءمة التشريع الوطني مع المعايير الدولية.

من خلال قراءة معمقة لأحكام القانون رقم 09-04، نلاحظ أن المشرّع الجزائري يسعى إلى ملاءمة الإطار القانوني الداخلي مع مقتضيات الاتفاقيات الدولية، ولا سيما تلك التي تحث على التعاون في مجال مكافحة الجرائم السيبرانية. ويتجلى ذلك في: [1]

- النص على أشكال التعاون المتعددة: القضائي، الفني، التقني.
- احترام المبادئ الدستورية (السيادة، الحريات، سرية المراسلات...).
- تبني المقاربات الوقائية والتحقيقية الحديثة.

[1]-شنتير خضرة ، المرجع السابق، ،ص210.

خلاصة الفصل الثاني:

تناول الفصل بالدراسة والتحليل الأبعاد المختلفة لمكافحة الجريمة السيبرانية على المستويين الوطني والدولي. فتم استعراض أبرز صور التعاون الدولي، مثل تبادل المعلومات، والمساعدة القضائية المتبادلة، وتسليم المجرمين، والتعاون الفني، وذلك في إطار اتفاقيات دولية محورية كاتفاقية بودابست والاتفاقية العربية لعام 2010. كما تم تسليط الضوء على أهمية التكوين والتدريب الفني للعاملين في المجالين الأمني والقضائي، باعتباره حجر الزاوية في بناء استجابة فعالة،. أما على المستوى الوطني، فقد بيّن الفصل كيف تعامل المشرّع الجزائري مع هذه الظاهرة من خلال القانون 09-04، مُقرًّا بضرورة الانفتاح على التعاون الدولي، مع الحفاظ على الضوابط السيادية والدستورية. ويخلص الفصل إلى أن مكافحة الجريمة السيبرانية تتطلب مقاربة شاملة، تستند إلى التنسيق الدولي الفعّال، والتحديث التشريعي المستمر، وبناء القدرات المؤسسية والبشرية القادرة على التصدي للتحديات المتنامية في الفضاء الرقمي.

الخاتـمـــة

الخاتمة

النتائج :

وفي ختام هذا العمل المتواضع توصلنا الى مجموعة من النتائج والاقتراحات ونذكر ما يلي:

-في ظل التحول الرقمي المتسارع الذي يشهده العالم اليوم، أصبحت الجرائم السيبرانية تشكل تهديداً حقيقياً ومتنامياً لأمن المعلومات، وسلامة الأنظمة المعلوماتية، واستقرار المجتمعات والدول على حد سواء. فقد أدى الاعتماد المتزايد على التكنولوجيا والفضاء الإلكتروني في مختلف مجالات الحياة الاقتصادية، والإدارية، والاجتماعية، وحتى الأمنية، إلى خلق بيئة محفوفة بالمخاطر والانتهاكات الرقمية. وتكمن خطورة هذه الجرائم في أنها لا ترتبط بمكان جغرافي محدد، ولا تخضع للحدود التقليدية، بل تمتاز بطبيعتها العابرة للحدود، مما يصعّب من مهام الكشف والملاحقة القانونية، ويزيد من تعقيد آليات المكافحة.

-وقد هدفت هذه الدراسة إلى الإحاطة الشاملة بمختلف الأبعاد النظرية والقانونية والتقنية المرتبطة بالجريمة السيبرانية، من خلال الوقوف عند مفهومها، خصائصها، دوافعها، وأشكالها المتعددة، وكذا استعراض أهم الآليات المعتمدة لمكافحتها، سواء من خلال التشريعات الوطنية كما هو الحال في القانون الجزائري (لا سيما القانون 04-09)، أو عبر الجهود الدولية التي تسعى إلى تنسيق العمل الجماعي لمواجهة هذا التهديد المشترك. وقد أظهرت النتائج أن التطور المستمر لأساليب الجريمة السيبرانية يقابله أحياناً بطء أو قصور في التحديث القانوني والمؤسساتي، ما يفتح المجال أمام استغلال الثغرات القانونية والتقنية.

-كما بيّنت الدراسة أن مكافحة هذا النوع من الجرائم لا يمكن أن تقوم على أساس الجهود الفردية أو المحلية فقط، بل تتطلب مقاربة شاملة ومتكاملة، تدمج بين الأطر التشريعية الوطنية والممارسات القضائية الفعالة، والتدابير الوقائية الأمنية والتكنولوجية، بالإضافة إلى تعزيز الوعي المجتمعي بالمخاطر السيبرانية، والتكوين المستمر للموارد البشرية المتخصصة في هذا المجال. ومن جهة أخرى، فإن التنسيق والتعاون الدولي يظل عنصراً أساسياً لا غنى عنه، بالنظر إلى الطابع العالمي لهذه الجرائم، وضرورة تبادل المعلومات والخبرات والمساعدة القانونية بين الدول.

-وعليه، فإن التصدي للجرائم السيبرانية يستلزم تبني استراتيجية وطنية واضحة للأمن السيبراني، تكون متعددة الأبعاد، وقائمة على التحليل الاستباقي للمخاطر، وتطوير الأدوات القانونية والتقنية الكفيلة بحماية

الفضاء الرقمي، وضمان حقوق الأفراد، واستقرار المؤسسات، وسيادة القانون في البيئة الرقمية. إن تأمين الفضاء السيبراني لم يعد ترفاً تشريعياً أو إدارياً، بل أصبح حاجة استراتيجية وأمنية ملحة تمليها التحديات الراهنة والمتوقعة في ظل الاقتصاد الرقمي والتحول الرقمي الشامل.

-أثبتت الدراسة أن الجريمة السيبرانية ليست مرتبطة فقط بالجوانب التقنية، بل تتداخل فيها أبعاد قانونية وأمنية واقتصادية واجتماعية.

-أظهرت التحاليل وجود تطور مستمر في أساليب الجرائم السيبرانية، مما يجعل مكافحتها أكثر تعقيداً من الجرائم التقليدية.

-أكدت الدراسة أن بعض النصوص القانونية الحالية لا تغطي كافة صور الجريمة السيبرانية المستجدة.

-بينت الدراسة ضعف التكامل بين الأجهزة المختصة بمكافحة الجريمة السيبرانية، سواء على المستوى الوطني أو الدولي.

أما الاقتراحات فكانت كما يلي:

-اعتماد سياسة وطنية موحدة للأمن السيبراني تتضمن إجراءات وقائية، قانونية، وتنسيقية.

-سن قوانين أكثر دقة وشمولاً تأخذ بعين الاعتبار طبيعة الجريمة السيبرانية المتجددة.

-تشجيع البحث العلمي والتقني في مجال الأمن السيبراني لتطوير حلول محلية فعالة.

-إقامة شراكات بين القطاعين العام والخاص لتعزيز حماية البنى التحتية المعلوماتية الحساسة.

قائمة المراجع والمصادر

قائمة المراجع والمصادر

1-المراجع

اولا: الكتب:

أ-الكتب العامة

1. إبراهيم خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009
2. احمد حليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، مصر، 2006
3. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الإسكندرية، 2011
4. بن يونس علي، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، مصر، 2004
5. خالد ممدوح، الجريمة الالكترونية، الدار الجامعية الجديدة، الإسكندرية، 2008
6. الزيدي وليد، القرصنة على الإنترنت والحاسوب، دار أسامة للنشر، عمان، 2009
7. شمسان ناجي صالح، الجرائم المستخدمة بطريقة غير مشروعة لشبكة الإنترنت، دار النهضة العربية، القاهرة، مصر، 2009
8. عبد العال الدريبي، محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قضائية قانونية مقارنة، المركز القومي للإصدارات القانونية، 2012
9. عقيقي كامل عفيفي، جرائم الكمبيوتر، دار النهضة العربية، القاهرة، 2010
10. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، 2009
11. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2009
12. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، مصر، 1993
13. نوري ياسين هرزاني، الإعلام والجريمة، مطبعة جامعة صلاح الدين، أربيل، 2005
14. أيمن عبد الله فكري، الجرائم المعلوماتية (دراسة مقارنة في التشريعات العربية والأجنبية)، مكتبة القانون والاقتصاد، الرياض، 2014
15. عادل عبد العال، إبراهيم الخراشي، مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة للنشر، 2015

ب- الكتب المتخصصة

1. احمد خليفة ملط، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
2. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2007
3. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، د.ت
4. امام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، العدد 630، 2026
5. أيمن بن ناصر بن جماد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، مكتبة القانون والاقتصاد، الرياض، 2015
6. الحمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، مصر، 2015
7. داودي خالد ، الجريمة الالكترونية ، دار الاعصر للنشر والتوزيع، عمان، 2011.
8. رستم هشام ، محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، ط1 ،مكتبة الآلات الحديثة، أسيوط، 1994 .
9. عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري، دار بلقيس، 2015
10. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006
11. العزيز سمير حامد، التعاقد عبر تقنيات الاتصال الحديثة (دراسة مقارنة)، دار النهضة العربية، 2001
12. قاسم محمد عبد الله، الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، مصر، 2010
13. القطاونة مصعب، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث منشور على شبكة قانوني، الأردن، 2010
14. قورة نائلة عادل محمد.، جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقية، ط1 دار النهضة العربية، القاهرة, ،2021.
15. قورة نائلة عادل، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، 2012
16. محمد امين شوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2009
17. محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، 2008
18. مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات –ماهيتها، صورها، الجهود الدولية لمكافحتها–، دار الخلدونية، الجزائر، 2018
19. ميرفت محمد جباية، مكافحة الجريمة الإلكترونية: دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري العلمية

ثانيا: المذكرات والرسائل العلمية:

ا-دكتوراه:

1. حسين ربيعي ، اليات البحث والتحقيق في الجرائم المعلوماتية ، أطروحة دكتوراه في العلوم تخصص قانون العقوبات ، جامعة باتنة 1، الجزائر ، 2015-2016.
2. شنتير خضرة الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية. ، ادرار، الجزائر، 2020-2021.
3. عمر بن محمد العتيبي، الامن المعلوماتي في المواقع الالكترونية و مدى توافقه مع المعايير المحلية و الدولية، أطروحة دكتوراه ، جامعة نايف للعلوم الأمنية ، كلية الدراسات العليا، 2010.
4. مجاهدي خديجة صافية، اليات التعاون الدولي لمكافحة الجريمة المنظمة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري،تيزي وزو، 2018.

ب-ماجستير:

5. سعيد علي نعيم اليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج الخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012.
6. سعيداني نعيم، اليات البحث و التحري عن الجريمة المعلوماتية ، مذكرة ماجستير في العلوم القانونية ، جامعة الحاج لخصر، باتنة، الجزائر، 2012-2013.
7. طرشي نورة مكافحة الجريمة المعلوماتية، رسالة ماجستير تخصص قانون جنائي، جامعة الجزائر 01 الجزائر 2011 -2012.
8. عبد الرحمان جميل محمود حسين الحماية القانونية لبرامج الحاسب الآلي، مذكرة ماجستير جامعة النجاح الوطنية نابلس فلسطين، كلية الدراسات العلياء 2008.
9. لصغير يوسف الجريمة المرتكبة عبر الأنترنت مذكرة لنيل شهادة ماجستير تخصص قانون دولي للأعمال، كلية الحقوق والعلوم سياسية، تيزي وزو الجزائر 2013.
10. يوسف صغير، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، جامعة مولود معمري تيزي وزو، 2013.

ج-ماستر:

1. أسامة مهمل، الاجرام السيبيراني، مذكرة ماستر في الحقوق تخصص قانون جنائي، جامعة محمد بوضياف، المسيلة، الجزائر،2017-2018

2. باخد نعيمة، الطيبي أمنة، دور العلام الرقمي في الحد من الجرائم السيبيرانية موقعي "الشروق" و "أخبار الوطن" اونلاين أنموذجا، مذكرة ماستر في علوم الاعلام و الاتصال تخصص صحافة مطبوعة الكترونية، جامعة احمد درايعية ، ادرار، الجزائر،2022-2023

3. بوديسة بجاد عبد الرؤوف ، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر في الحقوق تخصص قانون الاعلام الآلي والانترنيت، جامعة محمد البشير الابراهيمي، برج بوعريريج، الجزائر، 2021-2022.

4. بوعرعارة إبراهيم زياد، خصوصية الجريمة الالكترونية، مذكرة ماستر في الحقوق تخصص قانون جنائي، جامعة غرداية ، الجزائر، 2021-2022.

5. العيد شعثان، مسعود موفقي،الجرائم السيبيرانية في القانون الجزائري،مذكرة ماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية، جامعة زيان عاشور، الجلفة، الجزائر، 2021-2022

6. محمد بوعمرة، سيد على بينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية ، جامعة أكلى محمد أولحاج البويرة 2019/2020

7. هادي زيادة، آليات التعاون الدولي في مكافحة الجريمة السيبيرانية، مذكرة ماستر في القانون العام تخصص قانون جنائي و علوم جنائية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2022-2023

ثالثا: المجلات والمقالات العلمية:

1. بدر عدنان ، احمد سعيد الخبيزي، تحديات و تهديدات الأمن السيبراني و طرق التغلب عليها، حوليات آداب عين الشمس، جامعة عين الشمس، المجلد 51 ،العدد سبتمبر ،2023 مصر.

2. برقوق يوسف، المساعدة القضائية المتبادلة لمواجهة الجرائم الالكترونية، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 01، العدد2021،01،.

3. تومي يحي الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18/07، دراسة تحليلية مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2019.

4. جمال ابراهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية ، المجلد 11،العدد 02، جامعة مولود معمري، تيزي وزو، الجزائر، دت .

5. جمال براهيمي، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون و العلوم السياسية ، المجلد 11 kالعدد02، جامعة مولود معمري، تيزي وزو، الجزائر، دت .

6. راضية حميدة، الجريمة الإلكترونية غير مواقع التواصل الاجتماعي نحو تفعيل دور الأمن السيبراني المعلوماتي"، مجلة الإعلام والمجتمع، المجلد 05، العدد 02، ديسمبر 2021 .

7. راوية بنت عطية هلا الصحفي، الجرائم السيبرانية، مجلة الإلكترونية الشاملة متعددة التخصصات ، العدد 24، 2020.

8. زياد بن محمد عادي العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدوافع من ارتكابها المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 3، العدد 1، 2020.

9. سراء جبريل رشاد مرعي،"الجرائم الإلكترونية(الأهداف– الأسباب–طرق الجريمة ومعالجتها)"،مجلة الدراسات الإعلامية، المركز الديمقراطي العربي،العدد،1يناير 2018 .

10. صالح بن محمد المسند وعبد الرحمان بن راشد المهيني " جرائم الحاسب الآلى الخطر الحقيقي في عصر المعلومات ". المجلة العربية للدراسات الأمنية والتدريب العدد 29 (المجلد (15) أفريل 2000.

11. طباش عز الدين، "حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي"، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 56، العدد 1، 2019.

12. عائشة عبد الحميد، ملوك نوال الإجرام السيبراني وأثره على تهديد الأمن الثقافي في الجزائر" ، مجلة المفكر للدراسات القانونية والسياسية، المجلد 3، العدد 3، سبتمبر 2020 .

13. عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، مجلة معالم للدراسات القانونية و السياسية ، المجلد 04، العدد01، جامعة يحي فارس، المدية، الجزائر، 2020.

14. عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية : دراسة تأصيلية مقارنة ، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03،المملكة العربية السعودية، السعودية ،2020 .

15. علي قابوسة، عبد السلام محمد الميل، عادل محمد الشربجي، الجريمة الالكترونية في الفضاء الالكترونية –المفهوم، الأسباب، سبل المكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات سداسية، دولية محكمة، العدد 04، المركز الجامعي ايليزي، 2019.

16. فاروق خلف، الاليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات ، العدد02، كلية الحقوق ، جامعة ، جامعة حمه لخضر ، الوادي ، الجزائر، 2015.

17. فريد ناشف اليات التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، جامعة بليدة 02 الجزائر2022.

18. قرران مصطفى، زرقين عبد القادر الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن العدد 02 جامعة خميس مليانة الجزائر ، 2022.

19. قطاف سليمان، بوقرين عبد الحليم، الاليات الموضوعية والاجرائية المتبعة لتحقيق الامن السيبيراني (الجزائر نموذجا)، مجلة الحوكمة والقانون الاقتصادي، جامعة عمار ثليجي ، الاغواط، الجزائر، 2023.

20. كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الاكاديمية للبحث القانوني، المجلد 11، العدد 01، 2015، ص17.

21. لاكلي نادية، الجريمة السيبيرانية في الجزائر والعقوبات المقررة لها، مجلة الاجتهاد القضائي ، المجلد 15، العدد 01، جامعة بلحاج بوشعيب، عين تموشنت، الجزائر، 2023.

22. ليندة شرا بشة السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية – الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة الدراسات والأبحاث العدد 01، جامعة عاشور زبان الجلفة الجزائر ، 2009ء.

23. ليندة شرابسة، السياسة الدولية و الإقليمية في مجال الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة الدراسات والأبحاث ، العدد 01، جامعة عاشور زيان، الجلفة ، الجزائر، 2009.

24. محمد أحمد سليمان عيسى التعاون الدولي المواجهة الجرائم الإلكترونية المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016.

25. معاشي سميرة، ماهية الجريمة الالكترونية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة الجزائر 2011.

26. معاشي سميرة، ماهية الجريمة الالكترونية، بحث منشور في مجلة المنتدى القانوني، العدد الاسبع، دامعة محمد خيضر، بسكرة، الجزائر.

27. مغنية تشتاش، مداخلة حول الركن المفترض في الجريمة المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، 2015-2016.

28. مهدي رضا، الجرائم السيبيرانية و آاليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد 06، العدد 02، جامعة محمد بوضياف، المسيلة، الجزائر،2021.

29. مهدي رضا، الجرائم السيبيرانية وآليات مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث والدراسات، المجلد 06، العدد 02، جامعة محمد بوضياف ، المسيلة ، الجزائر، 2021.

30. نورهان محمد الربيعي، الجريمة السيبيرانية و آليات مكافحتها (دراسة مقارنة)، مجلة الفارابي للعلوم الإنسانية ، المجلد 03، العدد 01، كلية الحقوق، جامعة عجمان، الامارات العربية المتحدة، 2024.

31. ينو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون و التنمية، المجلد 4، العدد 1، 2022.

32. يوهرين فتيحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، مجلد 14، العدد 04، جامعة قسنطينة 02 الجزائر، 2021.

رابعا: الملتقيات والمداخلات العلمية:

1. امحمد مولاي، صعوبات تطبيق الإدارة الالكترونية بالجزائر : الجريمة الالكترونية نموذجا"، المؤتمر العالمي الأول للإدارة الالكترونية، مركز المدينة للوسائط المتعددة، طرابلس، ليبيا، 2010.

2. عبد المؤمن بن صغير " الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن ، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة الموسوم بعنوان الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و 17 نوفمبر 2015، ص 08

3. عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، قيادة الدرك الوطني، مداخلة بالملتقى الوطني حول : الجريمة المعلوماتية بين الوقاية والمكافحة جامعة محمد خيضر بسكرة 16 نوفمبر 1015 ، ص 30.

4. مروة خنتي، الملتقة الدولي بعنوان الجرائم السيبيرانية الظاهرة المستجدة الأسباب وسبل المعالجة ، مداخلة بعنوان الجريمة السيبيرانية نقطة تهديد للمحتوي الرقمي ، جامعة خميس مليانة، 24-25 نوفمبر 2024، الجزائر، ص15.

5. موسى مسعود أرحومة " الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، مداخلة مقدمة ضمن فعاليات المؤتمر المغاربي الأول الذي نظمته أكاديمية الدراسات العليا بطرابلس الموسوم بعنوان: المعلوماتية والقانون، يومي 28 -29 أكتوبر، 2010،ص03.

خامسا: المحاضرات و المطبوعات الجامعية:

1. فريد روايح، محاضرات في القانون الجنائي العام، مطبوعة دروس للسنة الثانية ليسانس، قسم الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر،2018-2019، ص87.

2-المصادر

أولا: القوانين:

2. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 يعدل و يتمم الامر رقم 66-155 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، المؤرخة في 10 نوفمبر 2004.

3. القانون رقم 04-09 المؤرخ في 05-08-2009، يتضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية ، العدد 47، الصادرة في 16-08-2009.

- القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات. جريدة الرسمية رقم 71 المؤرخة سنة 2004.
- القانون 18/07 المؤرخ في 10/05/2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34 المؤرخة في 10/05/2018
- القانون رقم 06/23 المؤرخ في 20/12/2006 والذي من المادة 303 واقراره بالمادة 303 مكرر إلى 303 مكرر 03، وهذا تصديا للاستخدام السيء لوسائل التكنولوجيا الحديثة.
- القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004.

ثانيا: المراسيم

1. مرسوم رئاسي رقم 20-183 مؤرخ في 13 يوليو 2020 (21 ذي القعدة 1441 هـ) يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد نُشر هذا المرسوم في الجريدة الرسمية للجمهورية الجزائرية بتاريخ 11 يوليو 2020، ص 12.

2. مرسوم رئاسي رقم 15-261 مؤرخ في 2015/10/08، تعدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم. المتصلة بتكنولوجيات الاعلام والاتصال والمكافحة الجريدة الرسمية، العدد 53 الصادرة بتاريخ 2015/10/08.

3. مرسوم رئاسي رقم 19-172 مؤرخ في 06-06-2019 يجدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها و تنظيمها وكيفيات سيرها جريدة رسمية رقم 37 لسنة 2019.

4. مرسوم رئاسي رقم 183-04 ، المؤرخ في 26 يونيو سنة 2004 بتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية 41 ، الصادرة في 27/06/2004.

5. المرسوم التنفيذي رقم 16-280 المؤرخ في 02-11-2016 المعدل والمتمم للمرسوم التنفيذي رقم 08-04 الموافق ل19 يوليو 2003، ج ر ، العدد 44، سنة 2003

الفهرس

بسملة .....أ

شكر وعرفان ..... ج

إهداء ..... هـ

قائمة المختصرات .....د

مقدمة 2

الفصل الأول: الاطار المفاهيمي للجرائم السيبيرانية

المبحث الأول: ماهية الجرائم السيبرانية 9

المطلب الاول: مفهوم الجرائم السيبرانية 9

الفرع الأول : تعريف الجرائم السيبرانية 9

الفرع الثاني: الدوافع الإجرامية وسمات الجاني في الجرائم السيبرانية واصنافه 14

الفرع الثالث: موقف المشرع الجزائري من الجريمة السيبرانية 18

المطلب الثاني: خصائص الجرائم السيبرانية وطبيعتها القانونية 20

الفرع الأول: خصائص الجريمة السيبيرانية 20

الفرع الثاني: الطبيعة القانونية للجرائم السيبيرانية 24

المبحث الثاني: مجال ونطاق الامن السيبيراني 26

المطلب الاول: انواع الجرائم السيبرانية 26

الفرع الأول : الجرائم الإلكترونية المرتكبة بواسطة النظام المعلوماتي 26

الفرع الثاني: الجرائم الإلكترونية المرتكبة داخل النظام المعلوماتي 29

المطلب الثاني: اركان الجرائم السيبرانية 32

الفرع الاول: الركن الشرعي.....33

الفرع الثاني: الركن المادي للجريمة الإلكترونية.....37

خلاصة الفصل.....40

الفصل الثاني: جهود القوانين المقارنة في مكافحة الجرائم السيبيرانية

المبحث الأول: آليات مكافحة الجرائم السيبرانية في التشريع الجزائري.....43

المطلب الاول: التدابير الإجرائية من الجرائم السيبرانية في ظل قانون 09-04.....43

الفرع الأول: التدابير الوقائية 43

الفرع الثاني: الهيئات المتخصصة في البحث والتحري عن الجرائم السيبيرانية.....49

المطلب الثاني: العقوبات المقررة للجرائم السيبرانية 55

الفرع الأول : العقوبات الاصلية للجرائم السيبيرانية 55

الفرع الثاني: العقوبات التكميلية للجرائم السيبيرانية.....58

المبحث الثاني: جهود القوانين المقارنة في مكافحة الجرائم السيبرانية 61

المطلب الأول: مواجهة الجريمة السيبيرانية على المستوى الدولي.....61

الفرع الأول: دور الأمم المتحدة في مواجهة الجريمة الإلكترونية.....62

الفرع الثاني: دور المجلس الأوروبي وجامعة الدول العربية في مواجهة الجريمة الإلكترونية.....64

المطلب الثاني: مجالات التعاون لمكافحة الجريمة السيبيرانية 67

الفرع الأول : مظاهر التعاون القضائي والإجرائي الدولي لمكافحة الجريمة الإلكترونية 67

الفرع الثاني: موقف المشرّع الجزائري من التعاون الدولي في مكافحة الجريمة الإلكترونية.....70

خلاصة الفصل الثاني 74

الخاتمة 76

قائمة المراجع والمصادر 79

ملخص 91

ملخص

تُعد الجريمة الإلكترونية من الظواهر الإجرامية المستحدثة التي تعتمد على وسائل تقنية متطورة ومهارات عالية لدى الجاني، مما يجعل التحقيق والمحاكمة فيها يتميّزان بخصوصية كبيرة. وقد ساهم التوسع السريع في استخدام تكنولوجيا المعلومات في جميع القطاعات في ظهور أنماط جديدة من الجرائم السيبرانية، الأمر الذي استدعى تدخلًا تشريعيًا على المستويين الدولي والوطني. وعلى الرغم من صدور قوانين تجرّم هذه الأفعال، إلا أن الجهود المنفردة بيّنت وجود قصور تشريعي وعملي. وفي الجزائر، بذل المشرع جهودًا مهمة لمواجهة هذه الظاهرة عبر نصوص قانونية وهيئات مختصة، لكن الحاجة لا تزال قائمة لتعزيز التعاون الدولي وتطوير الآليات التقنية والقانونية لمكافحة هذا النوع من الجرائم.

الكلمات المفتاحية :الجريمة السيبرانية – المجرم الإلكتروني–الجهود الوطنية – التعاون الدولي – المشرع الجزائري.

Abstract ;

Cybercrime is considered one of the emerging criminal phenomena that relies on advanced technological means and high-level skills possessed by the offender, which gives investigation and prosecution procedures a distinctive complexity. The rapid expansion in the use of information technology across all sectors has led to the emergence of new forms of cybercrime, prompting legislative intervention at both international and national levels. Although many laws have been enacted to criminalize such acts, individual efforts have revealed legislative and practical shortcomings. In Algeria, the legislator has made significant efforts to address this phenomenon through legal provisions and specialized bodies. However, there remains a pressing need to strengthen international cooperation and develop both technical and legal mechanisms to effectively combat this type of crime.

Keywords: Cybercrime – Cybercriminal – National efforts – International cooperation – Algerian legislator.

.