الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف بالمسيلة

كلية : الحقوق والعلوم السياسية
قسم : الحقوق
رقم :.....

ميدان : الحقوق والعلوم السياسية
التخصص : قانون الجنائي و العلوم الجنائية
فرع : الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تحت عنوان

الآليات المستحدثة لمكافحة الجريمة السيبرانية في التشريع الجزائري

من إعداد الطالب :
- بحاش خيرالدين

تحت الإشراف الأستاذ :
- أ . د . يحياوي حمزة

د. مقروف محمد	جامعة المسيلة	رئيسا
د. يحياوي حمزة	جامعة المسيلة	مشرفا ومقررا
د. الوافي السعيد	جامعة المسيلة	ممتحنا

تاريخ المناقشة : 2026/06/06

ملحق بالقرار رقم ....1082.... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): بحاش خير الدين الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم 200399005 والصادرة بتاريخ 2016-04-27

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: الآليات المستحدثة لمكافحة الجريمة السيبرانية في التشريع الجزائري

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2026/05/02

توقيع المعني (ة)


بسم الله الرحمن الرحيم



أحمدُ الله عزّ وجلّ وأشكره على توفيقه وعونه، إذ لولا فضله ما تمّ هذا العمل، فله الحمد والشكر على نعمه وتيسيره في إنجاز هذا العمل المتواضع.

وأتوجّه بخالص الشكر وعظيم التقدير إلى أستاذي الفاضل الأستاذ "يحياوي حمزة" الذي تفضّل بقبول الإشراف على هذه المذكرة، وتابع مختلف مراحل إنجازها بصدر رحب، ولم يبخل عليّ بتوجيهاته القيّمة ونصائحه السديدة التي كان لها بالغ الأثر في إتمام هذا العمل.

كما أتقدّم بجزيل الشكر والتقدير إلى الأستاذ " الوافي السعيد" على ما قدّمه لي من نصائح ، وما أسداه من ملاحظات أفادتني في إعداد هذه المذكرة.

ولا يفوتني أن أتقدّم بخالص الشكر والامتنان إلى الأساتذة الأفاضل أعضاء لجنة المناقشة، كلٌّ باسمه ومقامه، لتفضّلهم بقبول مناقشة هذه المذكرة، وما سيبدونه من ملاحظات وتوجيهات قيّمة من شأنها إثراء هذا العمل.

أيضا كل الشكر والتقدير إلى أساتذة كلية الحقوق بـ جامعة محمد بوضياف بالمسيلة، على ما قدّموه لي من علمٍ نافع وتوجيهٍ قيّم ودعمٍ أكاديمي كان له الأثر البالغ في مساري الجامعي فجزاهم الله عنّا خير الجزاء، وبارك في علمهم وجهودهم.

وأخيرًا، أتوجّه بالشكر إلى كل من ساهم من قريب أو بعيد في إنجاز هذا العمل، ولو بكلمة طيبة أو مساعدة يسيرة.

إهداء

إلى روح أبي الطاهرة

إلى من كلّله الله بالهيبة والوقار، إلى من كان سندي الأول وقدوتي في الحياة، إلى من علّمني معنى الكفاح، وغرس في نفسي حبّ العلم والعمل، وحثّني على طلب المعرفة والسير في دروب النجاح، إلى مصدر فخري وعزّتي، من أحمل اسمه بكل اعتزاز وافتخار، رحلتَ عن هذه الدنيا جسدًا لكنّك ما زلت حاضرًا في قلبي في دعواتي، وفي كل خطوة أخطوها نحو النجاح ، كم تمنّيت أن تكون اليوم إلى جانبي لترى ثمرة تعبك وغرسك، لكن عزائي أنّ دعواتك وتربيتك الصالحة ما تزال ترافقني ، رحمك الله رحمة واسعة، وجعل هذا العمل صدقة جارية في ميزان حسناتك، وأكرم مثواك في جنّات النعيم.

إلى أمي الغالية

إلى صاحبة أكبر قلب عرفته في حياتي، إلى النبع الذي أفاض عليّ حبًا وحنانًا لا ينضبان، إلى رمز الصبر والعطاء والتضحية، إلى من كانت سببًا في قوتي وثقتي بنفسي بعد الله، إلى مخبأ أسراري ورفيقة همومي وأفراحي ، إلى من وقفت إلى جانبي في كل خطوة من مساري الدراسي، تساندني بدعائها، ، ولا يهدأ قلبها حتى ترى أبناءها في أعلى مراتب النجاح والتفوق، إلى التي كانت تعطينا من راحتها وسعادتها دون انتظار مقابل، إلى من اليوم تشاركني نجاحًا آخر، حبيبتي وقرة عيني، أمي حفظها الله وأطال في عمرها، وأدام عليها الصحة والعافية. إلى من كانت وما تزال السند الحقيقي، والنور الذي يضيء عتمة الأيام، والدفء الذي ألوذ به كلما أثقلتني الحياة .

إليكِ أمي وأبي أهدي هذا النجاح، فلكما الفضل بعد الله في كل ما وصلتُ إليه.

إلى إخوتي وأخواتي الأعزاء، مهما كتبت فلن أوفيكم حقكم، إلى من تعلمت منهم الثبات والسير دون خوف، والصبر لبلوغ النجاح، شكرًا لوقفتكم الدائمة إلى جانبي، فكنتم السند والقوة في كل مرحلة، حفظكم الله وأدامكم أجمل نعمة في حياتي

إلى من تربّى وترعرع بيننا كأخٍ عزيز، ابن أختي يونس، الذي شاركنا تفاصيل الأيام وكان جزءًا من دفء العائلة وإلى البرعم الغالي عبد القادر يوسف، ابن أختي، الذي جاء إلى الدنيا بعد رحيل أبي حاملًا اسمه، فكأن القدر أراد أن يترك لنا أثرًا جميلًا وذكرى لا تغيب، فأدخل إلى قلوبنا فرحًا متجددًا

وإلى أكرم وريان، ختام الفرح وزينة اللقاءات، أبناء إخوتي، الذين تكتمل بضحكاتهم بهجة العائلة

إليكم جميعًا، بكل المحبة والامتنان، أهدي ثمرة هذا الجهد، راجيًا أن تبقى بيننا المودة سندًا، والمحبة رابطًا لا يزول.

خير الدين

قـــائمة الـــمختصـــرات:

- ق إ ج ج: قانون الإجراءات الجزائية الجزائري.
- ق ع ج: قانون العقوبات الجزائري.
- د س ن : دون سنة نشر.
- د ت ، دون ترقيم.
- ف: فقرة,
- ج: جزء.
- ط : الطبعة.

مـــقـدمـــة

مـقـدمــة

شهد التطور التكنولوجي المعاصر تحوّلًا نوعيًا في مختلف مناحي الحياة، حيث أسهم بشكل ملحوظ في تحسين أداء الأفراد والمؤسسات، سواء كانوا أشخاصًا طبيعيين أم معنويين، وذلك من خلال توظيف النظم المعلوماتية التي يسّرت الأنشطة اليومية والمهنية على حدّ سواء. وقد أفضت هذه النظم إلى توفير كمٍّ هائل من البيانات والمعلومات، مما عزّز مختلف المجالات الاقتصادية والاجتماعية والثقافية، وأسهم في رفع كفاءة الأداء وتسريع وتيرة الإنجاز.

غير أنّ هذا التقدم لم يخلُ من آثار سلبية، إذ أفرز في المقابل أنماطًا جديدة من السلوك الإجرامي، تمثّلت في الاستعمال غير المشروع للنظم المعلوماتية. فقد استغل بعض الأفراد هذه الوسائل لارتكاب جرائم، مستفيدين من خصائصها المتمثلة في تجاوز الحدود الجغرافية، وسرعة تنفيذ العمليات، وصعوبة تتبّعها، فضلًا عن القصور النسبي في الأطر القانونية والتنظيمية التي تكبح هذه الممارسات. ومن أبرز هذه الجرائم، الجريمة السيبرانية التي تتسم بهذه الخصائص، والتي بدورها مستّ العديد من المجالات والأبعاد، بحيث خلّفت آثارًا سلبية جسيمة على مختلف الأصعدة.

وأمام تنامي هذه الظاهرة المتمثلة في سوء استعمال النظم المعلوماتية لأغراض غير مشروعة، سارعت مختلف الدول إلى تطوير آليات قانونية وإجرائية مستحدثة لمواجهتها، سواء على المستوى الوطني أو من خلال تعزيز التعاون الدولي، وذلك بهدف الكشف عن الجرائم السيبرانية والتحقيق فيها وملاحقة مرتكبيها. غير أنّ هذه الجهود لا تزال تواجه تحديات قانونية وتقنية، تفرض ضرورة البحث المستمر عن وسائل أكثر فعالية ونجاعة.

وفي هذا السياق، عمل المشرّع الجزائري على استحداث جملة من الآليات القانونية والإجرائية لمكافحة الجرائم السيبرانية، مستلهمًا في ذلك من التجارب والتشريعات الدولية، قصد تعزيز الحماية القانونية للنظم المعلوماتية والحد من الاعتداءات الواقعة عليها، من خلال سنّ نصوص خاصة

وتعزيز الآليات الإجرائية والمؤسساتية الكفيلة بالتصدي لها، سواء على المستوى الوقائي أو الردعي.

الإشكـــاليـــة المطروحـــة

وتتمحور إشكالية هذه الدراسة حول التساؤل الآتي:

كيف نظّم المشرّع الجزائري استحداث آليات قانونية ومؤسساتية لمكافحة الجريمة السيبرانية؟

وللإجابة عن الإشكالية التي تم ذكرها سابقا، تم تقسيم هذه الدراسة **وفق الخطة المعتمدة** متكونة من فصلين متكاملين، يتناول كل منها جانبا أساسيا من الموضوع وهيا كآتي:

الفصل الأول: يُخصَّص هذا الفصل لعرض الإطار العام للجريمة السيبرانية، دراسة مختلف الأبعاد المفاهيمية والقانونية المرتبطة بالموضوع التي تُسهم في فهم هذه الظاهرة الإجرامية المستحدثة، فسيتم في **المبحث الأول** التطرّق إلى الإطار المفاهيمي للجريمة السيبرانية، حيث سيتم تحديد مفهومها من خلال تعريفها لغةً واصطلاحًا وفقهًا وقانونًا، ثم بيان أهم خصائصها التي تميزها عن غيرها من الجرائم التقليدية، إضافة إلى إبراز طبيعتها القانونية وموقف المشرّع الجزائري منها. كما سيتم في هذا المبحث التعرّض إلى تطوّر صور الجريمة السيبرانية، سواء في صورتها التقليدية أو في أنماطها المستحدثة المرتبطة بالتطور التكنولوجي.

كما نسلط الضوء في **المبحث الثاني**، لدراسة الإطار القانوني للجريمة السيبرانية، من خلال تحليل أركانها الأساسية المتمثلة في الركن الشرعي والمادي والمعنوي، ثم التطرّق إلى المجرم السيبراني من حيث تعريفه وسماته وفئاته، بالإضافة إلى تحديد مختلف الدوافع التي تقف وراء ارتكاب هذا النوع من الجرائم، سواء كانت دوافع شخصية أو خارجية.

وبذلك، يهدف هذا الفصل إلى تقديم رؤية شاملة ومتكاملة حول الجريمة السيبرانية، تمهيدًا للتعمق في دراسة الآليات القانونية والإجرائية المستحدثة لمكافحتها في الفصل الثاني.

وأما **الفصل الثاني:** تم تسليط الضوء عليه يُخصَّص هذا الفصل لدراسة الآليات المستحدثة لمكافحة الجريمة السيبرانية في التشريع الجزائري، باعتبارها استجابة قانونية ومؤسساتية لمواجهة التطور المتسارع لهذا النوع من الإجرام. وعليه، يتناول **المبحث الأول** الآليات التشريعية والإجرائية التي أقرها المشرّع، خاصة من خلال القانون 09-04 والقوانين الداعمة له، إضافة إلى الوسائل الخاصة بالملاحقة مثل التسرب الإلكتروني واعتراض المراسلات والحفظ العاجل للمعطيات الإلكترونية.

كما يسلّط **المبحث الثاني** الضوء على الآليات المؤسساتية الوطنية والدولية، من خلال مختلف الأجهزة الأمنية والهيئات المتخصصة، إلى جانب التعاون الدولي في إطار الاتفاقيات والمنظمات المعنية، بما يعكس سعي الجزائر إلى بناء منظومة شاملة وفعالة لمكافحة الجريمة السيبرانية.

المنهـــج المتبـــع

تم الاعتماد في هذه الدراسة على منهجين، هما **المنهج الوصفي والمنهج الاستدلالي؛** حيث استُخدم **المنهج الوصفي** في وصف الجريمة السيبرانية، وتعريفها، وبيان أركانها، وخصائصها، وأوجه اختلافها عن باقي الجرائم. كما استُخدم **المنهج الاستدلالي** في تحليل النصوص القانونية المتعلقة بالجريمة السيبرانية، واستنباط الأحكام القانونية منها، وبيان كيفية توظيفها من قبل القضاة في إدانة مرتكبي هذه الجرائم.

أهـــميـــة المـوضـــوع

وتتجلّى أهمية دراسة هذا الموضوع في كونه يمسّ أحد أبرز التحديات القانونية المعاصرة، كما يكتسي بُعدًا عمليًا يتصل بحماية الأمن الرقمي الوطني وضمان الثقة في المعاملات الإلكترونية. كما تبرز أهميته العلمية من خلال إلقاء الضوء على مدى انسجام الآليات المستحدثة مع خصوصية الجريمة السيبرانية، ومدى قدرتها على تحقيق التوازن بين مقتضيات الأمن الرقمي وضمانات حقوق الإنسان والحريات الأساسية.

ومن **الناحية النظرية**، تكتسي هذه الدراسة أهمية بالغة، كونها تسهم في إثراء الأدبيات القانونية حول مفهوم الجريمة السيبرانية باعتبارها ظاهرة مستحدثة ومعقّدة، كما تساهم في توضيح الإطار المفاهيمي والقانوني المرتبط بها، مما يفتح المجال أمام دراسات أكاديمية مستقبلية لفهم أعمق لأبعادها وتطوّراتها في ظل البيئة الرقمية المتغيرة.

أما من **الناحية العملية**، فتنبع أهمية هذه الدراسة من التهديد المتزايد للجرائم السيبرانية على الأمن القومي والمجتمعي والاقتصادي، حيث تبرز الحاجة إلى تقييم واقعي للجهود المبذولة على المستويين الوطني والدولي، بما يسهم في تعزيز آليات المواجهة القانونية والتقنية لهذا الخطر الرقمي المتنامي.

أهـداف دراسـة المـوضـــوع

ينطلق عرض أهداف هذا الموضوع من الرغبة في تحديد الغايات العلمية والعملية التي تسعى هذه الدراسة إلى بلوغها، وذلك من أجل إبراز مختلف الجوانب التي يعالجها البحث بشكل واضح ومنظم. فتمثلت الأهداف فيما يلي:

- تحديد الإطار المفاهيمي والقانوني للجريمة السيبرانية.
- إبراز الآليات القانونية والإجرائية المستحدثة لمكافحتها في التشريع الجزائري.
- تحليل دور الهيئات والأجهزة المختصة في التصدي لهذا النوع من الجرائم.
- إبراز النقائص والتحديات التي تواجه مكافحة الجريمة السيبرانية واقتراح حلول عملية.
- دراسة تطور التشريع الجزائري في مجال مكافحة الجريمة السيبرانية عبر الزمن.
- إبراز دور التعاون الدولي والإقليمي في مكافحة الجرائم السيبرانية.
- تحليل أثر التطور التكنولوجي (كالذكاء الاصطناعي والبيانات الضخمة) على طبيعة الجريمة السيبرانية.
- إبراز دور التكوين والتدريب المتخصص للأجهزة الأمنية والقضائية في هذا المجال.
-

أسبـاب اختيــار المـوضـــوع

يعود اختياري لهذا الموضوع إلى ما تفرضه الجرائم المعلوماتية، وبالأخص الجريمة السيبرانية، من تحديات حقيقية أمام المنظومة التشريعية التقليدية، وذلك بسبب الطابع المستحدث والمتطور لهذه الجرائم، مما يجعل النصوص القانونية القائمة عاجزة أحيانًا عن الإحاطة بها ومعالجتها بالشكل الكافي، إلى جانب مجموعة من الأسباب الأخرى، من بينها:

الأسـباب الذاتـية

- اهتمامي الكبير جدا بنظم المعلوماتية وكل ما يشملها من كل الزاوية.
- اهتمامي العميق بالقانون الجنائي، لا سيما في شقه المتعلق بالجرائم الحديثة التي أفرزها التطور التكنولوجي، والتي باتت تشكل تحديًا حقيقيًا للمنظومة العدلية.
- رغبتي في التعمق أكثر في أليات مكافحة الجريمة السيبرانية من زاوية جزائية تطبيقية، والوقوف على مدى نجاعة الآليات القانونية المعتمدة في التعامل معها.

الأسباب الموضوعية

- التزايد المطّرد للجريمة السيبرانية في الجزائر وتأثيرها المتنامي على الأفراد والمؤسسات وحتى على الأمن العام، ما يجعل من الضروري دراسة سبل مواجهتها قانونيًا.
- التطورات التشريعية التي شهدها القانون الجزائري، خاصة مع صدور القانون 21-11 المتعلق بمكافحة الجرائم المعلوماتية والقانون 24-06، مما يستوجب تحليل مدى فعاليتهما في مجابهة هذه الجرائم.
- معرفة الآليات المدعمة لقانون 09-04 للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- الحاجة إلى تقييم قدرة الآليات على مكافحة هذه الجريمة وعلى مواكبة التطورات التقنية، ومدى نجاعة الوسائل القانونية في حد من هذه الجريمة.
-

الـدراســات الســابقــة

- **أطروحة دكتوراه للباحثة شنتير خضرة بعنوان: الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، نوقشت بجامعة أحمد دراية بأدرار، كلية الحقوق والعلوم السياسية، خلال السنة الجامعية 2020-2021.** تناولت فيها الباحثة الجوانب الإجرائية الخاصة بمكافحة الجريمة الإلكترونية، من خلال التعرف على الآليات المكلفة بمكافحتها على المستويين الوطني والدولي، مع إبراز الأساليب المعتمدة في التحري عن هذه الجرائم. بينما تناولت في دراستي الآليات المكلفة بمكافحة الجريمة السيبرانية على المستويين الوطني والدولي.
- **أطروحة دكتوراه للباحث ربيعي حسين بعنوان: آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، نوقشت بجامعة باتنة كلية الحقوق والعلوم السياسية، السنة الجامعية 2015-2016.** درست الأطروحة خصوصية إجراءات البحث والتحقيق في هذا النوع من الجرائم، مع إبراز أهم الصعوبات التقنية والقانونية التي تواجه أجهزة الضبطية القضائية، وبيان الآليات المعتمدة لمكافحتها، ومدى ملاءمة القواعد الإجرائية التقليدية مع طبيعة البيئة الرقمية. بينما تناولت في دراستي الآليات الإجرائية المعتمدة على الصعيد الوطني في مكافحة الجريمة السيبرانية.
- **أطروحة دكتوراه للباحث غازي عبد الرحمان هيان الرشيد بعنوان: الحماية القانونية من الجرائم المعلوماتية، الحاسب والأنترنت، نوقشت بجامعة الإسلامية قفي لبان، كلية الحقوق، السنة 2004،** بحيث تطرق الباحث لتحليل طبيعة هذه الجرائم وخصائصها وتحديات مكافحتها. كما تبرز قصور التشريعات التقليدية وتقترح آليات قانونية حديثة لتعزيز الحماية ومواكبة التطور التكنولوجي. بينما تناولت في دراستي الطرق القانونية في مكافحة الجريمة السيبرانية.

صعوبـــات الـــدراســة

- قلة المراجع والدراسات المتخصصة باللغة العربية حول الموضوع نظرا لحداثته.
- صعوبة ضبط العناوين وهذا راجع للعناوين المختلفة في كل من المراجع العربية المتوفرة.
- تشابه الجرائم منها الإلكترونية والمعلوماتية والسيبرانية وإذا به المعلومات متكررة في كل مكن الجرائم هذه.
- صعوبة الإحاطة بجميع الأطر القانونية الدولية المختلفة والمتغيرة باستمرار.

الفصل الأول: الإطار العام للجريمة السيبرانية

الفصل الأول: الإطار العام للجريمة السيبرانية

شهد العالم في العقود الأخيرة تحولًا جذريًا على مستوى التكنولوجيا والاتصال، إذ أصبحت المعلومات الرقمية جزءًا أساسيًا من حياتنا اليومية، سواء على صعيد الأفراد أو المؤسسات أو الدول. هذا التحول وفر العديد من الفرص الاقتصادية والاجتماعية والتعليمية، ولكنه في الوقت نفسه أتاح مساحة واسعة لارتكاب سلوكيات غير مشروعة يُطلق عليها الجرائم السيبرانية.

تختلف هذه الجرائم عن الجرائم التقليدية في طبيعتها، إذ تعتمد على الوسائل الرقمية والشبكات الإلكترونية، وتتمتع بقدرة على تجاوز الحدود الجغرافية، ما يجعل كشفها وملاحقة مرتكبيها أكثر تعقيدًا، كما أن تطور التقنيات الحديثة أدى إلى تنوع صور هذه الجرائم وظهور أنماط مستحدثة لم تكن معروفة من قبل، مثل الهجمات السيبرانية المنظمة على البنوك والمؤسسات الحكومية، واستخدام البرمجيات الخبيثة والذكاء الاصطناعي لارتكاب الجرائم الرقمية.

ولذلك، أصبح من الضروري دراسة الجريمة السيبرانية من منظور شامل يربط بين الواقع العملي الذي تظهر فيه هذه الجرائم، والإطار القانوني الذي ينظمها ويحدد المسؤولية الجنائية لمرتكبيها. هذا الفصل يسعى إلى تقديم رؤية متكاملة عن الإطار المفاهيمي للجريمة السيبرانية، بداية من تحليل طبيعتها الواقعية، مرورًا بدراسة تطور صورها، وصولاً إلى الأطر القانونية التي تحدد أركانها وطبيعة المجرم السيبراني وسماته ودوافعه.

ومن خلال هذا الفصل سوف يتم التعرف على هذا الموضوع من خلال المبحثين:

المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية.

المبحث الثاني: الإطار القانوني للجريمة السيبرانية.

المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية

تُعتبر الجريمة السيبرانية نتيجة طبيعية لاستخدام التقنيات الرقمية بشكل واسع في الحياة اليومية، حيث توفر الشبكات الرقمية والأنظمة المعلوماتية بيئة خصبة لارتكاب أفعال غير مشروعة. وتتميز هذه الجرائم بقدرتها على التوسع والانتشار بسرعة، ما يجعلها تختلف عن الجرائم التقليدية من حيث الوسائل، نطاق الضرر، وطريقة الملاحقة. في هذا المبحث سنتناول طبيعة الجريمة السيبرانية من خلال دراسة مفهومها وتطور صورها بين الشكل التقليدي والأنماط المستحدثة.

المطلب الأول: مفهوم الجريمة السيبرانية

لفهم طبيعة الجريمة السيبرانية، يجب أولًا تحديد مفهومها الاصطلاحي واللغوي القانوني والفقهي، مع إبراز خصائصها وطبيعتها، وهو ما يسهل التمييز بينها وبين الجرائم التقليدية.

الفرع الأول: تعريف الجريمة السيبرانية

إن تحديد المفهوم الدقيق للجريمة السيبرانية من أكثر المسائل إثارةً للجدل في الفقه والقانون المقارن، نظرًا لحداثة هذا النوع من الجرائم وتشعّب أبعاده التقنية والقانونية وسيتم تعريفها بدءًا بالمعنى اللغوي أولًا، ثم الاصطلاحي ثانيًا، مرورًا بالتعريف الفقهي ثالثًا، وانتهاءً بالتعريف القانوني رابعًا.

أولا: تعريف الجريمة السيبرانية لغة

كلمة " **Cyber** " هي عبارة عن كلمة إنجليزية، وقد تم تعريف في قاموس أكسفورد [1] " **سيبراني** " " Cyber " على أنها صفة شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي. [2]

[1] Oxford English Dictionary, "**Cyber**", Oxford University Press, available at: https://www.oed.com , accessed on 22 February 2026.

[2] روان بنت عطية الله الصحفي، **الجرائم السيبرانية**، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، المملكة العربية السعودية، جدة، 2020، ص 7.

ثانيا: تعريف الجريمة السيبرانية اصطلاحا

يتألف مصطلح الجريمة السيبرانية من **شقين مترابطين**، يُشكّل كلٌّ منهما ركيزةً أساسية في بناء هذا المفهوم المركّب، فأما الشق الأول، وهو مصطلح "**الجريمة**"، فيعود في أصله اللغوي إلى مادة "**جَرَمَ**"، وتدل في جوهرها على معاني الجُرم والتعدي والذنب، ويجمع على "**إجرام**" و"**جروم**". أما في **السياق القانوني الجنائي**، فتُعرَّف الجريمة بوصفها " فعلاً غير مشروع، يصدر عن إرادة جنائية واعية ومتعمدة، ويُرتب عليه المشرع جزاءً جنائياً يتمثل في عقوبة محددة أو تدابير احترازية، وفقاً لما تقرره النصوص التشريعية النافذة " . [1]

أما **مصطلح** الجريمة السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الأنترنت الذي تعددت مصطلحاته وذلك لنشأة تطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات، وقد تمت صياغة المصطلح لأول مرة من قبل الكاتب " **ويليام جيبسون** " [2] في رواياته الخيالية عام 1982 ثم من قبل " **سوسمان وهيوستن**" [3]عام 1995 [4] ، حيث استخدم المصطلح بشكل أوضح في المجال القانوني والإعلامي ومنذ ذلك الحين اتسعت الحدود التي تحدد الجريمة السيبرانية.

ومع تطور المصطلحات المستخدمة جرى بذل جهود أكاديمية لتعريف الجريمة السيبرانية، ولابد لأي نهج عصري في هذا الشأن أن يسلم بأن تعبير الجريمة السيبرانية ليس مصطلح قانوني

---

[1] أيمن عبد الله فكري، **الجرائم المعلوماتية دراسة مقارنة بين التشريعات العربية والأجنبية**، ط1، مكتبة القانون والاقتصاد، الرياض، 2014، ص 82.

[2] هو كاتب وروائي أمريكي– كندي وُلد سنة 1948، ويُعد من أبرز رواد أدب الخيال العلمي ومؤسسًا لمفهوم الفضاء السيبراني (Cyberspace)، اشتهر بروايته Neuromancer التي أسهمت في ظهور أدب السايبربانك المرتبط بالتكنولوجيا والواقع الافتراضي.

[3] سوسمان هو باحث وأستاذ في علوم الحاسوب، عُرف بإسهاماته في مجال الأنظمة المعلوماتية والذكاء الاصطناعي، أمّا هيوستن فهو باحث اهتم بالقضايا المرتبطة بالتكنولوجيا والجرائم المعلوماتية، خاصة في سياق التطور الرقمي.

[4] Regner sabillon **Cybercrime and Cybercriminals A Comprechensive Study**. International Journal of Computer Networks and Communications Security, vol 4 no 6 2016 p6 .

قائم بذاته بل هو تعبير جامع يشمل مجموعة أفعال مرتكبة ضد بيانات أو نظم حاسوبية أو على استخدام موارد المعلومات لأغراض غير مشروعة. [1]

ثالثا: تعريف الجريمة السيبرانية فقها

يعرفها هالدر وجيشانكار على أنها " تلك الجرائم التي يرتكبها الأفراد والجماعات ضد الأفراد والجماعات والمنظمات التي لديها دوافع إجرامية لإلحاق الضرر المتعمد، أي الأذى الجسدي أو العقلي للضحية بشكل مباشر أو غير مباشر والذي يستخدم شبكات الاتصال مثل غرفة الدردشة ورسائل البريد الإلكتروني ولوحات الإعلانات والمجموعات والهواتف المحمولة للرسائل النصية القصيرة".[2]

عرفت أيضا على أنها: " نشاط إجرامي مصدره جهاز كمبيوتر أو شبكة كمبيوتر تستخدم للهجمات السيبرانية وقد تشمل الاحتيال والسرقة والابتزاز والتزوير والاختلاس، ولكن بسبب الوضع الافتراضي، ومن المعروف أنه من الصعب اكتشافه ومعاقبته بسبب التعقيد الفني والمهاجمين غير المرئيين الذين يجلسون على بعد آلاف الأميال". [3]

وعرفها البعض على أنها: " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود العرفان ". [4]

رابعا: تعريف الجريمة السيبرانية قانونا

أما بالنسبة **للتعريف الذي جاء به المشرع الجزائري** للجرائم المتصلة للتكنولوجيات الإعلام والاتصال فإنه **يعرفها بأنها:** " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في

---

[1] ماينو جيلالي وعروس كوثر، **الجريمة السيبرانية في صورها المستحدثة**، مجلة القانون والتنمية، مخبر القانون و التنمية، جامعة طاهري محمد بشار، المجلد 4، العدد 1، 2023، ص 53.

[2] Debarati Halder and K. Jaishankar, Cyber Crime and the Victimization of Women: Laws, Rights and Regulations, IGI Global, Hershey, 2012, p. 12.

[3] kundi, G. M Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries. Journal of Information Engineering and Applications, 4(4) 2014 .

[4] محمود أحمد العرفان، **الجرائم الإلكترونية**، دار وائل للنشر والتوزيع، عمان، 2017.

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 إرادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً.[2]

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

وقد عرف 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 وفقا لما ورد في المادة الأولى من القانون رقم 04-09 المتضمن الأحكام الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[5]

---

[1] محمد بوعمرة، سيد علي بينال، **جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري**، مذكرة التخرج لنيل شهادة الماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة أوكلي محمد أولحاج البويرة،2019-2020، ص ص 4 5.

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

[3] القانون **رقم 04 – 15** المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، العدد 71، المؤرخة في 10 نوفمبر 2004.

[4] مهدي رضا، **الجرائم السبيرانية وآليات مكافحاها في التشريع الجزائري**، مجلة ايليزا للبحوث والدراسات، المجلد 6، العدد 2، جامعة محمد بوضياف، المسيلة، الجزائر، 2021، ص 113.

[5] القانون **04 – 09** المؤرخ في 05 أوت 2009، يتضمن **قانون الوقاية من الجرائم المتصلة بتكنلوجيا الاعلام والاتصال ومكافحتها**، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، المؤرخة في 16 أزوت 2009.

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 القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات. [1] 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.[2]

الفرع الثاني: خصائص الجريمة السيبرانية

لا يكفي تعريف الجريمة السيبرانية للإحاطة بها من جميع جوانبها، بل لا بدّ من الوقوف عند **خصائصها** المميّزة التي تجعلها تنفرد عن غيرها من الجرائم التقليدية، وهي خصائص فرضتها طبيعة الفضاء الرقمي الذي تُرتكب فيه ويُفرد في هذا الفرع **أبرز الخصائص** التي تتّسم بها الجريمة السيبرانية، والتي تُلقي بظلالها على مسائل الإثبات والملاحقة القضائية والاختصاص.

أولا: الجريمة السيبرانية يصعب إثباتها

فهي لا تترك أثرًا ماديًا ملموسًا، كما أن تحديد مكان وقوعها أو التعامل معها معقد بسبب اتساع نطاقها وضخامة البيانات [3]، وغالبا ما يتم اكتشافها بالصدفة، وتعقبها يتطلب خبرة فنية عالية، وهوا ما يفتقر إليه المحقق العادي لتعامل معها.[4]

---

[1] العيد شعثان، مسعود موفقي، **الجرائم السيبرانية في القانون الجزائري**، مذكرة ماستر في القانون الجنائي والعلوم الجنائية، جامعة زيان عاشور، الجلفة، الجزائر، 2021 – 2022، ص 14.

[2] رحيمة نميلي، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة**، مداخلة في المؤتمر الدولي، 14 طرابلس، عنوان الجرائم الإلكترونية طرابلس، يومي 24 و25 مارس، 2017 ص 100.

[3] إبراهيم خالد ممدوح، **الجرائم المعلوماتية**، الإسكندرية، دار الفكر الجامعي، 2009، ص 79.

[4] هشام محمد فريد رستم، الجرائم المعلوماتية، **أصول التحقيق الجنائي الفني وآليات التدريب التخصصي للمحققين**، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد 2، 1999، ص 11.

ثانيا: الجريمة السيبرانية جريمة مستحدثة

الجرائم السيبرانية تعتبر من أبرز أنواع الجرائم الحديثة والتي يمكن أن تشكل خطرا وخاصة في ظل العولمة، فليس غريبا أن تعتبر الجرائم السيبرانية سواء التي تتعرض لها أجهزة الكمبيوتر أو التي يتم فيها تسخير تلك الأجهزة في ارتكابها من الجرائم المستحدثة، إذ أنه ومع التقدم التكنولوجي الذي تحقق خلال الفترة الماضية جعل العالم بمثابة قرية صغيرة، مما جعل هذا التقدم يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، وأصبح يهدد أمنها وأمن المواطنين.[1]

ثالثا: الجريمة السيبرانية عابرة للحدود

فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع الحرس الحدود، وهو خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى شكليات تتعلق بإجراءات الملاحقة القضائية وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.[2]

ومن **الأمثلة** على هذه الجرائم العابرة للحدود تمكن أحد الهواة في أوربا من حل شفرة أحد مراكز المعلومات في **البنتاجون** ومن ثم أصبح المجال أمامه مفتوحا للعبث ببيانات هذا المركز.[3]

رابعا: الجريمة السيبرانية جريمة ناعمة وسهلة الارتكاب

لا تتطلب أي جهد عضلي أو عنف، كما هو الحال في الجرائم التقليدية [4]، بل يكفي أن يمتلك المجرم المعلوماتي قدرة تقنية على التعامل مع جهاز الحاسوب، وتعتبر من الجرائم

---

[1] إبراهيم خالد ممدوح المرجع السابق، ص 86.

[2] غانم مرضي الشمري، **الجرائم المعلوماتية، ماهياتها، خصائصها، كيفية التصدي لها قانونيا**، ط1، الدار العلمية والدولية للنشر والتوزيع، عمان، 2016، ص37.

[3] غانم مرضي الشمري، المرجع السابق، ص 37.

[4] هي الجرائم التي تُرتكب بالوسائل والأساليب التقليدية المعروفة، دون الاعتماد على الأنظمة المعلوماتية أو الوسائط الإلكترونية، كالسرقة والقتل والاحتيال التقليدي .

"النظيفة"، لأنها ترتكب في صمت دون آثار مادية، بل تتمثل فقط في تغيرات رقمية داخل ذاكرة الأجهزة.[1]

وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف **مثل** ما ذهب إليه **مكتب التحقيقات الفيدرالي** بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف.[2]

خامسا: الجريمة السيبرانية جريمة الأذكياء

يمتاز مرتكبو هذا النوع من الجرائم بذكاء عالٍ وقدرة على التحكم في الأجهزة الإلكترونية، ما يسمح لهم بتنفيذ أفعالهم بدقة واحترافية، وتحقيق أهدافهم بهدوء دون إثارة فوضى أو استعمال للعنف.[3]

سادسا: قلة الإبلاغ عن الجريمة السيبرانية

أنها غالبًا لا تكون محل تبليغ أو شكوى عند وقوعها؛ فقد لا ينتبه الضحية لحدوثها أصلًا، أو يتردد في الإبلاغ خوفًا من التشهير، [4] لذلك، تُكتشف العديد من جرائم الإنترنت بمحض الصدفة، وأحيانًا بعد مرور فترة زمنية طويلة على ارتكابها. كما أن عدد الجرائم التي تبقى غير مكتشفة يفوق بكثير تلك التي يتم الكشف عنها، مما يجعل الفجوة بين العدد الحقيقي للجرائم المرتكبة وتلك المعلن عنها والمعروفة بالرقم المظلم فجوة خطيرة.[5]

---

[1] سيناء عبد الله محسن، **المواجهة التشرعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية**، الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر، الدار البيضاء، المملكة المغربية، 2007، ص 52.

[2] مفتاح بوبكر المطردي، **الجريمة الإلكترونية والتغلب على تحدياتها**، مقال مقدم الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-25-09-2012، ص 31.

[3] عميمر عبد القادر، المرجع السابق، ص 43.

[4] أمير فرج يوسف، **الجريمة الإلكترونية والمعلوماتية والجهود الجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت**، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص 157.

[5] عبد الرحمان جميل محمود حسين، **الحماية القانونية برامج الحاسب الآلي**، مذكرة ماجستير جامعة النجاح الوطنية نابلس، فلسطين، كلية الدراسات العليا، 2008، ص 09.

وتتجلى هذه الظاهرة بشكل أوضح داخل المؤسسات المالية، **مثل** البنوك ومؤسسات الادخار والإقراض والوساطة، إذ تميل إداراتها في كثير من الأحيان إلى تجنب الكشف عن هذه الجرائم أو اللجوء إلى القضاء بشأنها، خشية ما قد تسببه الدعاية السلبية من تراجع ثقة العملاء وانصرافهم عنها[1]. وبالتالي فإن الإبلاغ في هذه الجرائم يكون قليلا بالنسبة للجرائم الأخرى وهذا راجع إلى ما يتعرض له المجني عليه كطرف في الجريمة من تشهير فيما لو أبلغ عن الجريمة.[2]

الفرع الثالث: الطبيعة القانونية للجريمة السيبرانية

هناك ما يميز الجريمة السيبرانية عن غيرها من الجرائم التقليدية باعتبارها جريمة مستحدثة ما جعلها تكتسب طابعا قانونيا خاصا بها وهذا ما سنراه.

أولا: الطبيعة القانونية الخاصة بالجريمة السيبرانية

تُعد الطبيعة القانونية للجريمة السيبرانية من أهم الإشكالات المطروحة في ظل الانتشار الواسع لتقنيات المعلومات والاتصال، إذ تعكس تحولًا جوهريًا في مفهوم الجريمة من طابعها التقليدي إلى نمط رقمي أكثر تعقيدًا وتشابكًا.[3]

تتميّز الجريمة السيبرانية بكونها لا تُعدّ مجرد امتداد آلي حديث للجرائم التقليدية، بل تمثل في حقيقتها نتاجًا مباشرًا لتقنيات المعلومات، إذ تقوم عليها وترتبط بها ارتباطًا وثيقًا، وقد أكسبها ذلك طابعًا قانونيًا خاصًا يميزها عن غيرها من الجرائم التقليدية.[4]

فإذا كانت الجريمة، بوجه عام، تخضع لأحكام القانون الجنائي، فإن الطبيعة المتميزة للجريمة السيبرانية تجعلها، في الغالب، تندرج ضمن إطار ما يُعرف بالقانون الجنائي السيبراني.

---

[1] محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت**، ط2، دار النهضة العربية، القاهرة، مصر، 2009، ص 37.

[2] قاسحي فيروز، **الجريمة الالكترونية عبر مواقع التواصل الاجتماعي**، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة الجزائر 3، العدد 8، المجلد 7، 2023، ص ص 206 207.

[3] نورهان محمد الربيعي، **الجريمة السيبرانية وآليات مكافحتها دراسة مقارنة**، مجلة الفرابي للعلوم الإنسانية، المجلد 03، العدد 01، كلية الحقوق، جامعة عجمان، الإمارات العربية المتحدة، 2024، ص 81.

[4] سعيداني نعيم، **آليات البحث والتحري في الجريمة المعلوماتية في القانون الجزائري**، مذكرة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 30.

وقد أضفى هذا المعطى على هذا النوع من الجرائم خصوصية قانونية واضحة، سواء من حيث بنيتها الذاتية، أو من حيث طبيعة المحل الذي يقع عليه الاعتداء عند ارتكابها.[1]

وترتبط الجرائم السيبرانية ببيئة رقمية تعتمد على أنظمة المعالجة الإلكترونية للبيانات، حيث يتم الاعتداء عبر وسائل تقنية مثل التلاعب بالبرمجيات أو البيانات أو استخراجها بطرق غير مشروعة. ويكون محل هذه الجرائم إما البيانات والمعلومات أو البرامج أو حتى البنية التحتية الرقمية. كما يظهر ذلك بوضوح عند الحديث عن المال المعلوماتي الذي ينقسم إلى مال معنوي غير ملموس يتعلق بالمحتوى الرقمي، ومال مادي يمس الأجهزة والبنية التقنية الحاملة للمعلومة.[2]

ثانيا: موقف المشرع الجزائري من الجريمة السيبرانية

أمام الفراغ القانوني الذي كان قائمًا في مجال الجرائم المرتبطة بالتكنولوجيا، بادر المشرّع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15، حيث أدرج قسمًا سابعًا مكررًا تحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات**"، وقد أوضح عرض أسباب هذا التعديل أن التطور التكنولوجي المتسارع وانتشار وسائل الاتصال الحديثة أسهما في بروز أنماط جديدة من الإجرام، الأمر الذي استدعى تدخلًا تشريعيًا لمواجهتها.

وفي هذا الإطار، انطلق المشرّع الجزائري من اعتبار أن **جوهر المعلوماتية** يتمثل في" **المعطيات**" التي تُدخل إلى الحاسوب لتُعالج وتُخزَّن، ثم تتحول إلى معلومات، فعمل على إضفاء الحماية القانونية عليها بمختلف صورها. ولهذا، **تبنّى مصطلح " المساس بأنظمة المعالجة الآلية للمعطيات**"، وهو مصطلح يشمل وفق دلالته كلًا من المعطيات ذاتها والأنظمة التي تحتويها، بما في ذلك شبكات المعلومات.

---

[1] سعيداني نعيم، المرجع السابق، ص 30.

[2] فريد روابح، **محاضرات في القانون الجنائي العام**، مطبوعة دروس للسنة الثانية ليسانس، قسم الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر، 2025-2026، ص 89.

غير أن هذا التوجه أدى إلى حصر نطاق التجريم في الأفعال التي تمثل اعتداءً مباشرًا على النظام المعلوماتي، مستبعدًا بذلك الجرائم التي يُستَخدم فيها النظام المعلوماتي كوسيلة لارتكابها دون أن يكون هو محل الاعتداء.[1]

المطلب الثاني: تطور صور الجريمة السيبرانية

تتطور الجريمة السيبرانية باستمرار مع انتشار استخدام الإنترنت والتقنيات الرقمية الحديثة، فبينما كانت بعض الجرائم موجودة قبل ظهور البيئة الرقمية، ظهرت أنماط جديدة تعتمد على تقنيات متقدمة مثل البرمجيات الخبيثة والهجمات المنظمة على المؤسسات لذا يُعنى هذا المطلب لدراسة تطور صور الجريمة السيبرانية بين الشكل التقليدي والأنماط المستحدثة.

الفرع الأول: الجريمة السيبرانية في صورتها التقليدية

يشكّل هذا الفرع مدخلاً لفهم صور الجريمة السيبرانية التقليدية التي ارتبطت ببدايات تطور الفضاء المعلوماتي، حيث استهدفت أساساً سلامة وسرية البيانات، وتتمثل هذه الصور في التزوير المعلوماتي والتجسس السيبراني وسرقة المعلومات، وهي أفعال تعكس النمط الأولي للجريمة الرقمية قبل تطورها وتعقدها لاحقاً، وهو ما سوف نتطرق إليه بشيء من التفصيل في النقاط التالية:

أولا: التزوير المعلوماتي (السيبراني)

التزوير يقوم على تغيير الحقيقة بقصد الغش في محرر بطريقة بينها القانون تغيير يؤدي إلى إلحاق الضرر بالغير.[2]

وتغيير الحقيقة سواء كان في محرر رسمي أو عرفي، يمكن تصور حصوله في محررات في نطاق المعلوماتية، وهذه الحالة تسمى جريمة التزوير المعلوماتي، وهو ينصب على مخرجات

[1] عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، في ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، تخصص إدارة التحقيقات الاقتصادية والمالية، جامعة ورقلة، 2018-2019، ص17.

[2] محمد صبحي نجم، **شرح قانون العقوبات**، القسم الخاص، ديوان المطبوعات الجامعية، الجزائر،2005، ص 3.

الحاسب الآلي عن طريق تغيير الحقيقة على الشرائط والمستندات طالما أن التغيير ذاته قد طال البيانات الموجودة في جهاز الحاسب الآلي، شرط حصول ضرر والذي يتمثل في اهتزاز الثقة المفترضة في المحررات الرسمية.[1] حيث تجاوز التزوير الإلكتروني التزوير الورقي أن كان هو نفسه في المفهوم الوظيفي لناحية تحريف الحقائق والبيانات، فهو لم يعد مجرد حك في مضمون السند وتعديل بعض كلماته، أو حذف بعض عباراته، بل أصبح يتطلب التعامل مع تقنيات المعلوماتية وذلك عن طريق محو بيانات وإضافة بيانات أخرى مكانها، ودمج بيانات مما يصعب من إمكانية كشفه ، شأنه شأن سائر الأعمال الجرمية التي ترتكب في مجالا لمعلوماتية . [2]

ثانيا: التجسس السيبراني

يعرف سلوك التجسس فعل إيجابي قوامه الكشف واستظهار الحقائق المخفية، ولكنه كشف واستظهار غير مشروع، إما بوسائله أو غاياته، وهو لذلك فعل لا يقره الشارع ويفرد لمرتكبه العقوبة الجزائية الرادعة دون تهاون انسجاما مع روح التشريع، وإدراكا لعظم خطورة هذا السلوك.[3]

فالحاسب الآلي خزانة بلا أبواب أو مستودع بلا جارس، ولذلك استطاع أطفال لم يتجاوزوا العاشرة من عمرهم التجسس على وزارة الدفاع الأمريكية، لأن اختراق شبكات المعلومات أمر يسير لمن يتوصل من خلال التجسس أو من خلال الصدفة البحتة على كيفية هذا الاختراق. [4]

---

[1] عبد الفتاح، بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت**، بهجات للطباعة والتجليد، مصر، 2009، ص 146.

[2] بولين انطونيوس أيوب، **الحماية القانونية للحياة الشخصية في مجال المعلوماتية**، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت لبنان، 2009، ص ص 176 177.

[3] sophie Harleman, **Countering Economic Cyber Espionage and the Right to Privacy**, PhD Dissertation, Utrecht University, Netherlands, 2025, p 34

[4] محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب الآلي**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2001، ص87.

أما الأسرار السياسية وأسرار نظم الحكم داخل الدول فيدخل في ذلك أيضا إدخال المعلومات المتعلقة بوثائق الدولة في الحاسب الآلي وعندئذ تقوم الدول الأخرى في الوصول إلى هذه البيانات المعالجة الكترونيا من اجل الوقوف على أسرار الدولة ونظام الحكم فيها. [1]

وعليه يتم القول هي جرائم التي يتم بواسطتها اختراق أجهزة المستخدمين بطرق غير شرعية ولأغراض غير سوية، من أجل سرقة المعلومات تتعلق بذلك المستخدم سواء على الصعيد الشخصي أو السياسي أو العلمي أو الاجتماعي حيث لم يعد هناك سرية يمكن الاحتفاظ بها من دون أن يقوم الشخص بعمليات كثيرة لتجنب عمليات التجسس أو " **الهاكرز**".[2]

ثالثا: سرقة المعلومات

إن الصورة الغالبة لسرقة المال المعلوماتي المعنوي إن أمكن الوصف تأخذ صورة اختلاس البيانات والمعلومات والإفادة منها باستخدام السارق المعلومات الشخصية، **مثل** الاسم اللقب العنوان الأرقام السرية الخاصة بالمجني عليهم والاستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الأنترنت بحيث تؤدي بالغير إلى تقديم الأموال الإلكترونية والمادية إلى الجاني عن طريق التحويل البنكي. [3]

تتفق السرقة المعلوماتية مع السرقة التقليدية في أوجه كثيرة إلا أن اختلافهما يكون في محل السرقة ذاته، فمحل السرقة التقليدية مال منقول مملوك للغير، أما محل السرقة عبر الأنترنت فهي المعلومات والبيانات المعالجة إلكترونيا.[4]

---

[1] جلال محمد الزعبي، وأسامة أحمد المناعسة، **جرائم تقنية نظم المعلومات الإلكترونية**، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان الأردن، 2010، ص 256.

[2] نسيمة مقبل، **الجرائم السيبرانية في الفضاء الاتصالي الجزائري**، أنواعها، آثارها وسبال مواجهتها، مجلة معارف، العدد 21، المجلد 18، كلية علوم الإعلام والاتصال، جامعة الجزائر3، الجزائر، 2023 ص 1106.

[3] محمد أمين الشوابكة، **جرائم الحاسوب والأنترنت، الجريمة المعلوماتية**، الإصدار 2، دار الثقافة للنشر والتوزيع، عمان، الأردن،2007، ص 138.

[4] خديجة دحمان صباحية، **جرائم السرقة والاحتيال عبر الأنترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري**، رسالة ماجستير، جامعة الجزائر، كلية الشريعة والقانون، ص 10.

الفرع الثاني: الجريمة السيبرانية في أنماطها المستحدثة

لم تعد الجريمة السيبرانية حكراً على صور بعينها كالقرصنة وسرقة البيانات، بل امتدت لتشمل أنماطاً مستحدثة تجمع بين التطور التقني والخطورة البالغة على الأفراد والمجتمعات والدول. ومن أبرز هذه الأنماط: الحروب والإرهاب السيبراني، والجرائم المرتبطة بالذكاء الاصطناعي، وجرائم العملات المشفرة، وما توفره أسواق الشبكة الخفية من بيئة مواتية للنشاط الإجرامي، وصولاً إلى توظيف التكنولوجيا في تيسير الاتجار بالأشخاص. وهذا ما سيتطرق له هذا الفرع تباعاً.

أولا: الحروب السيبرانية والإرهاب السيبراني

أحدث التطور التكنولوجي تحولات عميقة في طبيعة الحروب والصراعات البشرية عبر مختلف العصور، حيث انتقلت من الحروب التقليدية التي كانت تعتمد على السيوف والرماح، إلى استخدام البنادق والرشاشات، ثم تطورت لاحقًا إلى الأسلحة النووية والصواريخ العابرة للقارات. ومع هذا التطور، برز شكل جديد من الحروب يتمثل في الحروب السيبرانية، التي تعتمد على أدوات وأساليب مختلفة، **أبرزها** فيروسات الحاسوب والبرمجيات الخبيثة. وتتميز هذه الأسلحة الرقمية بقدرتها على إحداث أضرار جسيمة قد تضاهي، بل وقد تتجاوز في بعض الحالات، آثار الأسلحة التقليدية من حيث حجم الدمار والتأثير. [1]

تختلف الحروب السيبرانية عن الحروب التقليدية في كون المفهوم التقليدي للحرب يقوم على استخدام الجيوش النظامية، وارتباطه عادة بإعلان صريح لحالة الحرب، إضافة إلى وجود ميدان قتال محدد وواضح، في حين تتسم هجمات الفضاء الإلكتروني بالغموض وعدم تحديد نطاقها أو أهدافها بشكل دقيق. كما تعتمد هذه الحروب على أسلحة إلكترونية حديثة تتماشى مع متطلبات

[1] إيهاب خليفة، **مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي**، ط1 العربي للنشر والتوزيع، القاهر، مصر، 2019، ص 14.

العصر الرقمي وتسارع التطور التكنولوجي. [1] ويستخدم هذا التنظيم وسائل التكنولوجيا بغرض التجنيد ونشر فكرة في أوساط الشباب، وكان بإمكان حملاته في بعض الأحيان أن تكون كافية لإثارة أعمال العنف والخوف والرعب لدى الدول المجتمعات.[2]

ثانيا: الجرائم المرتبطة بتقنية الذكاء الاصطناعي

أصبحت كيانات الذكاء الاصطناعي حقيقة وواقع فرض نفسه بعد أن كانت ضربًا من الخيال، حتى أننا بتنا نشاهد استخدام هذه التطبيقات الذكية في كثير من المجالات سواء الطبية أو الصناعية أو العسكرية، وكذلك التعليمية وغيرها من المجالات المختلفة.[3]

وقد ظهر مصطلح الذكاء الاصطناعي للمرة الأولى في مؤتمر عقد في دارت موث كوليدج، هانوفر، نيوهامشر في عام 1956، ثم توقف الاستثمار في أبحاثه وقل الاهتمام بها في ستينيات القرن الماضي ثم عاد للانتشار في العصر الحالي، حيث تستخدم فيه التكنولوجيا والتقنيات والبرمجيات المعقدة وقد يستحيل فيه تمييز الحقيقة عن الكذب، إنه عصر التزييف العميق أو أن التزييف العميق أو تقنية الديب فيك " **Deep fake** ".[4]

ويمكن القول تعريف الذكاء الاصطناعي: " قدرة الآلة على التصرف مثل البشر أو القيام بأفعال تتطلب ذكاء" [5] . لكن تعريف المفهوم تطور بنفس الوتيرة التي عرفها التطور التكنولوجي لتكون نقطة الالتقاء بين كل التعاريف الحديثة هي" محاولة تقليد السلوك البشري الذكي " [6] ،

---

[1] يحي ياسين مسعود، **الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني**، مجلة القانونية، جامعة القاهرة، المجلد 4، العدد 4، 2018، ص 74.

[2] غريب حكيم، **الإرهاب السبيراني والأمن الدولي التهديدات العالمية الجديد وأساليب المواجهة**، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، العدد 2، المجلد 5، 2018، ص ص 103 104.

[3] ممدوح حسن العدوان، **المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي**، مجلة الشريعة والقانون، جامعة الإمارات، العدد 2019، ص 149.

[4] أحمد محمد فتحي الخولي، **المسؤولية المدنية الناجمة عن الإستخدام غير المشروع لتطبيقات الذكاء الإصطناعي**، الديب فيك نموذجا، مجلة البحوث الفقهية والقانونية، العدد 36، 2021، ص 256.

[5] Stuart Russell & Peter Norvig, **Artificial Intelligence: A Modern Approach**, 3rd ed., Pearson Education, New Jersey, 2010, p. 2.

[6] Elaine Rich & Kevin Knight, **Artificial Intelligence**, 2nd ed., McGraw-Hill, New York, 1991, p. 3

ويمكن الوقوف عند أربعة أنواع من الأنظمة الذكية وهي: الأنظمة التي تفكر مثل البشر؛ الأنظمة التي تتصرف مثل البشر؛ الأنظمة التي تفكر بعقلانية؛ الأنظمة التي تعمل بعقلانية.[1]

وتُعد جرائم الذكاء الاصطناعي من جرائم المستقبل القريب، ويثير هذا التطور إشكالات قانونية معقدة، تتمثل أساسًا في تحديد المسؤولية الجنائية عند ارتكاب هذه الأنظمة لأفعال مجرّمة، وما إذا كان يمكن مساءلة المستخدم أو المطور أو الجهة المصنعة، كما يطرح في الوقت نفسه إشكالية منح الذكاء الاصطناعي شخصية قانونية اعتبارية، في ظل عجز القوانين التقليدية عن مواكبة هذا النوع من التطور التقني المتسارع.[2]

ثالثا: جرائم العملات المشفرة

المشرع الجزائري اكتفى بتعريف العملة الافتراضية في القانون 17-11 المتضمن قانون المالية لسنة 2018، في المادة 117 منه، حيث جاء على أنها العملة الافتراضية هي العملة التي يستخدمها أفراد الإنترنت عبر شبكة الإنترنت، وتتميز بعدم وجود دعم مادي **مثل** القطع النقدية أو الأوراق المالية، كما أنها لا تعتمد على عمليات الدفع بواسطة الصكوك أو البطاقات البنكية.[3]

ونظراً لأهمية هذا الموضوع فقد تم إدراجه من طرف الأمم المتحدة، ممثلة في لجنة منع الجريمة والعدالة الجنائية، ضمن أبرز الأشكال المستحدثة للجريمة على المستوى العالمي.[4]

وتُسهم درجة إخفاء الهوية التي توفرها العملات المشفرة وانخفاض قابلية تتبع المستخدمين في تسهيل غسل الأموال وتمويل الإرهاب داخل الفضاءات الرقمية، كما قد تُستغل في جرائم

---

[1] أمل فوزي أحمد عوض، **الملكية الرقمية في عصر الذكاء الإصطناعي، تحديات الواقع والمستقبل**، إصدارات المركز الوطني الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، المحرر، برلين ألمانيا، 2021، ص4.

[2] يحي إبراهيم دهشان، **المسؤولية الجنائية عن جرائم الذكاء الاصطناعي**، مجلة الشريعة والقانون، جامعة الإمارات، 2019، ص 5.

[3] القانون رقم 17-11 المؤرخ في 27-12-2017، والمتضمن **قانون المالية** للسنة 2018، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، عدد 76، المؤرخ في 28-12-2017.

[4] Elena Martellozzo, **Cybercrime and Its Victims: Understanding the Global Phenomenon and Responses of International Institutions**, PhD Thesis, Middlesex University, United Kingdom, 2019, p. 41.

أخرى كالابتزاز والاحتيال، مما يفرض تحديات على الجهات المختصة في تعزيز الرقابة والتعاون الدولي. وإضافة إلى ذلك، توفر الشبكة المظلمة بيئة ملائمة لتجارة المخدرات عبر العملات المشفرة مع ضمان سرية التبادل والتسليم.[1] حيث أيضا تقوم بتسهيل ارتكاب العديد من الجرائم، نظرًا لسهولة تداولها.[2]

أكدت مجموعة العمل المالي FATF أن هذه العملات تستعمل لتمويل الإرهابيين وإخفاء محاصيلهم الجرمية فقد تم الكشف عن عمليات تمويل لتنظيم الدولة الإسلامية ومجموعات إرهابية أخرى [3] .

يُعدّ استغلال الأطفال في المواد الإباحية عبر شبكة الإنترنت مشكلة عالمية، وقد أدّى تطور التقنيات الحديثة إلى زيادة كبيرة في إمكانية الحصول على هذه المواد غير المشروعة وتوزيعها وبيعها، مما ساهم في تفاقم هذه الظاهرة.[4] وأشار تقرير اليونيسف لسنة 2017 حول حالة الأطفال إلى أن من أبرز التحديات في مكافحة الجرائم الجنسية ضد الأطفال على الإنترنت، الاستخدام المتزايد للعملات المشفّرة ومنصات التشفير داخل الشبكة المظلمة. [5]

رابعا: الجرائم المرتبطة بأسواق الشبكة الخفية

تُوفّر شبكة الإنترنت إمكانيات جديدة لعمليات بيع وشراء السلع بطرق غير قانونية، سواء عبر الشبكة الظاهرة أو عبر الشبكة الخفية المعروفة بـ " **الدارك نت**"[6]. وعلى خلاف الشبكة

---

[1] الأمم المتحدة 2020، **دليل المناقشة لمؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية**، كيوتو، اليابان، 20 أبريل 2020، ص 54.

[2] توفيق شرف شمس الدين، **مخاطر العملات الافتراضية**، كتاب واقع المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية، جامعة الشارقة، حول العملات الافتراضية في الميزان، يومي الثلاثاء والأربعاء 16 و17 أبريل 2019، ص 673.

[3] مارلين أورديكيان، **العملات الافتراضية المشفرة في الحقل الجنائي السيبراني**، مجلة الدفاع الوطني، العدد 108، 2019، ص 77.

[4] إبراهيم رمضان إبراهيم عطايا، **الجريمة الإلكترونية وسبل مواجهتها في السريعة الإسلامية والأنظمة الدولية**، دراسة تحليلية تطبيقية، مجلة كلية الشريعة والقانون بطنطا، المجلد 30، العدد 2، 2015، ص 1116.

[5] اليونيسف، **تقرير حالة الأطفال لعام 2017**، الأطفال في عالم رقمي، ص 79.

[6] و هو جزء مخفي من الإنترنت لا يمكن الوصول إليه عبر المتصفحات العادية، ويعتمد على شبكات وتقنيات خاصة و تتكوّن من طبقات مشفّرة وغير مرئية تُخفي هوية المستخدمين وتؤمّن قدرًا عاليًا من السرية .

الظاهرة، والتي يُطلق عليها أيضاً "**الشبكة السطحية**"، وتضم محتوى متاحاً للعامة وتقوم محركات البحث بفهرسته بشكل مباشر.[1]

وتتيح أسواق الشبكة الخفية التي توصف أيضاً باسم "**الأسواق المشفرة**" للمشترين والبائعين عدم الكشف عن هويتهم، وفي تلك الأسواق، تُستخدم العملات المشفرة أساساً لدفع ثمن المشتريات لتيسير بيع وتداول سلع من قبيل الأسلحة والمخدرات غير المشروعة. [2]

ومن أمثلتها: تُعد قضية Silk Road seizure من أشهر الجرائم المرتبطة بالعملات المشفرة، حيث استُخدمت منصة إلكترونية سرية عبر الإنترنت المظلم في بيع المخدرات والسلع غير القانونية باستخدام عملة البيتكوين لتسهيل الدفع وإخفاء الهوية. وفي سنة 2013، تمكنت السلطات الأمريكية من إغلاق المنصة واعتقال مؤسسها، لتصبح القضية مثالًا بارزًا على استغلال العملات المشفرة في الأنشطة الإجرامية.[3]

خامسا: استخدام التكنولوجيا بغرض تيسير الاتجار بالأشخاص

يُعدّ الاتجار بالبشر واحداً من أبرز صور الجريمة المنظمة العابرة للحدود، والتي شهدت في السنوات الأخيرة توسعاً ملحوظاً في نطاق انتشارها، باعتبارها جريمة ذات طابع عابر للقارات، إذ لم تعد هناك أي منطقة جغرافية في العالم بمنأى عن هذا النوع من الجرائم الذي يُصنّف كشكل حديث من أشكال الاسترقاق، وقد جرى تجريمه في العديد من الاتفاقيات والمواثيق الدولية لما يمثله من انتهاك جسيم لحقوق الإنسان. [4]

---

[1] رامي متولي القاضي، **مكافحة الإجرام المنظم عبر شبكة الأنترنيت المظلمة**، المجلة الجنائية القومية، المجلد 64، العدد 3، 2021، ص 48.

[2] الأمم المتحدة مؤتمر الأمم المتحدة 14، المرجع السابق، ص 30.

[3] وزارة العدل الأمريكية، قضية إغلاق منصة Silk Road المرتبطة بالاتجار غير المشروع عبر الإنترنت المظلم، 2013، مقال في الموقع: https://www.justice.gov/ تم الاطلاع 23-03-2026 الساعة 04:50.

[4] أمحمد أقبلي، عابد العمراني الميلودي، **القانون الجنائي الخاص المعمق في شروح**، ط 1، دار الرشاد، المغرب، 2020، ص 57.

وتبرز الخطورة البالغة لجريمة الاتجار بالبشر في كونها تُعدّ، لدى جماعات الجريمة المنظمة، من الأنشطة الإجرامية التي تدرّ أرباحاً مالية ضخمة، وفي الوقت نفسه تنطوي على مخاطر أقل مقارنةً بجرائم أخرى مثل تهريب الأسلحة أو الاتجار بالمخدرات. [1]

المبحث الثاني: الإطار القانوني للجريمة السيبرانية

للتعامل مع الجريمة السيبرانية بشكل فعّال، يجب فهم الإطار القانوني الذي يحدد أركانها وطبيعة المجرم السيبراني وسماته ودوافعه، يتيح هذا التحليل فهم كيفية تطبيق القانون على الجرائم الرقمية، وتوضيح مسؤولية الجاني، سواء كان من الهواة أو المحترفين أو العصابات المنظمة، وفق الأطر القانونية الحديثة.

المطلب الأول: أركان الجريمة السيبرانية

تشكل أركان الجريمة السيبرانية الركيزة الأساسية لتحديد المسؤولية الجنائية، وتشمل الركن الشرعي الذي يحدد الأفعال المجرمة، الركن المادي الذي يمثل الفعل نفسه، والركن المعنوي الذي يعكس القصد لدى الجاني.[2]

الفرع الأول: الركن الشرعي

يقصد بالشرعية الجزائية الصفة غير المشروعة للفعل، بحيث لا يُعدّ أي سلوك جريمة إلا إذا وجد نص قانوني يجرّمه ويُحدد العقوبة المقررة له، وذلك تجسيدًا لمبدأ "**لا جريمة ولا عقوبة إلا بنص**". وبالتالي، إذا انتفى التجريم انتفت المسؤولية الجزائية عن مرتكب الفعل، ويُعد هذا المبدأ ضمانة أساسية لحماية حقوق الأفراد وصون الحريات الفردية، إذ إن ملاحقة الأفعال وتوقيع العقوبات يجب أن يستندا إلى قوانين صادرة عن السلطة التشريعية تُحدد الأفعال المجرّمة والعقوبات المترتبة عليه.[3]

---

[1] شريف سيد كمال، **الجريمة المنظمة في القانون المقارن**، ط1، دار النهضة العربية، مصر، 2001، ص 139.

[2] John Smith, **Cybercrime and Criminal Liability in Digital Environments**, Doctoral dissertation, University of Oxford, United Kingdom, 2019, p. 45.

[3] مهداوي حنان، **التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري**، مجلة الفكر القانوني والسياسي، جامعة محمد لمين دباغين، سطيف، كلية الحقوق والعلوم السياسية، العدد 02، المجلد 06، 2022، ص1064.

مما يعني جرّم القانون رقم 06-24 بعض صور الجرائم المعلوماتية، وحدّد العقوبات المقررة لمرتكبيها ضمن القسم السابع مكرر المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات" ، الوارد في الفصل الثالث المتعلق بـ "الجنايات والجنح ضد الأموال" من الباب الثاني الخاص بـ "الجنايات والجنح ضد الأفراد"، وذلك من خلال المواد الممتدة من 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدّل والمتمّم. [1]

في المقابل، جاء القانون رقم 09-04 المشار إليه سابقًا متضمنًا جملة من القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، باعتباره إطارًا وقائيًا يهدف إلى الحد من وقوع الجرائم المعلوماتية.

وإن لجوء المشرّع إلى تقنين الجرائم المعلوماتية والنص عليها صراحةً ضمن إطار مبدأ الشرعية الجزائية يترتب عليه منع القاضي من اللجوء إلى القياس في المجال الجنائي.[2]

الفرع الثاني: الركن المادي

عرفه الفقهاء على أنه كل فعل ينتج عنه توقيف نظام المعالجة الآلية للمعطيات عن أدائه الطبيعي، وبالرغم من الجهد الفقهي الذي صاحب مفهوم النظام المعلوماتي، حول شموله جل عناصره من عدمه، إلا أن غالبية الفقه ترى بضرورة عدم اشتراط أن يقع فعل التفضيل أو الإضرار للنظام جملة، بل يكفي أن يؤثر على أحد عناصره فقط، كجهاز الحاسوب نفسه أو تمتد إلى شبكات الاتصال أو البرامج والمعطيات.[3]

كما أن الركن المادي يختلف من حالة إلى أخرى تبعًا للتكييف القانوني الذي يُسند إلى الفعل، ولذلك لا يمكن حصر الجريمة المعلوماتية في وصف قانوني واحد، فقد تتخذ الواقعة المرتكبة، والتي تُصنف كجريمة معلوماتية، شكل قذف أو تهديد أو تحريض، وبما يتطابق مع ما

---

[1] حمزة خضري، عشاش حمزة، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، العدد 02، المجلد 06، 2020، ص 173.

[2] المرجع نفسه، ص 173.

[3] حسين نوارة، **آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا**، الملتقى الوطني، آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص ص 121 122.

هو مقرر في قانون العقوبات من خلال القواعد العامة التي قد تمتد لتشمل الجرائم المرتكبة عبر الحاسوب.[1]

ويتكون 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، **مثلا:** إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل ويتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب **مثلا:** جريمة الغش المعلوماتي الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية. [2]

الفرع الثالث: الركن المعنوي

تُعدّ الجرائم المعلوماتية، شأنها شأن سائر الجرائم، قائمة في أساسها على توافر القصد الجنائي العام المتمثل في **العلم والإرادة،** والذي يُعد شرطًا لتحديد المسؤولية الجزائية، ولا يمكن تصور قيام قصد خاص مستقل في الجريمة دون أن يسبقه هذا القصد العام، أمّا بخصوص القصد الخاص في الجرائم المعلوماتية، فإنه يرتبط بطبيعة الفعل الإجرامي المرتكب وبالغاية أو النية الخاصة التي يتجه إليها الجاني من خلال إقدامه على السلوك غير المشروع أو ارتكاب الجريمة.[3]

---

[1] بن غدفة شريفة والقص صليحة، **الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها،** أعمال الملتقى الوطني، آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 2017، ص 48.

[2] فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري،** المؤتمر الدولي الرابع عشر، الجرائم الإلكترونية، طرابلس، بتاريخ 24-25-03-2017، ص 118.

[3] لورنس سعيد الحوامدة، **الجرائم المعلوماتية أركانها وآلية مكافحتها،** دراسة تحليلية مقارنة، مجلة ميزان، للدراسات القانونية والشرعية، الأردن، 2016، ص 24.

يتشكل الركن المعنوي في الجريمة السيبرانية من عنصرين أساسيين هما **العلم والإرادة،** حيث يُقصد **بالعلم** إدراك الجاني للوقائع والظروف المحيطة بالفعل، في حين تتمثل **الإرادة** في توجيه سلوكه الإجرامي نحو تحقيق النتيجة غير المشروعة.[1]

وفقًا للمبادئ العامة المستقرة في قانون العقوبات، قد ينقسم القصد الجنائي إلى قصد عام وقصد خاص، ويتمثل **القصد الجنائي** العام في الغاية المباشرة من السلوك الإجرامي، حيث يقتصر على مجرد اتجاه إرادة الجاني إلى ارتكاب الفعل المجرّم، أما **القصد الجنائي** الخاص فهو الذي يُشترط توافره في بعض الجرائم دون غيرها، إذ لا يقتصر الأمر على مجرد ارتكاب الفعل المجرّم، بل يتجاوز ذلك إلى اتجاه نية الجاني نحو تحقيق نتيجة معينة.[2]

إذن فالقصد الجنائي العام متوافر في جميع الجرائم السيبرانية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص **مثلا:** جرائم تشويه السمعة عبر الأنترانت، وجرائم نشر الفيروسات عبر الشبكة. وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.[3]

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 بإعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها.[4]

---

[1] طلال أبو عفيفة، **جرائم الابتزاز الإلكتروني (جرائم الحاسوب)**، دار وائل للنشر والتوزيع، عمان، 2026، ص 45.

[2] شمسان ناجي صالح، **الجرائم المستخدمة بطريقة غير مشروعة لشبكة الأنترنت**، دار النهضة العربية، القاهرة، مصر، 2009، ص 44.

[3] فضيلة عاقلي، المرجع السابق، ص 120.

[4] لورنس سعيد الحوامدة، المرجع السابق، ص ص 25 26.

المطلب الثاني: المجرم السيبراني

المجرم السيبراني يمتاز بمهارات ومعرفة تقنية تمكنه من استغلال الوسائل الرقمية لارتكاب الجرائم، يشمل هذا المطلب دراسة تعريف المجرم، سماته، الفئات المختلفة، ودوافعه، بما يوضح طبيعة المسؤولية الجنائية في الجرائم الرقمية.

الفرع الأول: تعريف المجرم السيبراني

يُقصد بالمجرم السيبراني ذلك الشخص الذي يستخدم التقنيات المعلوماتية وشبكات الاتصال، وخاصة شبكة الإنترنت، لارتكاب أفعال غير مشروعة تمس بالأنظمة المعلوماتية أو البيانات أو الأفراد أو المؤسسات، وذلك بهدف تحقيق منفعة مادية أو معنوية أو لإلحاق الضرر بالغير.[1]

كما عرف من خلال **التقرير الأممي:** " هو الفرد الذي يستخدم الأنظمة الرقمية وشبكات الاتصال الإلكترونية لارتكاب أفعال غير قانونية، سواء كانت استهداف بيانات شخصية، أنظمة حكومية، أو مؤسسات مالية، بهدف تحقيق منفعة شخصية أو مادية أو للتسبب في ضرر للآخرين. " .[2]

الفرع الثاني: سمات المجرم السيبراني

يتميز بعدة سمات نذكر منها:

1. يمتاز بمهارات فنية متخصصة في الإجرام المعلوماتي، كالاختراق وتغيير المعلومات، وتقليد البرامج أو تحويل الأموال، ومحترف في استخدام الوسائل التقنية والأنترنت، والقدرة على التكيف الاجتماعي.[3]
2. يمتاز بالذكاء في استخدام التكنولوجيا الحديثة، معتمدا على القوة الذهنية لا العضلية.

---

[1] عبد الفتاح بيومي حجازي، **الدليل الجنائي في الجرائم المعلوماتية**، دار الكتب القانونية، مصر، 2008، ص 45.

[2] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations, New York, 2013, p. 23.

[3] فهد عبد الله العبيد العازمي، **الإجراءات الجنائية المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2016، ص 40.

3. الدراية والعلم بالظروف المحاطة بالجريمة المراد تنفيذها، وإمكانية نجاحها أو فشلها.[1]
4. يمتلك السلطة المباشرة او غير المباشرة على المعلومات المستهدفة، سواءً عبر الشفرات الخاصة بالدخول الى النظام، او باستخدام الأنظمة المعلوماتية وإجراء بعض التعاملات، وقد تكون هذه السلطة مزيفة، كاستخدام شفرات دخول شخص آخر.[2]

الفرع الثالث: فئات المجرم السيبراني

استنادًا إلى ما انتهت إليه الدراسات المتخصصة في مجال الجريمة السيبرانية، يمكن تصنيف مرتكبي هذه الجرائم إلى سبع فئات رئيسية، مع التنويه إلى أن الفرد الواحد قد يجمع بين خصائص أكثر من فئة في الوقت ذاته. وتتمثل هذه الأنماط الإجرامية فيما يلي:

1. **الفاعلون بدافع التسلية والمزاح:** هم أشخاص يقومون بأفعال سيبرانية بدافع الترفيه أو المزاح أو التحدي، دون وجود نية مسبقة لإحداث أضرار مباشرة، وغالبًا ما تنتمي هذه الفئة إلى فئة المراهقين أو صغار السن.
2. **المتسللون بدافع الفضول:** يسعى أفراد هذه الفئة إلى الدخول غير المشروع إلى أنظمة الحواسيب المحمية بهدف استكشافها أو اختبار مهاراتهم أو بدافع الفضول، دون وجود قصد إجرامي واضح أو نية لتحقيق منفعة مادية أو إلحاق ضرر.
3. **المخترقون الحاقدون:** وهم الذين يتعمدون إلحاق الضرر بالآخرين عبر تدمير البيانات أو نشر البرمجيات الخبيثة، دون أن يكون هدفهم تحقيق مكاسب مالية، وإنما بدافع الانتقام أو الإيذاء.
4. **المستخدمون للحلول الفردية غير المشروعة:** وتشمل هذه الفئة الأشخاص الذين يلجؤون إلى ارتكاب أفعال سيبرانية للحصول على نتائج لا يستطيعون بلوغها بالوسائل القانونية أو التقليدية، مثل اختراق قواعد بيانات لحل مشكلاتهم الشخصية.

---

[1] نائلة عادل محمد قورة، **جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية**، منشورات الحلبي الحقوقية، بيروت، 2005، ص 52.

[2] المرجع نفسه، ص 58.

5. **المجرمون المحترفون:** يسعى هؤلاء إلى تحقيق أرباح غير مشروعة من خلال استخدام وسائل تقنية، ويقومون بتنظيم نشاطهم بشكل منظم ودقيق، وغالبًا ما يكونون جزءًا من شبكات إجرامية منظمة، مما يجعلهم أقرب إلى نمط الجريمة المنظمة التقليدية.
6. **المتشددون ذوو الدوافع الإيديولوجية:** تضم هذه الفئة جماعات تستعمل الفضاء السيبراني كوسيلة للتعبير عن معتقدات سياسية أو دينية أو اجتماعية متطرفة، وقد تستهدف تعطيل الأنظمة أو تخريب الممتلكات العامة لفرض الانتباه إلى قضاياها، **مثل** ما قامت به جماعة "**الألوية الحمراء**" في أوروبا خلال ثمانينيات القرن الماضي عندما دمرت أكثر من 60 مركزًا معلوماتيًا.
7. **المهملون جنائيًا:** وهم أفراد يتسببون في أضرار خطيرة نتيجة إهمالهم في التعامل مع الأنظمة الرقمية، وقد تصل هذه الأضرار إلى فقدان أرواح، **مثل** ما حدث في إحدى الحوادث بنيوزيلندا عندما أدى تعديل غير مصرح به على برنامج تحديد مسار طائرة إلى تحطمها ووفاة عدد من الركاب، ما ترتب عليه متابعة المتسببين بتهمة القتل غير العمد.

الفرع الرابع: دوافع ارتكاب الجريمة السيبرانية

تشير مفاهيم "**الدافع**" و"**الباعث**" و"**الغاية**" إلى مصطلحات قانونية دقيقة ضمن نطاق القانون الجنائي، وهي ترتبط بما يُعرف بالقصد الخاص في الجريمة، أي تلك النية المحددة التي تدفع الجاني إلى الإقدام على سلوكه الإجرامي، وتتميّز الجريمة السيبرانية بتنوع الدوافع التي تقف خلف ارتكابها، إذ قد تكون ذات طابع شخصي أو ناتجة عن عوامل خارجية، أو مرتبطة ببيئة العمل والظروف المهنية، كما تكشف هذه الدوافع عن تداخل واضح بين الرغبة الداخلية في إلحاق الضرر بالغير، والسعي نحو تحقيق مكاسب مادية أو معنوية، أو حتى محاولة إثبات الذات وإبراز القدرات.[1]

[1] بوديسة بجاد عبد الرؤوف، **آليات التحري عن الجريمة الإلكترونية في القانون الجزائري**، مذكرة ماستر في الحقوق تخصص قانون الإعلام الآلي والأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2021-2022، ص 22.

أولا: الدوافع الشخصية

تنقسم الدوافع ذات الطابع الشخصي إلى فئتين أساسيتين: دوافع مالية من جهة، ودوافع فكرية أو سلوكية نمطية من جهة أخرى.

1. **الدوافع المالية:** يُعتبر الدافع نحو تحقيق الربح المادي من أبرز العوامل التي تحفّز الأفراد على ارتكاب الجرائم السيبرانية. وتتميز هذه الجرائم بإمكانية تحقيق عائدات مالية كبيرة بطرق غير تقليدية، **مثل** عمليات الاحتيال أو التلاعب بأنظمة المعالجة الآلية للبيانات. ومن **الأمثلة** على ذلك ما وقع في فرنسا سنة 1986، حيث تجاوزت أرباح إحدى جرائم الغش الإلكتروني 670,000 فرنك فرنسي، في حين لم تتعدَّ عائدات جريمة سرقة تقليدية 70,000 فرنك فقط. كما تُبرز تقارير المركز الوطني للاحتيال المعلوماتي بالولايات المتحدة (N.F.I.C) أن الدافع المالي يظل الأكثر انتشارا في هذا النوع من الجرائم.[1]
2. **الدوافع الذهنية أو النمطية:** توجد فئة من مرتكبي الجرائم يكون دافعهم الأساسي هو إثبات قدرتهم على تجاوز الأنظمة المعلوماتية، دون أن تكون لديهم نية مباشرة للإضرار بالغير أو تحقيق مكاسب مادية. إذ يقوم هؤلاء بمحاولات اختراق النظم بدافع التحدي وإبراز المهارة الشخصية، وهو ما يظهر غالبًا في سلوك قراصنة الأنظمة (Hackers)، ولا سيما ما يُعرف بالمتطفلين الداخليين، ومع ذلك، فإن المعطيات الإحصائية تشير إلى أن الدافع المالي يظل الأكثر شيوعًا وانتشارًا مقارنة ببقية الدوافع.[2]

ثانيا: الدوافع الخارجية

تلعب العوامل البيئية والاجتماعية والمهنية دورًا مباشرًا في دفع السلوك الإجرامي السيبراني، ولا سيما عندما تتداخل مع طبيعة بيئة العمل الرقمي.

1. دافع الانتقام: يتجلى هذا الدافع عندما يلجأ الموظف الحالي أو السابق إلى إلحاق الأذى بصاحب العمل، كما في إحدى الحالات التي عمد فيها محاسب إلى التلاعب بالبرمجيات

[1] داودي خالد، **الجريمة الإلكترونية**، دار الأعصر للنشر والتوزيع، عمان، 2011، ص ص 37-38.

[2] أحمد خليفة ملط، **الجرائم المعلوماتية**، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص ص 89 90 .

بهدف تخريب بيانات مؤسسة بعد مغادرته العمل. وتُعدّ أعمال إدخال الفيروسات أو حذف قواعد البيانات من أبرز الأشكال التي تتخذها هذه الجرائم.[1]

2. **الرغبة في قهر النظام وإثبات التفوق:** يسعى بعض الأفراد، لا سيما فئة الشباب، إلى إظهار مهاراتهم التقنية من خلال اختراق الأنظمة المعلوماتية.

من المهم الإشارة إلى أن الفعل الإجرامي الواحد قد تتداخل فيه عدة دوافع في آن واحد، **مثل** الجمع بين السعي لتحقيق مكاسب مالية والدوافع الأيديولوجية أو الانتقامية، وهو ما يظهر على سبيل المثال في حالات سرقة الأسرار التجارية أو في الهجمات السيبرانية ذات الطابع السياسي.[2]

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

[2] داودي خالد، المرجع السابق، ص 39.

خلاصة الفصل الأول

يتناول هذا الفصل الجريمة السيبرانية من حيث الإطار العام الذي يحدد مفهومها وخصائصها وبنيتها القانونية، إضافة إلى دراسة الفاعل الإجرامي والدوافع المؤثرة في سلوكه. وقد تبيّن من خلال مختلف المقاربات اللغوية والفقهية والقانونية أن هذا النوع من الجرائم يتميز بتعدد زوايا تعريفه، نتيجة ارتباطه الوثيق بالتطور التكنولوجي وبيئة المعلومات الرقمية.

وتتسم الجريمة السيبرانية بجملة من الخصائص التي تميزها عن الجرائم التقليدية، من أهمها صعوبة كشفها وإثباتها، وحداثة ظهورها، وطابعها العابر للحدود الوطنية، فضلاً عن سهولة ارتكابها مقارنة بغيرها من الجرائم. كما أنها ترتبط بدرجة عالية بالمهارات التقنية للجناة، مع ملاحظة انخفاض نسب التبليغ عنها في كثير من الحالات. وتظهر أيضًا في صور تقليدية مثل التزوير المعلوماتي والتجسس السيبراني وسرقة البيانات، إلى جانب أنماط مستحدثة تشمل الجرائم المرتبطة بالذكاء الاصطناعي والعملات المشفرة وأسواق الشبكة الخفية.

ومن الناحية القانونية، تقوم الجريمة السيبرانية على الأركان المعروفة في التجريم، حيث يجتمع الركن الشرعي الذي يستند إلى النصوص القانونية، مع الركن المادي المتمثل في السلوك الإجرامي في البيئة الرقمية، والركن المعنوي الذي يعكس القصد الجنائي لدى الفاعل. كما يبرز في هذا السياق مفهوم المجرم السيبراني الذي يتميز بسمات خاصة، ويأخذ أشكالاً متعددة وفق اختلاف مستواه التقني وطبيعة نشاطه الإجرامي.

وتتعدد الدوافع التي تقف وراء ارتكاب هذا النوع من الجرائم، إذ قد تكون شخصية مرتبطة بالرغبة في الربح أو التحدي أو إثبات الذات، أو خارجية ناتجة عن ظروف اجتماعية أو مهنية أو بيئية. ويؤدي هذا التداخل في الدوافع إلى تفسير تنوع السلوك الإجرامي داخل الفضاء السيبراني وتعقيده.

الفصل الثاني: آليات مكافحة الجريمة السيبرانية في التشريع الجزائري

الفصل الثاني: آليات مكافحة الجريمة السيبرانية في التشريع الجزائري

يُعدّ التصدي للجريمة السيبرانية من أكثر التحديات القانونية تعقيداً في العصر الرقمي، إذ لم يعد يكفي صياغة النصوص التجريمية وحدها لردع هذا النوع من الإجرام، بل باتت الحاجة ملحّة إلى منظومة متكاملة من الآليات الإجرائية والمؤسساتية القادرة على ملاحقة الجاني ووقف نشاطه الإجرامي في فضاء متسارع التحولات، لا تعرف حدوده حدوداً جغرافية ولا تخضع حركته لمبدأ التزامن الزمني.

انطلاقاً من هذا الإدراك، أفرز المشرّع الجزائري جملةً من الآليات التي تنتظم في مستويين متكاملين لا يغني أحدهما عن الآخر: مستوى الآليات الإجرائية والوقائية التي تُجسّد الإطار القانوني التشريعي لمكافحة الجريمة السيبرانية، ومستوى الآليات المؤسساتية التي تُجسّد الذراع التنفيذية لهذا الإطار على الصعيدين الوطني والدولي.

فعلى صعيد الآليات الإجرائية، شكّل القانون رقم 09-04 أساس التنظيم التشريعي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مدعوماً بالقوانين اللاحقة، من خلال إقرار قواعد خاصة وأساليب تحقيق حديثة تتلاءم مع خصوصية البيئة الرقمية، مع إخضاعها لرقابة قضائية ضماناً للحقوق والحريات.

أما على الصعيد المؤسساتي، فقد أنشأت الدولة هياكل متخصصة في التحقيق والملاحقة، مع تعزيز التعاون الدولي لمواجهة الطابع العابر للحدود للجريمة السيبرانية.

وعليه، سيتم تناول هذه الآليات من خلال مبحثين.

المبحث الأول: الآليات الإجرائية والوقائية المستحدثة لمكافحة الجريمة السيبرانية.

المبحث الثاني: الآليات المؤسساتية على المستويين الوطني والدولي.

المبحث الأول: آليات إجرائية وقائية المستحدثة لمكافحة الجريمة السيبرانية

لا تقتصر مكافحة الجريمة السيبرانية على التجريم والعقاب، بل تقتضي منظومة إجرائية وقائية متكاملة تواكب الكشف والملاحقة، ونظراً لخصوصيتها التقنية، أصبحت القواعد التقليدية غير كافية، مما استدعى إقرار إجراءات استثنائية ملائمة لطبيعة البيئة الرقمية.

وقد أدرك المشرّع الجزائري خصوصية الجريمة السيبرانية، فأقام منظومة إجرائية على مستويين متكاملين، يتمثل الأول في الإطار التشريعي الذي يرتكز على القانون 09-04 مدعوماً بالقوانين اللاحقة، بينما يتمثل الثاني في اعتماد أساليب إجرائية حديثة كالتسرّب الإلكتروني واعتراض المراسلات وجمع المعطيات، ويقتضي البحث دراسة هذين المستويين من خلال مطلبين، يُخصّص الأول للآليات التشريعية، والثاني للآليات الإجرائية المستحدثة لمكافحة الجريمة السيبرانية.

المطلب الأول: آليات التشريعية إجرائية لمكافحة الجريمة السيبرانية

أمام خصوصية الجريمة السيبرانية، أقرّ المشرّع الجزائري إطاراً إجرائياً خاصاً يتجاوز القواعد العامة، نظراً لقصورها عن مواكبة طبيعة الأدلة الرقمية ومجالها المفتوح، وقد تجلّى ذلك في القانون 09-04 بما تضمّنه من تدابير وقائية وإجرائية، مدعوماً بالقوانين اللاحقة كالقانون 18-04 و18-07 لتعزيز الحماية وتُعرض هذه الآليات في فرعين، الأول في إطار القانون 09-04، والثاني في القوانين المكمّلة له.

الفرع الأول: مكافحة الجريمة السيبرانية بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 09-04.

يُعدّ القانون رقم 09-04 المؤرخ في 05 أوت 2009 إطاراً قانونياً شاملاً لتنظيم الجوانب المرتبطة بالمنظومة المعلوماتية، بما يشمل المعطيات ومقدّمي الخدمات والبيانات المتصلة بالاتصالات الإلكترونية، وقد أقرّ مجموعة من الآليات للوقاية من الجرائم المعلوماتية ومكافحتها، من خلال تنظيم إجراءات مراقبة وتفتيش الأنظمة المعلوماتية وحجز المعطيات وحفظ بيانات

الحركة، إلى جانب تحديد التزامات مقدّمي خدمات الإنترنت، كما نصّ على إنشاء هيئة وطنية مختصة، مع التأكيد على تعزيز التعاون الدولي لمواجهة هذا النوع من الجرائم.[1]

أولا: التدابير الوقائية

فتتمثل فيما يلي:

1-المراقبة الإلكترونية

تعرف الرقابة الإلكترونية على أنها " استخدام الحاسوب الآلي في العملية الرقابية وفق برامج حاسوبية تعد خصيصا لهذا الغرض بما يحقق الاقتصاد في الجهد والوقت والتكلفة في الوصول إلى النتائج المطلوبة بأقل خسائر ممكنة ". [2]

وبالرجوع إلى القانون رقم 09-04 السابق ذكره **نلاحظ** أن المشرع الجزائري لم يعرف المراقبة الإلكترونية أو مراقبة الاتصالات الإلكترونية [3] وإنما اكتفى فقط بتحديد مفهوم الاتصالات الإلكترونية.

2-الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية

وتم تعريفها من قبل المشرع الجزائري على أنها " أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية، أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها. [4]

---

[1] قارة أمال، **الإطار القانوني للجريمة السيبرانية The legalframework for cybercrime**، محاضرة المدرسة العليا للقضاء دفعة 2023-2024، ص 16.

[2] عدنان مصطفى البار، **الخصوصية وسعي الدولة للرقابة الإلكترونية الشاملة**، مركز هردو لدعم التعبير الرقمي القاهر، 2018، ص 25.

[3] مصطفى محمد موسى، **المراقبة الإلكترونية عبر شبكة الأنترنت**، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، 2003، ص 192.

[4] المادة 02 و 04 من القانون رقم 09-04 .

يتولى مزودي خدمات في إطار مكافحة الجرائم المعلوماتية بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية بهدف جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها توضع المعطيات تحت تصرف السلطات [1] .

ثانيا: التدابير الإجرائية

حيث تمثلت هذه التدابير الإجرائية في:

1-تفتيش وحجز المنظومة المعلوماتية

عرف المشرع الجزائري المنظومة المعلوماتية ضمن نص المادة الثانية الفقرة الثانية من القانون رقم 09-04 السابق ذكره على أنها نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض، يقوم واحد منها أو أكثر بمعالجة الآلية للمعطيات تنفيذا لبرنامج معين. [2] والمقتضيات الحفاظ على النظام العام ومستلزمات التحريات وكذا التحقيقات الجارية في إطار مكافحة الجريمة السيبرانية، تم اتخاذ مجموعة من التدابير الإجرائية والترتيبات التقنية لمراقبة الاتصالات الإلكترونية. [3]

2-تمديد الاختصاص بنظر هذه الجرائم

تمديد الاختصاص المحلي لكل من ضباط الشرطة القضائية وقاضي التحقيق ووكيل الجمهورية المادة 37 من ق إ ج إذا تعلق الأمر بالجريمة المنظمة وجرائم المعالجة الآلية للمعطيات الإرهاب، تبييض الأموال وجرائم الصرف، ولعل اعتماد الاختصاص الإقليمي الموسع هو المواجهة الفعالة لطائفة من الجرائم المنظمة الخطيرة التي تتسم بالتعقيد حتى ولو كان في ذلك خروج عن معايير الاختصاص الأصلية المتمثلة في مكان وقوع الجريمة أو مكان القبض

[1] المادة 10 من القانون رقم 09-04 .

[2] المادة 02/02 من القانون رقم 09-04.

[3] مهدي رضا، المرجع السابق، ص 120.

على المتهم أو مكان إقامته، فهي في الأصل معايير موضوعية تبرر ردة فعل المجتمع اتجاه المجرم الذي اخل بالنظام العام .[1]

3-تبادل المساعدة القضائية الدولية

لقد أقر المشرع الجزائري بموجب القانون رقم 09-04 اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام الاتصال المرتكبة خارج إقليم التراب الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني. [2]

غير انه في إطار التحقيقات القضائية والمعاينات للجرائم السيبرانية وكشف عن مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في شكلها الإلكتروني [3]، ومن الممكن الاستجابة لطلبات المساعدة الرامية إلى تبادل المعلومات أو اتخاذ أي إجراء تحفظي وفقا للاتفاقيات دولية تطبيقا لمبدأ المعاملة بالمثل. [4]

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

نظرا لخطورة الجرائم السيبرانية استحدث المشرع الجزائري بموجب القانون رقم09-04 السابق ذكره الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ليحدد تنظيمها وتشكيلتها عن طريق التنظيم.[5]

فمن شأنها مكافحة الجرائم ومصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، كما يخول القانون لهذه الهيئة تولي جانب تجميع

---

[1] سعيدة بوزون، **مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، كلية الحقوق، جامعة الاخوة منتوري قسنطينة، عدد 52، المجلد ب، ص ص47-57، الجزائر، ص 50.

[2] المادة 15 من القانون رقم 09-04.

[3] المادة 16 من القانون رقم 09-04.

[4] مهدي رضا، المرجع السابق، ص 120.

[5] المادة 13 من القانون رقم 09-04.

المعلومات وإنجاز الخبرات القضائية وتبادل المعلومات مع نظيراتها في الخارج قصد محاربة هذا النوع من الجرائم. [1]

حيث تعرف أنها " سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع تحت تصرف رئيس الجمهورية "، يحدد مقرها بالجزائر العاصمة ويمكن نقله إلى أي مكان من التراب الوطني بموجب مرسوم رئاسي، [2] وتتكون من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية ويقدمان له عرضا لنشاطاتهما.[3]

تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في إطار مكافحتها للجرائم السيبرانية بمجموعة من الصلاحيات التي **تتمثل فيا يلي:**

1-اقتراح عناصر استراتيجية للوقاية من جرائم تكنولوجيا الإعلام والاتصال.

2-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام الاتصال.

3-مساعدة السلطة القضائية وضباط الشرطة القضائية في مكافحة الجرائم السيبرانية لاسيما ما يتعلق بجمع المعلومات والتزويد بها. [4]

4-ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم التي تتصف بالأفعال الإرهابية والمساس بأمن الدولة.

5-إضافة إلى ذلك تكلف الهيئة بتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.[5]

---

[1] نورة العقون، **واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر**، مذكرة التخرج لنيل شهادة الماستر في العلوم السياسية تخصص دراسات أمنية واستراتيجية، جامعة قصدي مرباح ورقلة، كلية الحقوق، 2019، ص 51.

[2] المادة 02، من المرسوم الرئاسي رقم 20-183، المؤرخ في 13 يوليو 2020، المتضمن **إعادة تنظيم الهيئة الوطنية للوقاية من المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها**، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، العدد 40، الصادرة بتاريخ 18 يوليو 2020.

[3] المادة 02 من المرسوم الرئاسي رقم 20-183.

[4] المادة 14 من القانون رقم 09-04.

[5] المادة 04 من المرسوم الرئاسي رقم 20-183.

الفرع الثاني: القوانين اللاحقة المدعمة للقانون 09-04 في مجال الحد من الإجرام السيبراني

أولا: القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية

حيث استحدث هذا القانون مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الافتراضي منها استحداث سلطة ضبط من بين مهامها السهر على احترام متعاملي البريد والاتصالات الإلكترونية من خلال أحكام قانونية وتنظيمية تتعلق بالأمن السيبراني.[1]

وعليه حرمت انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها، وتحريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة، وسنت مجموعة من العقوبات.[2]

ثانيا: القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

تعرف المعطيات ذات الطابع الشخصي في المادة الثالثة من القانون رقم 18-07 المتعلق بحماية المعطيات الشخصية بأنها "**كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه الشخص المعني** " بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيو مترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

وأقر هذا القانون المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي فنجد المادة 7 من القانون 18-07 تنص على ضرورة إبداء الموافقة الصريحة للشخص المعني من أجل السماح

---

[1] المادة 13 من القانون 18-04 المؤرخ في 10 مايو 2018، الذي يحدد **القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية**، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، عدد 27، الصادرة بتاريخ 13 متايو 2018.

[2] المادة 164 و 188 من القانون رقم 18-04 .

بمعالجة معطياته الشخصية، وله التراجع عن موافقته في أي وقت، غير أن موافقته لا تكون ضرورية متى تعلق الأمر باحترام التزام قانوني يخضع له المعني.[1]

كما انه كانت جزاءات الإخلال بالقانون 18-07، بحيث نجد جزاءات إدارية فجعل المشرع كل من الإنذار، الإعذار، السحب المؤقت للرخصة أو السحب النهائي والغرامة جزاءات الإخلال بأحكام هذا القانون تصدر هذه العقوبات السلطة الوطنية وتكون قراراتها قابلة للطعن أمام مجلس الدولة، كما تستطيع السلطة فرض غرامة مالية قدرها 500 ألف دينار جزائري. [2]

إجمالاً يتضح أن المشرع الجزائري عمل على تعزيز منظومته التشريعية بحزمة من النصوص القانونية التي سبق التطرق إليها بالتفصيل، وذلك في سياق توجه الدولة نحو تبني استراتيجية الرقمة الشاملة في مختلف القطاعات، ولعل من أبرز هذه النصوص ما يمكن الإشارة إليه على سبيل المثال لا الحصر:[3]

1-قانون الإعلام – القانون العضوي- رقم 12- 05 المؤرخ في 12-01-2012.

2-قانون حماية حقوق المؤلف والحقوق المجاورة قانون رقم 03-05 المؤرخ في 19-07-2003.

3-قانون التوقيع الإلكتروني رقم 15- 03 المؤرخ في 01-02-2015 المتعلق بعصرنة العدالة.

4-قانون المتعلق بحماية المعلومات والوثائق الإدارية الأمر رقم21-09 المؤرخ في 08-06-2021.

---

[1] تومي يحي، **الحماية القانونية للمعطيات ذات الطابع الشخصي**، على ضوء القانون ر قم 18-07، دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، جامعة المسيلة، الجزائر، 2018، ص 1528.

[2] يوسف رزوق، **حماية المعطيات الشخصية في الجزائر على ضوء قانون رقم 18-07**، مجلة معالم الدراسات القانونية والسياسية، العدد 05 ديسمبر 2018، ص127.

[3] حايط فاطمة، **إجراءات التحقيق في الجرائم الإلكترونية، دراسة مقارنة**، أطروحة لنيل شهادة دكتوراه، تخصص قانون جنائي والعلوم الجنائية، جامعة ابن خلدون، كلية الحقوق والعلوم السياسية، تيارت، الجزائر، 2022 -2023، ص 156.

5-قانون يحدد القواعد المتعلقة بالتوقيع والتصديق الإلكترونيين رقم 15-04 المؤرخ في 01-02-2015.

المطلب الثاني: الآليات الإجرائية المستحدثة لملاحقة الجريمة السيبرانية

نظراً لخصوصية الجريمة السيبرانية وتعقيدها، استلزم الأمر استحداث آليات إجرائية حديثة تتماشى مع طبيعتها الرقمية وتمكّن من تتبع مرتكبيها بفعالية، مع مراعاة الضوابط القانونية وحماية الحقوق والحريات. وعليه، سيتم عرض أهم هذه الآليات، والمتمثلة في التسرب الإلكتروني، واعتراض المراسلات والمراقبة الإلكترونية، إضافة إلى جمع وتسجيل المعطيات التقنية.

الفرع الأول: التسرب الإلكتروني

سيتم الإحاطة بتعريفه، والجهات المخوّلة قانوناً بمباشرته، وصور المتسرب الإلكتروني، والشروط المطلوبة لمشروعيته، وانتهاءً بالقيود التي أحاط بها المشرع هذه العملية.

أولا: تعريف التسرب الإلكتروني

عرف المشرع الجزائري التسرب بموجب المادة 121 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية، بأنه " إجراء مستحدث يقوم به ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، والتي يتم بمقتضاها مراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة وإيهامهم بأنه فاعل معهم أو شريك لهم أو خاف " .[1]

أما التسرب الإلكتروني فقد أشار إليه المشرع الجزائري في نص المادة 26 من القانون رقم 20-05 ، أنه يمكن لوكيل الجمهورية بعد إخطاره لقاضي التحقيق، أن يأذن وتحت رقابته، لضابط الشرطة القضائية بالتسرب الإلكتروني إلى منظومة معلوماتية أو أنظمة اتصالات

[1] المادة 120 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية.

الكترونية، بُغية مراقبة الأشخاص المشتبه في ارتكابهم لأي جريمة من الجرائم الوارد ذكرها في القانون السالف ذكره، بصفتهم فاعلين أصليين أو شركاء لهم في الجريمة.[1]

ثانيا: الجهات المخول لها قانونا مراقبة عملية التسرب الإلكتروني

أسند المشرع الجزائري مهمة الإشراف والرقابة على إجراءات التسرب الإلكتروني المنجزة من قبل ضباط وأعوان الشرطة القضائية إلى كل من وكيل الجمهورية وقاضي التحقيقي فيعد **وكيل الجمهورية** ممثلًا للنيابة العامة على مستوى المحكمة، ويعد المسؤول الأول عن رقابة عملية التسرب الإلكتروني وقد خُوِّل بموجب القانون جملة من الصلاحيات، من بينها اتخاذ الإجراءات الضرورية للبحث والتحري عن الجرائم. وتبعًا لهذه الصفة، مُنح سلطة الترخيص لضابط الشرطة القضائية المكلف بتنسيق عملية التسرب، لمباشرة هذا الإجراء متى اقتضت ضرورات التحقيق والتحري في الجرائم المحددة على سبيل الحصر ضمن أحكام المادة 114. [2]

خوّل المشرع الجزائري أيضا **لقاضي التحقيق** سلطة الرقابة على إجراءات التسرب الإلكتروني، حيث منحه صلاحية الترخيص لضابط الشرطة القضائية المكلف بتنسيق هذه العملية للشروع في تنفيذها، وذلك بعد إخطار مسبق لوكيل الجمهورية، متى استدعت ضرورات التحري والتحقيق في الجرائم المحددة على سبيل الحصر في أحكام المادة 114 ق إ ج اتخاذ هذا الإجراء.[3]

ثالثا: صور المتسرب الإلكتروني

اقتصر المشرع على بيان صورتين فقط للمتسرب الإلكتروني، إذ قد يظهر إما بوصفه فاعلًا أصليًا أو شريكًا في الجريمة، دون أن يتطرق إلى الصورة الثالثة المتمثلة في المتسرب

---

[1] المادة 26 من القانون رقم 20-05 المؤرخ في 28 أفريل 2020، يتعلق **بالوقاية من التمييز وخطاب الكراهية ومكافحتهما**، جريدة رسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 25، الصادرة بتاريخ 29 أفريل 2020.

[2] وداعي عز الدين، **التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن**، المجلة الأكاديمية للبحث القانوني، المجلد 16، عدد 02، 2017، ص 208.

[3] المادة 114 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية .

بوصفه خافيًا، **فالمتسرب كفاعل** في الجريمة، وذلك من خلال التسلل إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية يضم مجموعة من المجرمين، حيث يتواصل معهم ويوهمهم بأنه شريك في نشاطهم الإجرامي تحت هوية مستعارة، بهدف تمكينه من جمع الأدلة الكافية لإدانتهم[1]، وبصورة أخرى **المتسرب كشريك** في الجريمة، " وهو الشخص الذي يتوغل داخل منظومة معلوماتية من خلال قيامه ببعض الأفعال التي تساهم في تهيئة أو تسهيل أو تنفيذ الجريمة " .[2] و **كمتسرب كخافٍ** هي الصورة الثالثة من صور المتسرب التي نص عليها المشرع في المادة 121 ق إ ج، حيث أجاز بموجبها لضباط الشرطة القضائية أو أعوانهم مراقبة المشتبه في ارتكابهم جناية أو جنحة، وذلك من خلال إيهامهم بأنه يقوم بإخفاء أشياء متحصلة من هذه الجرائم أو تم اختلاسها بواسطتها، مع استعمال هوية مستعارة، بهدف التمكن من جمع الأدلة التي تثبت إدانتهم.[3]

رابعا: شروط التسرب الإلكتروني

أخضع المشرع الجزائري إجراء عملية التسرب الإلكتروني لمجموعة من الشروط، وهي:

1. الشروط الشكلية للتسرب الإلكتروني

لضمان صحة إجراء التسرب الإلكتروني الذي يقوم به ضابط أو عون الشرطة القضائية، اشترط المشرع ضرورة تحقق جملة من الشروط الشكلية هي كالتالي:

1-الحصول على الإذن بالتسرب.

2-تحرير ضابط الشرطة القضائية لمحضر حول عملية التسرب.

3-إيداع الرخصة في ملف الإجراءات.

---

[1] العرفي فاطمة، **تطبيق إجراء التسرب في القانون الجزائري، إشكالية الموازنة بين حماية حق الخصوصية الرقمية ومكافحة جريمة اختطاف الأشخاص**، مجلة دراسات وأبحاث، المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، مجلد 13، عدد 4 جويلية 2021، ص 216.

[2] المادة 42 من الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، **المتضمن قانون العقوبات** المعدل والمتمم، جريدة رسمية للجمهورية الجزائرية، العدد 49، الصادرة بتاريخ 11 يونيو 1966.

[3] العرفي فاطمة، المرجع السابق، ص 217.

2. الشروط الموضوعية للتسرب الإلكتروني

وتتمثل هذه الشروط في:

1- اقتضاء ضرورة التحري والتحقيق اللجوء إلى عملية التسرب: فالمشرع الجزائري قد علق اللجوء إلى هذا الإجراء على شرط توفر حالة الضرورة، هذه الأخير يمكن لوكيل الجمهورية أو قاضي التحقيق تقدير مدى توافره من عدمه.[1] وإن تحقق حالة الضرورة في التحري والتحقيق، يعد من الشروط الجوهرية التي يلتزم بها وكيل الجمهورية أو قاضي التحقيق لمنح الإذن لعملية التسرب الإلكتروني.[2]

2- مجال تطبيق التسرب الإلكتروني: نص المشرع الجزائري صراحة على نطاق تطبيق التسرب الإلكتروني والولوج إلى منظومة معلوماتية أو نظام الاتصالات الإلكترونية.[3]

3- إجراء التسرب الإلكتروني تحت مسؤولية الضابط المنسق للعملية.

4- أن تكون عملية التسرب الإلكتروني تحت رقابة وكيل الجمهورية أو قاضي التحقيق.

خامسا: القيود الواردة على مباشرة التسرب الإلكتروني

قيد هذه العملية بجملة من الضوابط القانونية التي يتعين احترامها أثناء تنفيذ التسرب الإلكتروني، هذه الضوابط فيما يلي:

1. قيد الالتزام بالأفعال التيُ يأذن فيها للمتسرب الإلكتروني القيام بها

منح المشرع الجزائري لضابط أو عون الشرطة القضائية، أثناء تنفيذ عملية التسرب، ترخيصًا للقيام ببعض الأفعال التي تُعد في الأصل جرائم يعاقب عليها القانون، غير أنه يُسمح له أو

---

[1] درياد مليكة، **نطاق سلطات قاضي التحقيق والرقابة عليها**، ط1، ديوان المطبوعات الجامعية، الجزائر، 2014، ص 154.

[2] عمارة فوزي، **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية**، مجلة العلوم الإنسانية، جامعة منتوري، قسنطينة، عدد 33، 2010، ص 247.

[3] نصت المادة 114 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية الجديد، على مجموعة من الجرائم الخطيرة التي يمكن فيها اللجوء إلى إجراء التسرب المادي وهي: جرائم القتل العمدي، جرائم المخدرات؛ الجريمة المنظمة العابرة للحدود الوطنية؛ الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ؛ جرائم تبييض الأموال؛ جرائم الإرهاب؛ الجرائم المتعلقة بالتشريع الخاص بالصرف؛ جرائم الفساد، جرائم التهريب، جرائم الاتجار بالبشر، جرائم الاتجار بالأعضاء، جرائم تهريب المهاجرين جرائم اختطاف الأشخاص .

للعون المتسرب، وكذا للأشخاص المسخرين لإنجاز هذه العملية، بمباشرتها متى اقتضت الضرورة ذلك، وذلك في إطار ما يُعرف بالأفعال المبررة قانونًا.[1]

2. قيد عدم التحريض على الجريمة

ويقصد بالتحريض، دفع الغير إلى ارتكاب الجريمة سواء عن طريق خلق فكرة الجريمة لديه بعد أن كانت غير موجودة من قبل، أو عن طريق تشجيعه على تحقيق فكرة الجريمة التي كانت موجودة لديه قبل التحريض.[2]

الفرع الثاني: اعتراض المراسلات والمراقبة الإلكترونية في إطار الإجراءات القانونية

يتناول هذا الفرع موضوع اعتراض المراسلات، في حين تم التطرق إلى المراقبة الإلكترونية سابقًا ضمن المطلب الأول.

أولا: تعريف عملية اعتراض المراسلات السلكية واللاسلكية

يناط باعتراض المراسلات تلك العملية التي تسمح بمراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة، وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في إرتكاب الجريمة.[3]

وعرفت المادة 114 من القانون 25-14 ق إ ج عملية مراقبة المراسلات على أنها " **اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية** ".

وعليه، يتضح أن المشرّع الجزائري قد جمع بين تسجيل الأصوات والتقاط الصور واعتراض المراسلات ضمن سياق قانوني واحد، دون أن يقدّم تعريفًا صريحًا لكل منها، مكتفيًا بالإشارة إليها

---

[1] عدو عبد القادر، **مبادئ قانون العقوبات الجزائري**، القسم العام، نظرية الجريمة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2010، ص 151.

[2] سليمان عبد الله، **شرح قانون العقوبات الجزائري**، القسم العام، الجريمة، الجزء الأول، دار المطبوعات الجامعية، الجزائر، 2009، ص 204.

[3] العدواني عبد الحميد، **إدارة التحريات والتحقيقات الأولية في الجرائم التي تدخل في إختصاص القطب القضائي الجزائي**، الملتقى الجهوي حول مكافحة الإجرام الخطير، مجلس قضاء ورقلة، 2009، ص 7.

باعتبارها إجراءات تمسّ بالحياة الخاصة وتخضع لذات الإطار القانوني[1] و**تعرف** على أنها: وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية " [2] .

ويقصد به كذلك " حفظ الحديث على جهاز معد لذلك بهدف الاستماع إليه مرة أخرى ".[3]

ثانيا: الشروط المطلوبة في المراسلات محل الاعتراض

يشترط في المراسلات التي يمكن إخضاعها لإجراء الاعتراض أو المراقبة أن تتصف بطابع السرية والخصوصية، وهو ما لا يتحقق إلا بتوافر عنصرين أساسيين:[4]

1- أن يتضمن محتوى الرسالة معلومات أو أفكار ذات طابع شخصي وسري.

2- أن يكون المرسل قد حدّد جهة الاستلام مع إبداء رغبته في حصر الاطلاع على مضمون المراسلة وعدم تمكين الغير منه.

ثالثا: الشروط القانونية لاعتراض المراسلات

تبقى عملية الاعتراض أو مراقبة المراسلات مرهونة على توافر الشروط التالية:[5]

1-يشترط لاعتراض المراسلات الحصول على إذن مكتوب من الجهة القضائية المختصة، سواء وكيل الجمهورية في مرحلة التحقيق الابتدائي أو قاضي التحقيق في مرحلة التحقيق القضائي، تحت طائلة بطلان الإجراء.[6]

---

[1] عباسي خولة، **الوسائل الحديثة للإثبات في القانون الجنائي**، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2014، ص 42.

[2] أحسن بوسقيعة، ص 113

[3] نقادي عبد الحفيظ، **التسجيل الصوتي**، المجلة للعلوم القانونية والاقتصادية، كلية الحقوق الجزائر، العدد 01، 2009، 312.

[4] براهيمي جمال، **مكافحة الجرائم الالكترونية في التشريع الجزائري**، المجلة النقدية، جامعة مولود معمري، تيزي وزو، العدد 02، 2016، ص 14.

[5] جبار فطيمة، **مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري**، مجلة الدراسات القانونية المقارنة، جامعة مولود معمري بتيزي وزو، العدد 3، ديسمبر 2016، ص 15.

[6] بن كثير بن عيسى، **الإجراءات الخاصة المطبقة على الإجرام الخطير**، نشرة القضاة، مديرية الدراسات القانونية والوثائق، العدد 63، ص89.

2-يُشترط تسبيب الإجراء، أي بيان مبررات اللجوء إلى اعتراض ومراقبة المراسلات، مع إبراز جديتها ودورها في كشف الجريمة وتحديد مرتكبيها.

3-كما يجب تحديد الجرائم محل الاعتراض والمراقبة في حدود ما يجيزه القانون، مع الالتزام بسرية الإجراءات واحترام واجب كتمان السر المهني.

الفرع الثالث: الحفظ وإفشاء العاجلان للمعطيات الإلكترونية

يُعدّ إجراء الحفظ من الآليات المستحدثة ذات الطابع الوقائي، التي أقرّها القانون رقم 04-09 وألزم بموجبها مزوّدي خدمات الإنترنت[1]، وذلك انسجامًا مع ما جاء في قرار الجمعية العامة للأمم المتحدة رقم 55-3 المؤرخ في 22 يناير 2001 المتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، لا سيما في الفقرة (و) من مادته الأولى التي دعت إلى تمكين الدول من حفظ المعطيات الإلكترونية المرتبطة بالتحقيقات الجنائية. ويُنفَّذ هذا الإجراء من قبل مقدّمي الخدمات عبر حفظ البيانات في الأرشيف لضمان صونها من التلف أو التغيير أو فقدان قيمتها القانونية، مع الالتزام بتقديمها لجهات التحقيق المختصة فور طلبها.[2]

[1] سبق التطرق إليها وبيان تعريفها وتعرف أيضا " **على أنهم كل كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصال وأي كيان اخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصالات المذكورة أو المستعمليها** "

[2] رشيدة بوبكر، **جرائم الإعتداء على نظم المعالجة الالية في التشريع الجزائري**، ط1، منشورات الحلبي الحقوقية، بيروت لبنان، 2012، ص 448.

المبحث الثاني: آليات المؤسساتية لمكافحة الجريمة السيبرانية

إن التشريعات وحدها لا تكفي لمواجهة الجريمة السيبرانية، إذ لا بدّ من ترجمة النصوص القانونية إلى هياكل مؤسساتية متخصصة تضطلع بمهام الوقاية والكشف والتحقيق والملاحقة، وقد أدركت الجزائر مبكرًا أن التصدي لهذا النوع من الإجرام يستلزم بناء منظومة متكاملة تجمع بين الكفاءة التقنية والصلاحية القانونية، فأنشأت على الصعيد الوطني أجهزة متخصصة تتوزع بين فرق تابعة للأمن الوطني والدرك الوطني إضافة إلى مصلحة الدفاع السيبراني والقطب الجزائي المتخصص، فيما عزّزت على الصعيد الدولي انخراطها في آليات التعاون متعددة الأطراف نظرًا للطابع العابر للحدود الذي يميّز هذه الجرائم، وصولاً إلى انضمامها إلى معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية، وعليه يتناول هذا المبحث هذه الآليات في مطلبين: الأول وطني، والثاني دولي.

المطلب الأول: آليات المؤسساتية الوطنية لمكافحة الجريمة السيبرانية

أولت الجزائر اهتماماً بالغاً ببناء منظومة مؤسساتية متخصصة لمكافحة الجريمة السيبرانية، إدراكاً منها لقصور الأساليب التقليدية أمام تطور هذا الإجرام وما يستلزمه من هياكل تقنية وقانونية متكاملة، وقد توزعت هذه الآليات بين أجهزة أمنية للتحري والاستقصاء كفرق الأمن الوطني والدرك الوطني، وهياكل للدفاع السيبراني، وجهات قضائية متخصصة كالقطب الجزائي المتخصص، وهو ما سيتم تناوله من خلال ثلاثة فروع متتالية.

الفرع الأول: الفرق التابعة للأمن والدرك الوطني

في ظل التطور التكنولوجي المتسارع وتنامي الجريمة السيبرانية بوصفها تهديدًا يمس الأفراد والمؤسسات على حدٍّ سواء، عمدت أجهزة الأمن إلى تطوير قدراتها من خلال إنشاء فرق متخصصة داخل كل من الأمن الوطني والدرك الوطني للتحقيق في الجرائم المعلوماتية ومكافحتها، وهو ما سيتم تناوله في فرعين: الأمن الوطني أولًا، والدرك الوطني ثانيًا.

أولا: الفرق التابعة للأمن الوطني

تتوافر لدى المديرية العامة للأمن الوطني هياكل متخصصة[1] ، وتتمثل أبرزها في المصلحة المركزية لمكافحة الجريمة المعلوماتية، إضافة إلى نيابة مديرية الشرطة العلمية والتقنية.

1. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني SCLC

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشأت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في 2015 . [2]

تتمثل مهامها فيما يلي: [3]

1-تقديم الدعم الفني لمصالح الشرطة القضائية في مجالات التحري والتقنيات الرقمية.

2-الإسهام في تأمين وحماية الأنظمة المعلوماتية والفضاء السيبراني على المستوى الوطني.

3-التعاون والمساهمة في تنفيذ التحقيقات والتحريات ذات الطابع الوطني والدولي

4-الإسهام في تأهيل وتكوين العناصر المتخصصة ضمن فرق مكافحة الجريمة المعلوماتية على مستوى أمن الولايات.

5-المشاركة الفاعلة في تنفيذ برامج الوقاية وحملات التوعية

---

[1] **الهياكل المتخصصة:** هي أجهزة أو هيئات تُنشأ للقيام بمهام محددة في مجال معين، وتضم مختصين ذوي كفاءة وخبرة لضمان فعالية أكبر في أداء وظائفها.

[2] إدريس عطية، **مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، 2019، ص 114.

[3] فتيحة سويسي، **التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها**، مداخلة مقدمة خلال الندوة البحثية من طرف مركز البحوث القانونية والقضائية، بتاريخ 2022/01/18، ص ص 17 18.

6-تقنيات المراقبة الإلكترونية الاستباقية لرصد المخاطر والتهديدات.

7-تشكيل فرق ولائية متخصصة في مكافحة الجرائم المعلوماتية على الصعيد الوطني [1]

2. نيابة مديرية الشرطة العلمية والتقنية

بادرت المديرية العامة للأمن الوطني إلى تحديث هيكلها التنظيمي من خلال إنشاء وحدات متخصصة لمكافحة مختلف أنواع الجرائم، حيث استحدثت المديرية العامة للشرطة القضائية أربع مصالح على شكل نيابات مديرية تتمثل في نيابة مديرية الشرطة العلمية، ونيابة مديرية الاقتصادية والمالية، ونيابة القضايا الجنائية، ونيابة مديرية الشرطة العلمية والتقنية، وقد أُسندت لهذه الأخيرة مهمة مكافحة الجريمة المعلوماتية عبر مصالح عملية متخصصة تتكفل بالبحث والتحري والتحقيق في الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، وتتمثل هذه الوحدات في المخبر المركزي للشرطة العلمية بالجزائر العاصمة والمخابر الجهوية بكل من قسنطينة ووهران، حيث تضطلع جميعها بمهام تحليل الأدلة الجنائية وإجراء التحريات التقنية، ويضم كل مخبر منها دائرتين متخصصتين في هذا المجال هما : [2]

1-الدائرة العلمية تتولى أعمال البحث والتحقيق وتحليل الأدلة المتصلة بالمجال البيولوجي، الطب الشرعي والكيمياء والمخدرات، المتفجرات.

2-الدائرة التقنية تتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية عن الجرائم التي

3-تستعمل فيها الأسلحة والقذائف بمختلف أنواعها وكذلك جرائم التزوير، إضافة إلى الجرائم المعلوماتية.

---

[1] سميحة بلقاسم، حميد بوشوشة، **الجريمة الالكترونية بعد جديد للإجرام في الجزائر واقعها واليات مجابهتها**، مجلة العلوم الإنسانية، لجامعة أم البواقي، المجلد 10 العدد 01، 2023، ص ص 548 549.

[2] ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه في الحقوق، تخصص قانون العقوبات، والعلوم الجنائية، جامعة باتنة، كلية الحقوق والعلوم السياسية، 2015-2016، ص ص 177 178 .

ثانيا: الفرق التابعة للدرك الوطني

في إطار تعزيز منظومة الأمن السيبراني الوطني، بادرت فرق الدرك الوطني إلى إنشاء هياكل ومراكز متخصصة تُعنى بالتصدي للتهديدات الإلكترونية ومواجهة الجرائم المعلوماتية، ومن أبرز هذه الهياكل نذكر:

1. مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني

أنشأته قيادة الدرك الوطني في سنة 2008 وهو مركز متخصص في محاربة الجريمة السيبرانية، ويعتبر عصب الجهاز المختص في مكافحة الجريمة السيبرانية مقره بئر مراد رايس، [1] اعتبر بمثابة مركز توثيق يعكف هذا المركز على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت، ويعتبر أيضا هذا المركز نقطة اتصال وطني [2] .

تتمثل مهامه فيما يلي: [3]

1- ضمان المراقبة الدائمة والمستمرة على شبكة الإنترانت.

2-القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.

3-مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة في شبكة الإنترانت.

4-المشاركة في عمليات التحري والتسرب عبر شبكة الإنترانت لفائدة وحدات الدرك الوطني والسلطات القضائية.

---

[1] نورة العقون، المرجع السابق، ص 58.

[2] سمير بارة، **الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر والتحديات**، مداخلة في كلية الحقوق والعلوم السياسية جامعة ورقلة، د س ن، ص 435.

[3] عمار حشمان، المرجع السابق، ص 43.

5-المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية. [1]

2. المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع للدرك الوطني

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني " ببوشاوي " حيث أنشئ هذا المعهد بموجب المرسوم الرئاسي 183/04 الصادر بتاريخ 26-06-2004 ودخل حيز الخدمة ابتداء من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و2009 كرست لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية. ويعد مكسبا مؤسساتيا مهما للجزائر بفضل اعتماده على تقنيات حديثة ومتطورة في مجال التحقيقات ومكافحة الجريمة[2]، إضافة إلى تبنيه نظام إدارة الجودة الذي مكنه من الحصول على شهادات اعتماد وطنية ودولية وهو مؤسسة عمومية ذات طابع إداري وتتمتع بالشخصية المعنوية والاستقلال المالي موضوع تحت وصاية وزير الدفاع الوطني.[3]

تنقسم دائرة الإعلام الآلي والإلكتروني إلى ثلاثة مخابر متخصصة، يُلحق بكل منها فريق عمل (فصيلة) يتولى مهام استخراج المعطيات من وسائط المعلومات المختلفة، مع ضمان سلامة الدليل الإلكتروني ومشروعيته، وتشمل هذه المخابر مخبر الإعلام الآلي، مخبر معالجة الفيديو، ومخبر تحليل الصوت الذي يعنى على سبيل المثال بالتأكد من شرعية التسجيلات الصوتية. [4]

الفرع الثاني: مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة

بالنظر الحساسية قطاع الدفاع الوطني أستحدث بتاريخ 06 نوفمبر 2015، على مستوى دائرة الاستعمال والتحضير الأركان الجيش الوطني الشعبي مصلحة الدفاع السيبراني ومراقبة أمن

---

[1] سمير بارة، المرجع السابق، ص 435.

[2] https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php تاريخ الاطلاع 26-04-2026، الساعة 02:20.

[3] إدريس عطية، المرجع السابق، ص 113.

[4] عدلي دحمان، سعد الدين ثامر البشير، **التحقيق الجنائي في الجرائم الالكترونية**، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية جامعة زيان عاشور، الجلفة 2020-2021، ص 40.

الأنظمة"، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، ومن بين المحاور التي تناولتها الأرضية العملياتية لهذه المصلحة، تذكر ما يلي: [1]

1-توجيه، تنفيذ وتأطير الأعمال في هذا المجال لا يجب أن يتعدى الإطار الوظيفي أو التنظيمي.

2-تطوير وتعزيز المنظومة القانونية لتفادي التجاوزات أثناء استخدام التكنولوجيا وضمان حماية منظومات الإعلام.

3-اعتماد التكوين التقني والعلمي لإنتاج الكفاءات والمهارات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية وبالتالي تفادي الأخطار الإجرامية.

4- غرس ثقافة الاستعمال الكيفي لهذا العنصر الحيوي تكنولوجيات الإعلام والاتصال من خلال حملات تحسيسية لكافة مستخدمي المؤسسة بغض النظر عن الرتبة أو الوظيفة.

5-الاعتماد وبطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع استجابة للتطورات الحاصلة في مجال التكنولوجيا.

6-فتح مجال التعاون الدولي مع المؤسسات العسكرية الأجنبية، خاصة تلك التي لها رصيد في المجال لتبادل الخبرات والاستفادة من تجاربهم في هذا المجال.

وتتمحور إستراتيجية الدفاع السيبراني للجيش الوطني الشعبي على سبعة محاور أساسية **تتمثل في الجوانب التالية:**

1-الجانب الوظيفي من أجل تعزيز وتحيين الأطر القانونية التي تضمن التطور المتعلق باستعمال تكنولوجيا الإعلام والاتصال وتامين منظومات الإعلام؛

2-الجانب البشري من خلال تكوين وكفاءة وجاهزية الموارد البشرية لأي هجوم سيبراني يهدد الأمن القومي الجزائري؛

[1] بوعرعار عادل، المرجع السابق، ص ص 101 102.

3-الجانب التقني ويتعلق بمدى كفاءة الأجهزة والوسائل المستعملة مع ضمان اليقظة للكشف والرد على الهجمات السيبرانية. [1]

الفرع الثالث: القطب الجزائي لمكافحة الجرائم المتعلقة بتكنلوجيا الإعلام والاتصال

تم إنشاء القطب الجزائي الوطني المتخصص لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون 21- 11 المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية وحدد اختصاصه النوعي والإقليمي ضمن المواد 211 مكرر 22 و23 و24 و25 و26 و27 و28 و29 منه [2] ويمكن تعريفه بأنه هيئة قضائية جزائية أنشأها المشرع الجزائري تختص بالنظر في الجرائم التي تتعلق بالجرائم المعلوماتية. [3]

ويختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتدقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:

1- الجرائم التي تمس بأس الدولة أو بالدفاع الوطني.

2- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.

---

[1] عبد الله جعفري، **التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري**، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية أدرار المجلد 06، العدد 06، 2022، ص 2.

[2] القانون رقم 21-11 المؤرخ في 25 أوت يتمم الأمر رقم 66-155 المؤرخ في 8 جوان 1966، **المتضمن قانون الإجراءات الجزائية**، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، عدد 65، الصادرة بتاريخ 26 أوت 2021 ص ص 7 8 9.

[3] سهيل صليحة، سويسي فريدة، القطب **الجزائي الوطني المتخصص بمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال** شهادة ماستر، جامعة البشير الإبراهيمي برج بوعريريج، 2021 – 2022، ص 8.

3- جرائم نشر وترويج أنباء مغرضه تمس النظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية. [1]

المطلب الثاني: آليات المؤسساتية الدولية لمكافحة الجريمة السيبرانية في إطار التعاون الدولي

لا تعترف الجريمة السيبرانية بالحدود الجغرافية ولا تقف عند سيادة الدول، مما يجعل الاعتماد على الآليات الوطنية وحدها غير كافٍ لمكافحتها، ويستدعي ذلك الانخراط في منظومة تعاون دولي متكاملة لمواجهة هذا النوع من الإجرام العابر للحدود. وقد تجسد هذا التعاون في جهود الأمم المتحدة لوضع أطر قانونية دولية، إلى جانب الاتفاقيات الإقليمية، فضلًا عن دور المنظمات الدولية في تنسيق الجهود وتبادل المعلومات بين الدول. وفي هذا الإطار، انخرطت الجزائر في هذه المنظومة الدولية، وتُوِّج ذلك بتوقيعها على معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية، وعليه سيتم تناول هذه الآليات في أربعة فروع متتالية.

الفرع الأول: الأمم المتحدة في مكافحة الجريمة السيبرانية

أوصى المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة بأن تتولى المنظمة دورا رئيسيا في صياغة سياسة منع الجريمة وإرساء العدالة الجنائية الدولية، وقد تحقق ذلك عندما وافقت الجمعية العامة للأمم المتحدة على هذه التوصية في عام 1950 مما أدى إلى إنشاء اللجنة الاستشارية لمنع الجريمة ومعاملة المجرمين التي تضطلع بمكافحة الجريمة وتقديم المشورة للأمين العام بالإضافة إلى وضع برامج ورسم سياسات للتدابير الدولية في هذا المجال.[2]

---

[1] قانون 09-04، المرجع السابق، ص ص 8 9.

[2] قطاف سليمان، بوقرين عبد الحليم، **مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية**، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 02، 2022، ص 73.

كما أكد المؤتمر على ضرورة تطبيق التطورات الجديدة في العلم والتكنولوجيا في جميع الأماكن لصالح الجمهور وبالتالي منع الجريمة بفعالية، ويمكن إجمال توصيات مؤتمر هافانا 1990 في المبادئ التالية:

1-تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية.

2-تعزيز أمن الكمبيوتر والضوابط الوقائية.

3-توفير تدريب كافي للموظفين والهيئات المسؤولة عن منع الجرائم الاقتصادية وجرائم الحاسب الآلي والتحري والادعاء فيها.[1]

4-تضمين آداب الحاسب الآلي ضمن مقررات الاتصال والمعلومات وتبني سياسات لمعالجة القضايا المتعلقة بالضحايا في هذه الجرائم.

5-تعزيز التعاون الدولي لمكافحة هذه الجرائم بشكل فعال.

ضف إلى ذلك أن أفضل إستراتيجية طويلة الأجل لمكافحة الجريمة السيبرانية هي من خلال اتفاقيات الدولية أي التعاون في تقديم مرتكبي جرائم الكمبيوتر إلى العدالة نظرا لانتشار العالمي للأنترنت. [2]

الفرع الثاني: الاتفاقيات الإقليمية في مكافحة الجريمة السيبرانية

تتصدى الاتفاقيات الإقليمية لمواجهة الجريمة السيبرانية بما تعجز عنه الجهود الفردية للدول، وفي هذا الفرع نستعرض أبرزها متمثلةً في اتفاقية بودابست، واتفاقية جامعة الدول العربية، وجهود الاتحاد الإفريقي، والمعاهدة الأوروبية.

أولا: اتفاقية بودابست

شهدت العاصمة المجرية بودابست في أواخر عام 2001 اعتماد أولى المعاهدات الدولية لمكافحة الجرائم المعلوماتية، وهو ما شكل نقطة محورية في بلورة التضامن والتعاون الدولي

[1] قطاف سليمان، بوقرين عبد الحليم، المرجع السابق، ص 74.

[2] المرجع نفسه، ص 75.

لمواجهة هذه الظاهرة المتنامية التي أصبحت تهدد الأملاك والأفراد على حد سواء، وقد شارك في صياغة هذه المعاهدة عدد كبير من الخبراء القانونيين التابعين لمجلس أوروبا، بالتعاون مع دول أخرى أبرزها الولايات المتحدة الأمريكية بعد سلسلة من المشاورات المكثفة بين الحكومات وأجهزة الشرطة وقطاع تقنية المعلومات على مستوى العالم، وانتهى هذا الجهد إلى توقيع الاتفاقية بتاريخ 23 نوفمبر 2001 من قبل 30 دولة لتفتح الباب لاحقا أمام دول خارج مجلس أوروبا مثل كندا واليابان والولايات المتحدة وجنوب أفريقيا للانضمام إليها ما يعكس طبيعتها العالمية وأهميتها العابرة للحدود.[1]

وتتكون هذه الاتفاقية من ديباجة 48 مادة على أربع فصول، الأول: يعالج استخدام المصطلحات، أما الثاني يعين الإجراءات الواجب اتخاذها على مستوى الوطني، والفصل الثالث يتضمن التعاون الدولي، والفصل الرابع يحدد الأحكام الختامية.[2]

ومن العناصر الأساسية لاتفاقية بودابست: [3]

1-أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعة لهذا المجال.

أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الإلكترونية.

2-أهمية تدابير التعاون الدولي والإقليمي في مكافحة هذه الجرائم والانطلاق أساسا من الإنجازات والجهود الدولية.

3-تحديد الحقوق المتصلة بالرأي وحرية الوصول للمعلومات وحرية البحث والتنقل للمعلومات والأفكار.[4]

ويعكس هذا الهيكل التنظيمي الشامل التوازن بين النصوص الموضوعية، الإجراءات الوطنية والتعاون الدولي، بما يضمن فعالية مكافحة الجرائم المعلوماتية وحماية الحقوق الرقمية على

---

[1] هدى حامد قشوش، **جرائم الحاسب الإلكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة، ص 6.

[2] أشرف عبد القادر قنديل، **الاثبات الجنائي في الجريمة الالكترونية**، دار الجامعة الجديدة، الإسكندرية 2015، ص 95.

[3] خالد الغثير ومحمد القحطاني، **أمن المعلومات بلغة ميسرة**، ط 1، جامعة الملك سعود، الرياض، ص7.

[4] عبد الله عبد الكريم عبد الله، **جرائم المعلوماتية والأنترنت**، الطبعة 1، منشورات الحلبي الحقوقية، لبنان، 2007، ص ص 126 127.

الصعيد العالمي [1] ، ويعتبر هذا الإجراء من أصعب الإجراءات التطبيقية بسبب الطبيعة المؤقتة للأدلة الرقمية وسرعة تغيرها أو محوها.[2]

وعليه اتفاقية بودابست رؤية قانونية دولية متكاملة لمكافحة الجريمة المعلوماتية، حيث وفرت سياجا تشريعيًا وإجرائيًا شاملا، مع تعزيز التعاون الدولي وتطوير أدوات قانونية وتقنية حديثة لضمان كشف الجرائم الرقمية ومعاقبة مرتكبيها بفعالية، مع الحفاظ على حقوق الأفراد وخصوصيتهم. [3]

ثانيا: اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

تعرف الاتفاقية العربية لمكافحة الجرائم التقنية المعلوماتية بأنها اتفاقية إقليمة الدولية المبرمة بين الدول العربية في نطاق جامعة الدول العربية بصورة خطية في أكثر من وثيقة، وقد وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعها الذي عقد في مقر الأمانة العامة لجامعة الدول العربية بتاريخ 21/01/2010 القاهرة وتسمية الاتفاقية " الاتفاقية العربية لمكافحة الجرائم التقنية المعلومات" وتتكون الاتفاقية من ديباجة وثلاثة وأربعين مادة موزعة على خمسة فصول.[4]

ثالثا: جهود الإتحاد الإفريقي

قام الاتحاد الإفريقي بالدعوة إلى عقد مؤتمر استثنائي لوزراء الاتحاد الإفريقي المكلفين بتكنولوجيات المعلومات والاتصالات، والذي انعقد في جنوب إفريقيا خلال الفترة الممتدة من 02 إلى 05 نوفمبر 2009، وذلك بمشاركة مفوضية الاتحاد الإفريقي وبالتعاون مع لجنة الأمم المتحدة الاقتصادية لإفريقيا. وقد تم خلال هذا الاجتماع إعداد اتفاقية تهدف إلى وضع حلول تشريعية وقضائية تتماشى مع احتياجات القارة، وتستجيب للمتطلبات القانونية والتنظيمية المرتبطة بالمعاملات الإلكترونية والأمن السيبراني وحماية البيانات الشخصية. كما أوصى المؤتمر بضرورة

---

[1] يوسف أبو فارة، **الأعمال الإلكترونية**، جامعة القدس المفتوحة، رام الله، د س ن، ص 17.

[2] أحمد الحلو وآخرون، الأدلة الإلكترونية، **الجوانب القانونية والتقنية**، معهد الحقوق، جامعة برزيت، رام الله، 2015، ص 35.

[3] مصطفى، محمد موسى، **دليل التحري عبر شبكة الأنترنت**، دار الكتب القانونية، مصر، المجلة الكبرى، 2005 ص 23.

[4] أحمد حيمي، **أصور جرائم تقنية المعلومات وفقا للاتفاقية العربية**، مجلة العلوم القانونية والسياسية، المركز الجامعي تمنراست الجزائر، المجلد 10، العدد 1، 2014، ص ص 778 779.

إرساء حماية قانونية لأنظمة المعلومات باعتبارها من القيم الأساسية للمجتمع، وهو ما أدى لاحقًا إلى تعزيز الجهود الرامية إلى سن تشريعات خاصة بمكافحة الجريمة الإلكترونية، حيث اجتمع في جوان 2014 قادة الدول الأعضاء في الاتحاد الإفريقي البالغ عددها 54 دولة، وتمت المصادقة على اتفاقية الاتحاد الإفريقي المتعلقة بالأمن السيبراني وحماية البيانات الشخصية. [1]

رابعا: جهود المجلس الأوروبي (المعاهدة الأوربية)

وقّعت اللجنة الخاصة بقضايا الجريمة، بتكليف من المجلس الأوروبي، على المسودة النهائية للمعاهدة التي تهدف إلى مساعدة الدول في مكافحة الجرائم الإلكترونية، وبعد المصادقة عليها من طرف رئاسة المجلس وتوقيع الدول المعنية، أصبح من الضروري على هذه الدول سنّ التشريعات اللازمة، على الأقل في حدها الأدنى، لمواجهة الجرائم المعلوماتية العالمية، بما في ذلك الدخول غير المصرح به، والتلاعب بالبيانات، والاحتيال، والتزوير المرتبط بالحاسوب.[2]

الفرع الثالث: المنظمات الدولية الفعالة في مواجهة الإجرام السيبراني

بادرت العديد من المنظمات الدولية الكبرى في مواجهة هذا النمط من الجريمة من منظمات تقنية وتشريعية الى منظمات أمنية وغيرها ... الخ مثل: الأنتربول (INTERPOL) [3] الاتحاد الدولي للاتصالات (ITU)، منظمة التعاون الاقتصادي والتنمية (OECD) المنظمة العالمية للملكية الفكرية (WIPO). في هذا الفرع سنأخذ منظمة التعاون الاقتصادي والتنمية (أولا) والمنظمة العالمية للملكية الفكرية (WIPO) (ثانيا) كمثال فقط على المنظمات الدولية الفاعلة في هذا المجال وهذا لا يمنع أن هناك منظمات أخرى فاعلة غير التي ذكرتها سابقا.

---

[1] مراد مشوس، **الجهود الدولية لمكافحة الإجرام السيبراني**، مجلة الواحات للبحوث والدراسات جامعة غرداية، العدد02، 2019، د ت.

[2] جعفر حسن جاسم الطائي، **جرائم تكنلوجيا المعلومات**، ط1، دار البادية ناشرون وموزعون، عمان، 2010، ص 228.

[3] المنظمة الدولية لشرطة الجنائية **(أنتربول)** هي منظمة حكومية دولية خاضعة للقانون الدولي ولديها هدفان هما ربط أجهزة الشرطة ومنع ومحاربة الجريمة وتعد أكبر منظمة دولية في العالم حيث تضم 195 من البلدان الأعضاء.

أولا: منظمة التعاون الاقتصادي والتنمية (OECD)

هي منظمة اقتصادية حكومية دولية تضم 35 دولة عضو، تأسست عام 1961 لتحفيز التقدم الاقتصادي والتجارة العالمية [1]. من خلال العمل على تحقيق أعلى مستويات النمو الاقتصادي، بدأت هذه المنظمة الاهتمام بالجرائم المرتكبة عبر الأنترنت منذ عام 1978، حيث وضعت مجموعة أدلة وقواعد إرشادية تتصل بتقنية المعلومات، وبعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها. [2]

ثانيا: المنظمة العالمية للملكية الفكرية (WIPO)

هي إحدى الوكالات التابعة للأمم المتحدة، وقد اهتمت هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم، بهدف دعم وتشجيع الابتكار، وتطوير الأدوات الإدارية التي تختص بحماية الملكية الصناعية المصنفات الأدبية والفنية.[3]

فلقد تعددت الاتفاقيات التي نظمت حقوق الملكية الفكرية عموما وبراءة الاختراع بصفة خاصة بداية من اتفاقية " **برن** " انتقالا إلى اتفاقية المنظمة العالمية للملكية الفكرية (WIPO)، وأخيرا اتفاقية " **التربس** " [4]

اهتمت هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، [5] ، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة

---

[1] الموقع الرسمي لمنظمة التعاون الاقتصادي و التنمية الدولية :
https://www.ccacoalition.org/ar/partners/organisationeconomic-co-operation-and-development-oecd تاريخ الاطلاع 25-04-2026 على الساعة 3:12

[2] غازي عبد الرحمان هيان الرشيد، **الحماية القانونية من الجرائم المعلوماتية**، الحاسب والأنترنت، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية قفي لبان، كلية الحقوق، 2004، ص 179.

[3] Ginevra Assia Antonelli, **Tackling Open Innovation Challenges: Intellectual Property, Trust Dynamics and Stakeholder Governance**, PhD Dissertation, Luiss Guido Carli University, Italy, 2025, p. 22.

[4] ربحي محمد، قراءة **في اتفاقية تريبس (TRIPS)**، مجلة المعيار، جامعة تيسمسيلت، المجلد 13، العدد 01، 2022 ص 552.

[5] غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص 181.

المتعمدة والمرتكبة في إطار[1]، والتي وفرت بموجبها الحماية القانونية للبرامج وقواعد البيانات المعلوماتية تنص المادة الرابعة من معاهدة هذه المنظمة (1996) على أنه:[2]

ساد الاتجاه لدى أغلب الدول الصناعية ودول العالم الثالث إلى الميل إلى خضوع برامج الحاسب الآلي لقوانين حماية حق المؤلف حيث عدلت معظم الدول تشريعاتها الخاصة بحق المؤلف وأضافت برامج الحاسب إلى المصنفات الأدبية المحمية وفقا للقانون وذلك نتيجة لاستمرار لجان الخبراء في دراسة الأسلوب المناسب لحماية برامج الحاسب الآلي ومسائلتها الفنية عبر الاجتماعات المتكررة وبالتعاون ما بين الويبو واليونسكو.[3]

الفرع الرابع: توقيع الجزائر على معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية

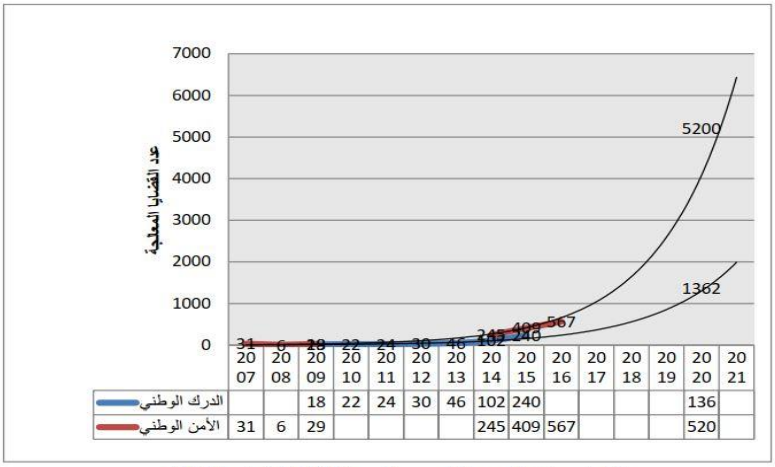
عرفت الجزائر بداية الجريمة السيبرانية قبل سنة 2008 بصورة محدودة نسبيا، حيث لم تتعد عمليات نسخ الأقراص بشكل غير قانوني وما إلى ذلك، فلم تكن تتطلب التدخل الأمني، لكن بعد اقتحام الجزائر عالم الأنترنت الفائق السرعة عبر خطوط ADSL والزيادة الطردية لعدد المشتركين سنة بعد سنة حتى وصل سنة 2021 إلى 26.35 مليون مشترك في مواقع التواصل حسب آخر تقرير لموقع داتاريبورتال – DATAREPORTAL" ، حيث أدى هذا التحول الرقمي الهائل إلى حتمية مواجهة السلبيات المرافقة له ، فمن خلال المخطط البياني التالي سنحاول استعراض تطور نسب الجرائم السيبرانية المسجلة بدلالة التسلسل الزمني:[4]

[1] يوسف صغير، **الجريمة المرتكبة عبر الأنترنت**، مذكرة ماجستير حقوق جامعة مولود معمري تيزي وزو، 2013، ص 98.

[2] أسماء فيلالي، **حقوق الملكية الفكرية للمصنفات المعلوماتية**، مجلة آفاق علمية، جامعة تلمسان المجلد 14 العدد 01، ص 615.

[3] محمود احمد عبابنة، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 161.

[4] بوعرعار عادل، **الاليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر**، مجلة سوسيولوجيا الجريمة للبحوث والدراسات في الظواهر الإجرامية، جامعة محمد فارس المدية، المجلد 06، العدد 01، 2025، ص 95.



المصادر: (حملاوي و المقدم عز الدين 2015)(باشوش 2021)

شكل رقم 01: قضايا الجرائم السيبرانية المعالجة من قبل المصالح الأمنية خلال 15 سنة الماضية.

وفي ظل التنامي المتسارع للجرائم السيبرانية وتزايد آثارها العابرة للحدود، برزت الحاجة إلى وضع إطار دولي موحّد يهدف إلى مكافحة هذه الجرائم وتعزيز التعاون القضائي والأمني بين الدول، في إطار انخراطها في الجهود الدولية، قامت الجزائر بالتوقيع على هذه الاتفاقية بتاريخ 25 أكتوبر 2025 بالعاصمة الفيتنامية هانوي، ممثلة في الأمين العام لوزارة الشؤون الخارجية، وذلك بتكليف من رئيس الجمهورية. ويعكس هذا التوقيع التزام الجزائر بتعزيز التعاون الدولي في مكافحة الجريمة السيبرانية، كما يؤكد سعيها إلى مواكبة التطورات القانونية الدولية في هذا المجال.

ومن جهة أخرى، يُبرز الدور الفعّال للجزائر في إعداد هذه الاتفاقية، حيث ترأست اللجنة المخصصة لصياغتها منذ سنة 2021 [1] ، وعليه، فإن توقيع الجزائر على هذه الاتفاقية لا يُعد مجرد إجراء شكلي، بل هو امتداد لدورها الريادي في بلورة قواعد القانون الدولي في مجال مكافحة الجرائم المعلوماتية.

غير أنّ دخول هذه الاتفاقية حيّز التنفيذ يبقى مرهوناً باستكمال إجراءات التصديق من قبل عدد كافٍ من الدول، وهو ما يجعل من المرحلة المقبلة حاسمة في تفعيل أحكامها على الصعيد الدولي.

[1] وزارة الشؤون الخارجية الجزائرية، **توقيع الجزائر على اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية**، بيان رسمي، 25 أكتوبر 2025، الموقع الرسمي: www.mfa.gov.dz

خلاصة الفصل الثاني

يتضح من خلال هذا الفصل أن المشرّع الجزائري سعى إلى بناء منظومة متكاملة لمكافحة الجريمة السيبرانية تجمع بين الجوانب التشريعية والإجرائية والمؤسساتية، حيث يشكّل القانون 09-04 الإطار الأساسي في هذا المجال، وتم تدعيمه بالقانون 18-04 المتعلق بالبريد والاتصالات الإلكترونية والقانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي، بما يعكس توجه المشرّع نحو تعزيز الحماية القانونية للفضاء الرقمي ومواكبة التطور التكنولوجي. كما تم استحداث آليات إجرائية خاصة مثل التسرب الإلكتروني واعتراض المراسلات والحفظ والإفشاء العاجل للمعطيات الإلكترونية، بهدف تسهيل كشف الجرائم السيبرانية وجمع الأدلة الرقمية وملاحقة مرتكبيها في إطار قانوني يوازن بين الفعالية الإجرائية وضمان الحقوق والحريات. ومن الناحية المؤسساتية، تم الاعتماد على أجهزة متخصصة على مستوى الأمن الوطني والدرك الوطني، إلى جانب إنشاء مصالح للدفاع السيبراني وأقطاب جزائية متخصصة، فضلاً عن تعزيز التعاون الدولي من خلال الاتفاقيات والمنظمات ذات الصلة، نظراً للطابع العابر للحدود لهذه الجرائم. ورغم ذلك، تبقى فعالية هذه الآليات مرتبطة بمدى تطويرها المستمر ومواكبتها للتطور التكنولوجي المتسارع.

الخـــاتـــمة

الخاتمة

في ضوء دراستنا لموضوع الآليات المستحدثة لمكافحة الجريمة السيبرانية يتضح أن هذه الجريمة تُعد من أخطر صور الإجرام المعاصر، لارتباطها الوثيق بالتطور التكنولوجي واعتمادها على الوسائل الإلكترونية الحديثة، كما يتميز مرتكبوها بكونهم مجرمين غير تقليديين ذوي قدرات تقنية عالية، مما يجعل من هذه الجرائم صعبة الاكتشاف والتحري، وأصعب في الإثبات عند وقوعها.

وتزداد خطورة الجريمة السيبرانية لكونها جرائم عابرة للحدود، لا تقف عند إقليم معين، إضافة إلى ما قد يساهم به الضحية أحياناً في وقوعها نتيجة الجهل أو الإهمال أو ضعف الوعي الأمني الرقمي، فضلاً عن كونها جرائم " ناعمة " تعتمد على الخداع والتلاعب أكثر من القوة المادية المباشرة، لكنها رغم ذلك تُحدث أضراراً جسيمة تمس الأفراد والمؤسسات وحتى الدول.

ومن هنا تبرز أهمية تطوير وتفعيل الآليات المستحدثة لمكافحة هذه الجرائم، سواء على المستوى التشريعي أو الإجرائي أو التقني، بما يضمن تعزيز القدرة على الوقاية منها، وكشفها، وملاحقة مرتكبيها بفعالية أكبر، حمايةً للأفراد وصوناً للأمن السيبراني داخل المجتمع.

نتائج

- الجريمة السيبرانية جعلت جميع الأنظمة المعلوماتية التابعة للمؤسسات السيادية، والشركات الكبرى، والمراكز المالية، إضافة إلى الحسابات الخاصة بالأفراد، عرضة للاختراق والتهديد بهدف الابتزاز والمساومة والتجسس، رغم ما توفره الدولة من إمكانيات مادية وتقنية وبشرية مخصصة للحماية.
- القصور في البنية التشريعية والتنظيمية، وعدم إلمام القوانين بمختلف مكونات الثورة المعلوماتية، مثل المعاملات البنكية والشبكة العنكبوتية، إضافة إلى التوجه نحو الإجراءات

الردعية والتدابير الوقائية للحد من القرصنة، قد أظهر ضعف التحكم في تكنولوجيات الإعلام والاتصال.

- تسعى الدول والحكومات بشكل واضح إلى الحد من الجرائم السيبرانية وآثارها من خلال عدة وسائل، منها فرض سياسات دولية وعقوبات صارمة على مرتكبي هذه الجرائم، وتفعيل أحدث التقنيات والوسائل للكشف عن هوية الجناة، إضافة إلى نشر التوعية داخل المجتمع حول مخاطر الجرائم الإلكترونية، وتعريف الأفراد بطرق حماية معلوماتهم وخصوصيتهم مثل الحسابات البنكية وبطاقات الائتمان، فضلاً عن إنشاء خطوط هاتفية ومؤسسات تابعة للدولة لتلقي البلاغات المتعلقة بهذا النوع من الجرائم.

اقتراحات

1. وضع تعريف قانوني دقيق للجريمة السيبرانية في التشريع الجزائري، سواء من خلال أحكام القانون رقم 25-14 لقانون الإجراءات الجزائية الجديد ، أو عبر مراجعة وتعديل القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
2. مراجعة وتعديل أحكام القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال استحداث نصوص قانونية وآليات حديثة تتلاءم مع التطور المتسارع للجريمة السيبرانية وأساليب ارتكابها، مع تطوير وسائل المكافحة والتحري، بالنظر إلى أن الآليات التقليدية لم تعد كافية لمواجهة هذا النوع المستحدث والمتجدد من الإجرام.
3. إعداد استراتيجية وطنية شاملة لتعزيز ثقافة الأمن المعلوماتي، مع تنظيم دورات تدريبية وفق المعايير الدولية وإشراك الفاعلين الأمنيين والتقنيين.
4. تطوير المنظومة التشريعية السيبرانية لمواكبة التطور التكنولوجي وتعزيز حماية الأنظمة المعلوماتية والحد من الجريمة السيبرانية .

5. تعزيز التعاون الدولي لمكافحة الجريمة السيبرانية، خاصة في مجال تسليم المجرمين والإنابة القضائية الدولية، بالنظر إلى الطابع العابر للحدود الذي تتسم به هذه الجرائم، الأمر الذي يقتضي الإسراع في تفعيل الاتفاقيات الدولية التي صادقت عليها الجزائر مؤخراً، بما يسهم في سد الثغرات الإجرائية وتحقيق فعالية أكبر في مكافحة هذا النوع من الإجرام.
6. إنشاء نظام اتصال دولي بين أجهزة الشرطة لتسريع تبادل المعلومات وجمع الأدلة.
7. تأهيل كوادر متخصصة من الضبط القضائي للتعامل مع الأدلة الرقمية وضمان سلامتها.
8. تشجيع الضحايا على التبليغ عن الجرائم السيبرانية للحد من الإفلات من العقاب.

" خِتاماً أُنجز هذا البحث بعون الله وتوفيقه "

" كما قال تعالى: ﴿ وَقُل رَّبِّ زِدْنِي عِلْمًا ﴾ [طه: 114] "

" راجيًا من الله القبول والسداد."

المصادر والمراجع

قائمة المصادر والمراجع

I. المصادر والمراجع بالغة العربية

أولا: النصوص القانونية

أ- القوانين والأوامر والمراسيم التشريعية

1. الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم، جريدة رسمية للجمهورية الجزائرية، العدد 49، الصادرة بتاريخ 11 يونيو 1966.
2. القانون 04 – 09 المؤرخ في 05 أوت 2009، يتضمن قانون الوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، المؤرخة في 16 أزوت 2009.
3. القانون 18-04 المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، عدد 27، الصادرة بتاريخ 13 مايو 2018.
4. القانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، العدد 71، المؤرخة في 10 نوفمبر 2004.
5. القانون رقم 17-11 المؤرخ في 27-12-2017، والمتضمن قانون المالية للسنة 2018، جر، عدد 76، المؤرخ في 28-12-2017.
6. القانون رقم 20-05 المؤرخ في 28 أفريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، جريدة رسمية للجمهورية الجزائرية، عدد 25، الصادرة بتاريخ 29 أفريل 2020.
7. القانون رقم 21-11 المؤرخ في 25 أوت يتمم الأمر رقم 66-155 المؤرخ في 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، عدد 65، الصادرة بتاريخ 26 أوت 2021.
8. قانون رقم 25-14 مؤرخ في 9 صفر 1447 الموافق 3 غشت 2025، يتضمن قانون الإجراءات الجزائية.

ب- المراسيم الرئاسية

1. المرسوم الرئاسي رقم 20-183، المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 40، الصادرة بتاريخ 18 يوليو 2020.

ثانيا: قرارات دولية

1. الأمم المتحدة، قرار الجمعية العامة رقم 79- 243، 24 ديسمبر 2024.

ثالثا: الكتب

1. إبراهيم خالد ممدوح، الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي، 2009.

2.أحمد الحلو وآخرون، الأدلة الإلكترونية، الجوانب القانونية والتقنية، معهد الحقوق، جامعة برزيت، رام الله، 2015.

3.أحمد خليفة ملط، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

4.أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015.

5.أمحمد أقبلي، عابد العمراني الميلودي، القانون الجنائي الخاص المعمق في شروح، ط 1، دار الرشاد، المغرب، 2020.

6.أمل فوزي أحمد عوض، الملكية الرقمية في عصر الذكاء الاصطناعي، تحديات الواقع والمستقبل، إصدارات المركز الوطني الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، المحرر، برلين ألمانيا.

7. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2011.

8. أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة بين التشريعات العربية والأجنبية، ط1، مكتبة القانون والاقتصاد، الرياض، 2014.

9.إيهاب خليفة، مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي، ط1 العربي للنشر والتوزيع، القاهر، مصر، 2019.

10.بولين انطونيوس، أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت لبنان، 2009.

11.توفيق شرف شمس الدين، مخاطر العملات الافتراضية، كتاب واقع المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية، جامعة الشارقة، حول العملات الافتراضية في الميزان، يومي الثلاثاء والأربعاء 16 و17 أبريل 2019.

12. جعفر حسن جاسم الطائي، جرائم تكنلوجيا المعلومات، ط1، دار البادية ناشرون وموزعون، عمان، 2010.

13.جلال محمد الزعبي، وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان الأردن، 2010.

الحمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر و التوزيع، ط 1، مصر، 2015.

14.خالد الغثير ومحمد القحطاني، أمن المعلومات بلغة ميسرة، ط 1، جامعة الملك سعود، الرياض.

15.داودي خالد، الجريمة الإلكترونية، دار الأعصر للنشر والتوزيع، عمان، 2011.

16.درياد مليكة، نطاق سلطات قاضي التحقيق والرقابة عليها، ط1، ديوان المطبوعات الجامعية، الجزائر، 2014.

17.رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة الالية في التشريع الجزائري، ط1، منشورات الحلبي الحقوقية، بيروت لبنان، 2012.

18.سليمان عبد الله، شرح قانون العقوبات الجزائري، القسم العام، الجريمة، الجزء الأول، دار المطبوعات الجامعية، الجزائر، 2009.

19.شريف سيد كمال، الجريمة المنظمة في القانون المقارن، ط1، دار النهضة العربية، مصر، 2001، ص 139.

20.شمسان ناجي، صالح، الجرائم المستخدمة بطريقة غير مشروعة لشبكة الأنترنت، دار النهضة العربية، القاهرة، مصر، 2009.

21. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، بهجات للطباعة والتجليد، مصر، 2009.

22.عبد الفتاح بيومي حجازي، الدليل الجنائي في الجرائم المعلوماتية، دار الكتب القانونية، مصر، 2008.

23.عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت، الطبعة 1، منشورات الحلبي الحقوقية، لبنان، 2007.

24.عدنان مصطفى البار، الخصوصية وسعي الدولة للرقابة الإلكترونية الشاملة، مركز هردو لدعم التعبير الرقمي القاهر، 2018.

25.عدو عبد القادر، مبادئ قانون العقوبات الجزائري، القسم العام، نظرية الجريمة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2010.

26. غانم مرضي الشمري، الجرائم المعلوماتية، ماهياتها، خصائصها، كيفية التصدي لها قانونيا، ط1، الدار العلمية والدولية للنشر والتوزيع، عمان 2016.

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

28. محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، الجريمة المعلوماتية، الإصدار 2، دار الثقافة للنشر والتوزيع، عمان، الأردن ،2007.

29. محمد صبحي نجم، شرح قانون العقوبات، القسم الخاص، ديوان المطبوعات الجامعية، الجزائر،2005.

30. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، ط2، دار النهضة العربية، القاهرة، مصر، 2009.

31.محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2001.

32. محمود أحمد العرفان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان، 2017.

33. محمود احمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005.

34. مصطفى، محمد موسى، دليل التحري عبر شبكة الأنترنت، دار الكتب القانونية، مصر، المجلة الكبرى، 2005.

35.مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الأنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، 2003.

36. نائلة عادل محمد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، 2005.

37. هدى حامد قشوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة.

38. يوسف أبو فارة، الأعمال الإلكترونية، جامعة القدس المفتوحة، رام الله، د س ن.

39. طلال أبو عفيفة، جرائم الابتزاز الإلكتروني (جرائم الحاسوب)، دار وائل للنشر والتوزيع، عمان، 2026.

رابعا: المذكرات الجامعية وأطروحات الدكتوراه

أ- أطروحات الدكتوراه

1. حايط فاطمة، إجراءات التحقيق في الجرائم الإلكترونية، دراسة مقارنة، أطروحة لنيل شهادة دكتوراه، تخصص قانون جنائي والعلوم الجنائية، جامعة ابن خلدون، كلية الحقوق والعلوم السياسية، تيارت، الجزائر، 2022 -2023.

2. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق، تخصص قانون العقوبات، والعلوم الجنائية، جامعة باتنة، كلية الحقوق والعلوم السياسية، 20015-2016.

3. غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، الحاسب والأنترنت، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية قفي لبان، كلية الحقوق، 2004.

ب- رسائل الماجستير

1. خديجة دحمان صباحية، جرائم السرقة والاحتيال عبر الانترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، رسالة ماجستير، جامعة الجزائر، كلية الشريعة والقانون.

2. سعيداني نعيم، آليات البحث والتحري في الجريمة المعلوماتية في القانون الجزائري، مذكرة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013.

3. عبد الرحمان جميل محمود حسين، الحماية القانونية برامج الحاسب الآلي، مذكرة ماجستير جامعة النجاح الوطنية نابلس، فلسطين، كلية الدراسات العليا، 2008.

4. يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير حقوق جامعة مولود معمري تيزي وزو 2013.

ج- مذكرات الماستر

1. بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة ماستر في الحقوق تخصص قانون الإعلام الآلي والأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، 2021-2022.

2. سهيل صليحة، سويسي فريدة، القطب الجزائي الوطني المتخصص بمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال شهادة ماستر، جامعة البشير الإبراهيمي برج بوعريريج، 2021 – 2022.

3. عباسي خولة، الوسائل الحديثة للإثبات في القانون الجنائي، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2014.

4. عدلي دحمان، سعد الدين ثامر البشير، التحقيق الجنائي في الجرائم الإلكترونية ، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية جامعة زيان عاشور الجلفة 2020-2021.

5. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، في ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، تخصص إدارة التحقيقات الاقتصادية والمالية، جامعة ورقلة، 2019.

6. العيد شعثان، مسعود موفقي، الجرائم السيبرانية في القانون الجزائري، مذكرة ماستر في القانون الجنائي والعلوم الجنائية، جامعة زيان عاشور، الجلفة، الجزائر، 2021 – 2022.

7. محمد بوعمرة، سيد علي بينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري ، مذكرة التخرج لنيل شهادة الماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة أوكلي محمد أولحاج البويرة، 2019-2020.
8. نورة العقون، واقع الفضاء السبيراني وإشكالية الدفاع الوطني في الجزائر، مذكرة التخرج لنيل شهادة الماستر في العلوم السياسية تخصص دراسات أمنية واستراتيجية، جامعة قصدي مرباح ورقلة، كلية الحقوق، 2019.

خامسا: المقالات والدراسات العلمية

1. إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في السريعة الإسلامية والأنظمة الدولية، دراسة تحليلية تطبيقية، مجلة كلية الشريعة والقانون بطنطا، المجلد 30، العدد 2، 2015.
2. أحمد حيمي، أصور جرائم تقنية المعلومات وفقا للاتفاقية العربية، مجلة العلوم القانونية والسياسية، المركز الجامعي تمنراست الجزائر، المجلد 10، العدد 1، 2014.
3. أحمد محمد فتحي الخولي، المسؤولية المدنية الناجمة عن الإستخدام غير المشروع لتطبيقات الذكاء الاصطناعي، الديب فيك نموذجا، مجلة البحوث الفقهية والقانونية، العدد 36، 2021.
4. إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة المصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، المجلد 1، العدد 1، 2019.
5. أسماء فيلالي، حقوق الملكية الفكرية للمصنفات المعلوماتية، مجلة آفاق علمية، جامعة تلمسان المجلد 14 العدد 01.
6. براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، جامعة مولود معمري، تيزي وزو العدد 02، 2016.
7. بن كثير بن عيسى، الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاة، مديرية الدراسات القانونية والوثائق، العدد 63.
8. بوعرعار عادل، الآليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر، مجلة سوسيولوجيا الجريمة للبحوث والدراسات في الظواهر الإجرامية، جامعة محمد فارس المدية، المجلد 06، العدد 01، 2025.

9. تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي، على ضوء القانون ر قم 18-07، دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، جامعة المسيلة، الجزائر، 2018.

10. جبار فطيمة، مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، جامعة مولود معمري بتيزي وزو، العدد 3، ديسمبر 2016.

11. حمزة خضري، عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، العدد 02، المجلد 06، 2020.

12. حنان مهداوي، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، المجلد السادس، العدد 02، 2022.

13. رامي متولي القاضي، مكافحة الإجرام المنظم عبر شبكة الأنترنيت المظلمة، المجلة الجنائية القومية، المجلد 64، العدد 3، 2021.

14. ربحي محمد قراءة في اتفاقية تريبس (TRIPS) مجلة المعيار، جامعة تيسمسيلت المجلد 13 العدد 01, 2022 ص 552.

15. روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، المملكة العربية السعودية، جدة، 2020.

16. سعيدة بوزون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، كلية الحقوق، جامعة الإخوة منتوري قسنطينة، عدد 52، المجلد ب، ص ص47-57، الجزائر.

17. سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر واقعها واليات مجابهتها، مجلة العلوم الإنسانية، جامعة أم البواقي، المجلد 10، العدد 01، جوان 2023.

18. عبد الله جعفري، التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية أدرار المجلد 06، العدد 06، 2022.

19. العرفي فاطمة، تطبيق إجراء التسرب في القانون الجزائري، إشكالية الموازنة بين حماية حق الخصوصية الرقمية ومكافحة جريمة اختطاف الأشخاص، مجلة دراسات وأبحاث، المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، مجلد 13، عدد 4 جويلية 2021.

20. عمارة فوزي، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة منتوري، قسنطينة، عدد 33، 2010.

21. قاسحي فيروز، الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة الجزائر 3، العدد 8، المجلد 7، 2023.

22. قطاف سليمان، بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 02، 2022.

23. لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة، مجلة ميزان، للدراسات القانونية والشرعية، الأردن، 2016.

24. مارلين أورديكيان، العملات الافتراضية المشفرة في الحقل الجنائي السيبراني، مجلة الدفاع الوطني، العدد 108، 2019.

25. ماينو جيلالي وعروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، مخبر القانون والتنمية، جامعة طاهري محمد بشار، المجلد 4، العدد 1، 2023.

26. مراد مشوس، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات جامعة غرداية، العدد02، 2019، دون ترقيم.

27. ممدوح حسن العدوان، المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي، مجلة الشريعة والقانون، جامعة الإمارات العدد 2019.

28. مهدي رضا ، الجرائم السيبرانية وآليات مكافحاها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد 6، العدد 2، جامعة محمد بوضياف، المسيلة، الجزائر، 2021.

29. نسيمة مقبل، الجرائم السيبرانية في الفضاء الاتصالي الجزائري، أنواعها، آثارها وسبال مواجهتها، مجلة معارف، العدد 21، المجلد 18، كلية علوم الإعلام والاتصال، جامعة الجزائر3، الجزائر، 2023.

30. نقادي عبد الحفيظ، التسجيل الصوتي، المجلة للعلوم القانونية والاقتصادية، كلية الحقوق الجزائر، العدد 01، 2009.

31. نورهان محمد الربيعي، الجريمة السيبرانية وآليات مكافحتها دراسة مقارنة، مجلة الفرابي للعلوم الإنسانية، المجلد 03، العدد 01، كلية الحقوق، جامعة عجمان، الإمارات العربية المتحدة، 2024.

32. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآليات التدريب التخصصي للمحققين، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد 2، 1999.

33. وداعي عز الدين، التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، المجلة الأكاديمية للبحث القانوني، مجلد 16، عدد 02، 2017.

34. يحي إبراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، جامعة الإمارات، 2019.

35. يحي ياسين مسعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، مجلة القانونية، جامعة القاهرة، المجلد 4، العدد 4، 2018.

36. يوسف رزوق، حماية المعطيات الشخصية في الجزائر على ضوء قانون رقم 18-07، مجلة معالم الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسبية، الجلفة العدد 05، المجلد 02، 2018.

سادسا: المداخلات والملتقيات والمؤتمرات العلمية

1. الأمم المتحدة 2020، دليل المناقشة لمؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو، اليابان، 20 أبريل 2020.

2. بن غدفة شريفة والقص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها، أعمال الملتقى الوطني، آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 2017.

3. حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني، آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 متارس 2017.

4. رحيمة نميلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، مداخلة في المؤتمر الدولي، 14 طرابلس، عنوان الجرائم الإلكترونية طرابلس، يومي 24 و25 مارس.

5. سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر والتحديات، مداخلة في كلية الحقوق والعلوم السياسية جامعة ورقلة، د س ن.

6.سيناء عبد الله محسن، المواجهة التشرعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر، الدار البيضاء، المملكة المغربية، 2007.

7. العدواني عبد الحميد، إدارة التحريات والتحقيقات الأولية في الجرائم التي تدخل في إختصاص القطب القضائي الجزائي، الملتقى الجهوي حول مكافحة الإجرام الخطير، مجلس قضاء ورقلة، 2009.

8. فتيحة سويسي، التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها، مداخلة مقدمة خلال الندوة البحثية من طرف مركز البحوث القانونية والقضائية، بتاريخ 2022/01/18.

9. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر، الجرائم الإلكترونية، طرابلس، بتاريخ 24-25-03-2017.

10. مفتاح بوبكر المتردي، الجريمة الإلكترونية والتغلب على تحدياتها، مقال مقدم الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-25-09-2012.

11. مؤتمر الأمم المتحدة 14 لمنع الجريمة والعدالة الجنائية، مدينة كيوتو باليابان في الفترة من 7 إلى 12 مارس 2021

سابعا: المحاضرات

1. فريد روابح، محاضرات في القانون الجنائي العام، مطبوعة دروس للسنة الثانية ليسانس، قسم الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر، 2025-2026.

2. قارة أمال، الإطار القانوني للجريمة السبيرانية The legalframework for cybercrime، محاضرة المدرسة العليا للقضاء دفعة 2023-2024.

ثامنا: التقارير

1. اليونيسف، تقرير حالة الأطفال لعام 2017، الأطفال في عالم رقمي.

II. المراجع بالغة الأجنبية

A. Rapports

1. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations, New York, 2013.

B. Livres

1. Debarati Halder and K. Jaishankar, Cyber Crime and the Victimization of Women: Laws, Rights and Regulations, IGI Global, Hershey, 2012.

2. Elaine Rich & Kevin Knight, Artificial Intelligence, 2nd ed., McGraw-Hill, New York, 1991.

3. Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, 3rd ed., Pearson Education, New Jersey, 2010.

C. Theses et mémoires

1. Elena Martellozzo, Cybercrime and Its Victims: Understanding the Global Phenomenon and Responses of International Institutions, PhD Thesis, Middlesex University, United Kingdom, 2019.

2. Ginevra Assia Antonelli, Tackling Open Innovation Challenges: Intellectual Property, Trust Dynamics and Stakeholder Governance, PhD Dissertation, Luiss Guido Carli University, Italy, 2025.

3. John Smith, Cybercrime and Criminal Liability in Digital Environments, Doctoral dissertation, University of Oxford, United Kingdom, 2019.

4. sophie Harleman, Countering Economic Cyber Espionage and the Right to Privacy, PhD Dissertation, Utrecht University, Netherlands, 2025.

D. Articles et études

1. G. M Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries. Journal of Information Engineering and Applications, 4(4) 2014.

2. Regner sabillon Cybercrime and Cybercriminals A Comprechensive Study. International Journal of Computer Networks and Communications Security, vol 4 no 6 2016.kundi,

E. Sites internet

1. Oxford English Dictionary, “Cyber”, Oxford University Press, available at https://www.oed.com

III. المراجع الإلكترونية

1. وزارة الشؤون الخارجية الجزائرية، توقيع الجزائر على اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، بيان رسمي، 25 أكتوبر 2025، الموقع الرسمي: www.mfa.gov.dz

2. المديرية المركزية لأمن الجيش – المعهد الوطني للأدلة الجنائية وعلم الإجرام https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

3. الموقع الرسمي لمنظمة التعاون الاقتصادي و التنمية الدولية https://www.ccacoalition.org/ar/partners/organisationeconomic-co-operation-and-development-oecd

4. الموقع الرسمي وزارة العدل الأمريكية https://www.justice.gov/

5. الموقع الرسمي المنظمة العالمية للملكية الفكرية. https://www.wipo.int/treaties/ar/ip/berne/index.html

الفهرس

الفهرس

مـقـدمـة 1
الفصل الأول: الإطار العام للجريمة السيبرانية
المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية..... 10
المطلب الأول: مفهوم الجريمة السيبرانية..... 10
الفرع الأول: تعريف الجريمة السيبرانية 10
أولا: تعريف الجريمة السيبرانية لغة..... 10
ثانيا: تعريف الجريمة السيبرانية اصطلاحا..... 11
ثالثا: تعريف الجريمة السيبرانية فقها 12
رابعا: تعريف الجريمة السيبرانية قانونا..... 12
الفرع الثاني: خصائص الجريمة السيبرانية 14
أولا: الجريمة السيبرانية يصعب إثباتها..... 14
ثانيا: الجريمة السيبرانية جريمة مستحدثة 15
ثالثا: الجريمة السيبرانية عابرة للحدود 15
رابعا: الجريمة السيبرانية جريمة ناعمة وسهلة الارتكاب 15
خامسا: الجريمة السيبرانية جريمة الأذكياء 16
سادسا: قلة الإبلاغ عن الجريمة السيبرانية 16
الفرع الثالث: الطبيعة القانونية للجريمة السيبرانية 17
أولا: الطبيعة القانونية الخاصة بالجريمة السيبرانية 17
ثانيا: موقف المشرع الجزائري من الجريمة السيبرانية 18
المطلب الثاني: تطور صور الجريمة السيبرانية..... 19
الفرع الأول: الجريمة السيبرانية في صورتها التقليدية 19

أولا: التزوير المعلوماتي (السيبراني) 19
ثانيا: التجسس السيبراني 20
ثالثا: سرقة المعلومات..... 21
الفرع الثاني: الجريمة السيبرانية في أنماطها المستحدثة..... 22
أولا: الحروب السيبرانية والإرهاب السيبراني..... 22
ثانيا: الجرائم المرتبطة بتقنية الذكاء الاصطناعي 23
ثالثا: جرائم العملات المشفرة..... 24
رابعا: الجرائم المرتبطة بأسواق الشبكة الخفية..... 25
خامسا: استخدام التكنولوجيا بغرض تيسير الاتجار بالأشخاص..... 26
المبحث الثاني: الإطار القانوني للجريمة السيبرانية 27
المطلب الأول: أركان الجريمة السيبرانية 27
الفرع الأول: الركن الشرعي..... 27
الفرع الثاني: الركن المادي 28
الفرع الثالث: الركن المعنوي 29
المطلب الثاني: المجرم السيبراني 31
الفرع الأول: تعريف المجرم السيبراني 31
الفرع الثاني: سمات المجرم السيبراني 31
الفرع الثالث: فئات المجرم السيبراني 32
الفرع الرابع: دوافع ارتكاب الجريمة السيبرانية 33
أولا: الدوافع الشخصية 34
ثانيا: الدوافع الخارجية..... 34
خلاصة الفصل الأول 36
الفصل الثاني: آليات مكافحة الجريمة السيبرانية في التشريع الجزائري

المبحث الأول: آليات إجرائية وقائية المستحدثة لمكافحة الجريمة السيبرانية..... 39
المطلب الأول: آليات التشريعية إجرائية لمكافحة الجريمة السيبرانية 39
الفرع الأول: مكافحة الجريمة السيبرانية بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 09-04. 39
أولا: التدابير الوقائية 40
ثانيا: التدابير الإجرائية 41
الفرع الثاني: القوانين اللاحقة المدعمة للقانون 09-04 في مجال الحد من الإجرام السيبراني .. 44
أولا: القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية 44
ثانيا: القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي..... 44
المطلب الثاني: الآليات الإجرائية المستحدثة لملاحقة الجريمة السيبرانية 46
الفرع الأول: التسرب الإلكتروني 46
أولا: تعريف التسرب الإلكتروني 46
ثانيا: الجهات المخول لها قانونا مراقبة عملية التسرب الإلكتروني..... 47
رابعا: شروط التسرب الإلكتروني..... 48
خامسا: القيود الواردة على مباشرة التسرب الإلكتروني..... 49
الفرع الثاني: اعتراض المراسلات والمراقبة الإلكترونية في إطار الإجراءات القانونية 50
أولا: تعريف عملية اعتراض المراسلات السلكية واللاسلكية 50
ثانيا: الشروط المطلوبة في المراسلات محل الاعتراض 51
ثالثا: الشروط القانونية لاعتراض المراسلات..... 51
الفرع الثالث: الحفظ وإفشاء العاجلان للمعطيات الإلكترونية 52
المبحث الثاني: آليات المؤسساتية لمكافحة الجريمة السيبرانية 53
المطلب الأول: آليات المؤسساتية الوطنية لمكافحة الجريمة السيبرانية..... 53

الفرع الأول: الفرق التابعة للأمن والدرك الوطني 53
أولا: الفرق التابعة للأمن الوطني..... 54
ثانيا: الفرق التابعة للدرك الوطني 56
الفرع الثاني: مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة 57
الفرع الثالث: القطب الجزائي لمكافحة الجرائم المتعلقة بتكنلوجيا الإعلام والاتصال 59
المطلب الثاني: آليات المؤسساتية الدولية لمكافحة الجريمة السيبرانية في إطار التعاون الدولي 60
الفرع الأول: الأمم المتحدة في مكافحة الجريمة السيبرانية 60
الفرع الثاني: الاتفاقيات الإقليمية في مكافحة الجريمة السيبرانية..... 61
أولا: اتفاقية بودابست..... 61
ثانيا: اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية 63
رابعا: جهود المجلس الأوروبي (المعاهدة الأوربية)..... 64
الفرع الثالث: المنظمات الدولية الفعالة في مواجهة الإجرام السيبراني 64
أولا: منظمة التعاون الاقتصادي والتنمية (OECD) 65
ثانيا: المنظمة العالمية للملكية الفكرية (WIPO) 65
الفرع الرابع: توقيع الجزائر على معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية 66
خلاصة الفصل الثاني..... 68
الخاتمة 70
نتائج..... 70
اقتراحات 71
قائمة المصادر والمراجع 74
الفهرس 88

الملخص

تتناول هذه الدراسة موضوع الجريمة السيبرانية، التي تُعرّف بأنها كل سلوك غير مشروع يُرتكب باستخدام تكنولوجيا المعلومات والاتصال أو يستهدف الأنظمة المعلوماتية، مثل الاختراق والاحتيال الإلكتروني وانتهاك البيانات، وتهدف إلى تحديد إطارها المفاهيمي والقانوني، وتحليل الآليات القانونية والإجرائية المستحدثة لمكافحتها في التشريع الجزائري، مع إبراز دور الهيئات والأجهزة المختصة، ورصد أبرز التحديات التي تعيق فعالية مكافحتها. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية والتنظيمية وتفسيرها، مع بيان كيفية تطبيقها في الواقع العملي، حيث أظهرت النتائج أن الجريمة السيبرانية تمثل تهديداً متزايداً يستهدف مختلف الأنظمة المعلوماتية الخاصة بالأفراد والمؤسسات، في ظل تسارع التطور التكنولوجي الذي يفوق أحياناً قدرة التشريعات على مواكبته، مما يكشف عن وجود بعض النقائص في المنظومة القانونية والتنظيمية. كما أبرزت الدراسة أهمية تعزيز التعاون الدولي، وتطوير التكوين المتخصص، ونشر الوعي الرقمي كمرتكزات أساسية للحد من هذه الجرائم، وخلصت إلى ضرورة تبني مقاربة شاملة ومتكاملة تجمع بين الجوانب القانونية والتقنية والوقائية، بما يعزز فعالية التصدي للجريمة السيبرانية في الجزائر.

الكلمات المفتاحية: الجريمة السيبرانية، التشريع الجزائري، الأمن السيبراني

Abstract

This study addresses cybercrime, which is defined as any unlawful act committed using information and communication technologies or targeting information systems, such as hacking, online fraud, and data breaches. It aims to identify its conceptual and legal framework, analyze the modern legal and procedural mechanisms adopted to combat it within Algerian legislation, highlight the role of competent authorities and institutions, and examine the main challenges hindering effective enforcement. The study adopts a descriptive-analytical approach through the examination and interpretation of relevant legal and regulatory texts, with a focus on their practical application. The findings reveal that cybercrime represents an increasing threat to the information systems of both individuals and institutions, especially in light of rapid technological developments that often outpace legislative responses, thereby exposing certain shortcomings in the legal and regulatory framework. The study also emphasizes the importance of strengthening international cooperation, enhancing specialized training, and promoting digital awareness as key pillars in combating cybercrime. It concludes that an integrated and comprehensive approach, combining legal, technical, and preventive dimensions, is essential to improve the effectiveness of combating cybercrime in Algeria.

Keywords: Cybercrime, Algerian Legislation, Cybersecurity