الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية الحقوق و العلوم السياسية
قسم الحقوق

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Ghardaïa
Faculté de droit et de sciences politiques
Département de droit

غرداية في: 2025/07/09

شهادة تصحيح

يشهد الأستاذ (ة) : الأخضري فتيحة بصفتها رئيسا في لجنة المناقشة مذكرة الماستر ل:

الطالب : امحمد إسماعيل رقم التسجيل : **39097817**

الطالب : زوبيري عبد الحليم رقم التسجيل : **9074995**

تخصص : ماستر قانون جنائي دفعة **2025** لنظام (ل م د)

أن المذكرة المعنونة بـ : دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية و سبل مكافحتها

تم تصحيحها من طرف الطالبين و هي صالحة للإيداع

إمضاء الأستاذ (ة) رئيس اللجنة المكلف(ة) بمتابعة التصحيح

رئيس القسم

رئيس قسم الحقوق
أبو القاسم عيسى

جامعة غرداية
قسم الحقوق

ملاحظة : تترك هذه الشهادة لدى القسم

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية الحقوق والعلوم السياسية
التخصص القانون الجنائي والعلوم الجنائية

مذكرة تخرج لنيل شهادة الماستر تخصص قانون جنائي والعلوم الجنائية

دور التكنولوجيا الحديثة في ارتكاب الجرائم الإلكترونية وسبل مكافحتها

إعداد الطالب:

– أمحمد إسماعيل

–زوبيري عبد الحليم

إشراف الأستاذ:

الدكتور: كيحول بوزيد

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
الاخضري فتيحة	أستاذ	جامعة غرداية	رئيسا
كيحول بوزيد	أستاذ	جامعة غرداية	مشرفا ومقررا
لغلام عزوز	أستاذ	جامعة غرداية	عضواً مناقشا

الموسم الجامعي :1446/1445 الموافق 2024 /2025

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية الحقوق والعلوم السياسية
التخصص القانون الجنائي والعلوم الجنائية

مذكرة تخرج لنيل شهادة الماستر تخصص قانون جنائي والعلوم الجنائية

دور التكنولوجيا الحديثة في ارتكاب الجرائم الإلكترونية وسبل مكافحتها

إعداد الطالب:

– أمحمد إسماعيل

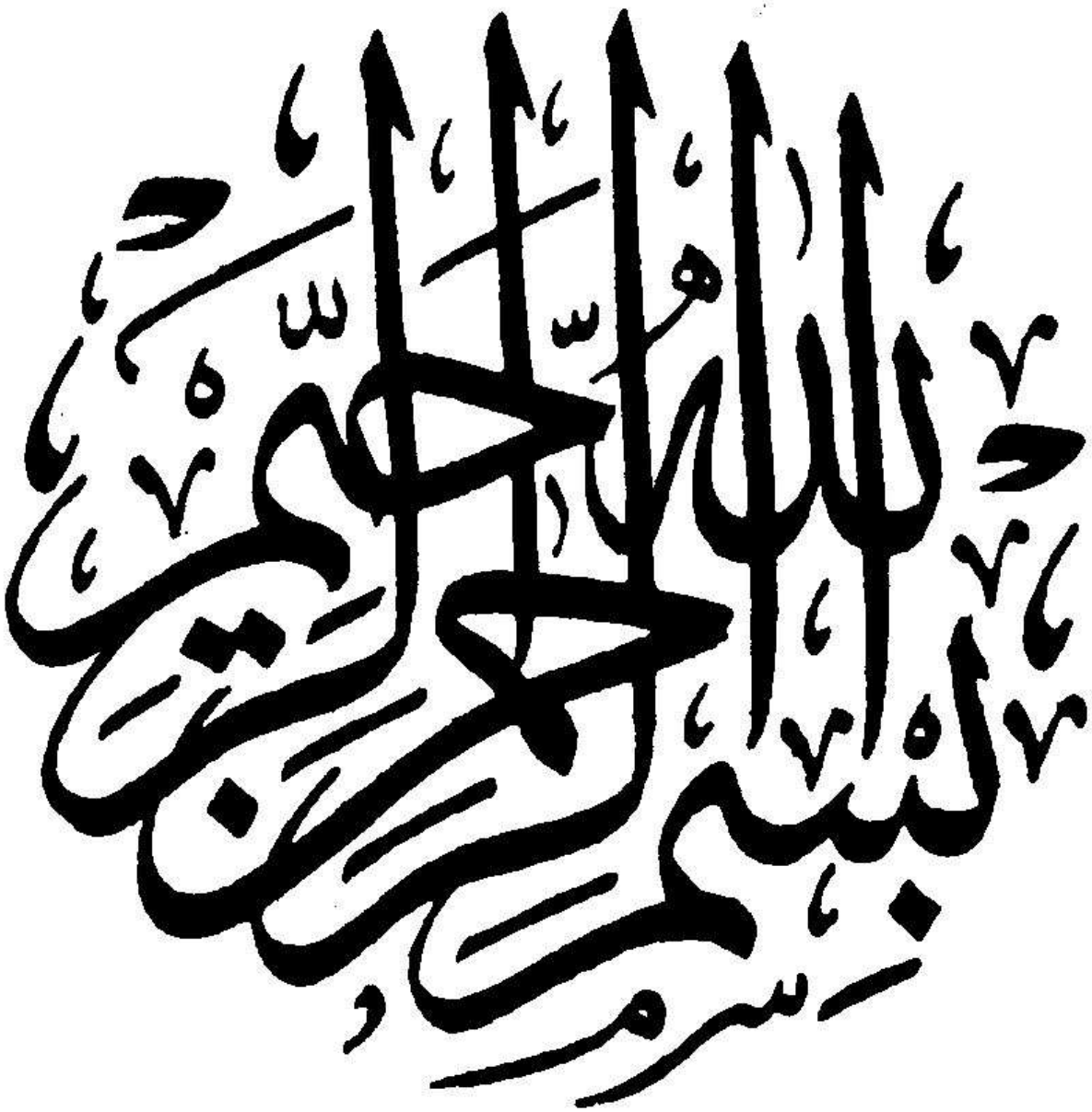
–زوبيري عبد الحليم

إشراف الأستاذ:

الدكتور: كيحول بوزيد

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
الاخضري فتيحة	أستاذ	جامعة غرداية	رئيسا
كيحول بوزيد	أستاذ	جامعة غرداية	مشرفا ومقررا
لغلام عزوز	أستاذ	جامعة غرداية	عضواً مناقشا

الموسم الجامعي :1446/1445 الموافق 2024 /2025


بسم الله الرحمن الرحيم

الإهـــــــــــــــــداء

إلى الوالدين الكريمين الذين سهروا وتعبوا

إلى العزيز الذي حملت اسمه فخرا رحمة الله على روحه الطاهرة

إلى الجسر الصاعد به الى الجنة

أمي الغالية

إلى كل من له فضل علينا حتى وصلنا إلى هنا

إلى كل أستاذ علمنا حرفا

إلى جميع الإخوة و الأحبة وزملاء العمل الذين اخذوا مساحة من قلبنا

نهدي لهم جميعا ثمرة هذا العمل المتواضع

شكر وتقدير

الحمد لله الذي أنار لنا باب العلم والمعرفة وأعاننا على أداء هذا الواجب ووفقنا في إنجاز هذا العمل.

نتوجه بجزيل الشكر والامتنان إلى كل من ساعدنا من قريب أو بعيد على انجاز هذا العمل والى كل من أشعل شمعة في دروب علمنا إلى من وقف على المنابر وأعطى حصيلة فكر لينير دربنا ونخص بالشكر الدكتور كيحول بوزيد الذي لم يبخل علينا بتوجيهاته القيمة ومعاملته الطيبة جزاه الله عنا كل خير وله منا كل الاحترام والتقدير.

ولا يفوتنا أن نتقدم بخالص الشكر والامتنان لكل عائلاتنا من الوالدين والإخوة والأخوات كما لا ننسى الزملاء والأصدقاء

ملخص الدراسة

تسلّط هذه الدراسة الضوء على الجريمة الإلكترونية باعتبارها من أبرز التحديات القانونية في ظل التحول الرقمي المتسارع، حيث ترتكز على تحليل الإطار القانوني المنظم لهذا النوع المستحدث من الجرائم المعلوماتية في الجزائر، مع مقارنة تشريعية عربية ودولية. وقد اعتمدت الدراسة على تحليل معمق لعدد معتبر من النصوص القانونية، لاسيما القانون الجزائري رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إضافة إلى أحكام قانون العقوبات ذات الصلة، وبيّنت مدى تجاوب المنظومة القانونية الجزائرية مع التحديات التي تفرضها البيئة الرقمية وتوصّلت الدراسة إلى أن مواجهة الجريمة السيبرانية تستلزم آليات قانونية متطورة، وتعاونًا دوليًا موسعًا، مع ضرورة تكريس الحماية القانونية للمجتمع الرقمي عبر قوانين مرنة وشاملة تواكب التطور التكنولوجي المستمر.

الكلمات المفتاحية: الجريمة الإلكترونية، النصوص القانونية، القانون الجزائري.

Abstract :

This study highlights cybercrime as one of the most significant legal challenges facing the accelerating digital transformation. It analyzes the legal framework regulating this emerging type of cybercrime in Algeria, along with a comparative study of Arab and international legislation

The study relied on an in-depth analysis of a significant number of legal texts, particularly Algerian Law No. 09-04 on the prevention and combating of crimes related to information and communication technology, in addition to the relevant provisions of the Penal Code.

It demonstrated the extent to which the Algerian legal system is responsive to the challenges posed by the digital environment. The study concluded that combating cybercrime requires advanced legal mechanisms and extensive international cooperation, along with the need to establish legal protection for the digital community through flexible and comprehensive laws that keep pace with ongoing technological development.

Keywords: Cybercrime, Legal texts, Algerian law.

مقدمـــة

مقدمة:

في عصر يشهد تطورًا متسارعًا وغير مسبوق في مجال التكنولوجيا، أصبحت هذه الأخيرة جزءًا لا يتجزأ من حياة الإنسان اليومية، فقد غيرت أنماط التواصل، وأساليب العمل، وطرق الوصول إلى المعرفة، بل تجاوز تأثيرها إلى إعادة تشكيل البُنى الاقتصادية والاجتماعية والثقافية للدول والمجتمعات. ومع هذا التقدم التكنولوجي المذهل، ظهرت على الساحة تحديات جديدة تهدد أمن الأفراد والمؤسسات والدول، ومن أبرز هذه التحديات ما يُعرف بـ "**الجرائم الإلكترونية**"، وهي جرائم ترتكب عبر الوسائل التكنولوجية الحديثة، كالإنترنت، والهواتف الذكية، والشبكات الرقمية المختلفة.

تُعد الجرائم الإلكترونية ظاهرة عالمية متنامية ومعقدة، تختلف عن الجرائم التقليدية من حيث طبيعتها وأدواتها ومجال انتشارها، إذ أنها لا تعترف بالحدود الجغرافية أو القيود الزمانية، ما يجعل مكافحتها أكثر تعقيدًا. وقد تنوعت أشكال هذه الجرائم لتشمل اختراق الحسابات البنكية، والابتزاز الإلكتروني، والتجسس الصناعي، وسرقة الهوية، ونشر البرمجيات الخبيثة، والهجمات على البنية التحتية الرقمية، وغيرها من الممارسات التي تستغل الوسائل التكنولوجية لتحقيق أهداف إجرامية. والمقلق في هذا السياق أن الجريمة الإلكترونية لا تقتصر على الأفراد فحسب، بل تطال الشركات الكبرى والمؤسسات الحكومية، ما يهدد الأمن القومي والمجتمعي على حد سواء.

ومن هنا تطرح هذه الدراسة الإشكالية التالية:

إلى أي مدى ساهمت التكنولوجيا الحديثة في ارتكاب الجرائم الإلكترونية، وما هي السبل الفعالة لمكافحتها في ظل التحديات الأمنية والقانونية الراهنة؟

اعتمدنا في هذه الدراسة على المنهج الوصفي في تعريف الجريمة الالكترونية للتكنولوجيا الحديثة وايضا المنهج التحليلي القانوني من جانب بعض النصوص القانونية التي تنظم اهم العقوبات في الجريمة الالكترونية وسبل المكافحة.

وللإجابة على هذه الاشكالية ارتأينا الى تقسيم موضوع الدراسة الى فصلين، كل فصل ينقسم الى ثلاثة مباحث التي بدورها تنقسم الى اربع مطالب في كل مبحث.

يتعلق الفصل الاول ب"الاطار النظري للجرائم الالكترونية الي يشتمل بدوره على ثلاثة مباحث، المبحث الأول مفاهيم اساسية والمبحث الثاني حول "الاطر التشريعية الوطنية والدولية" آما المبحث الثالث فكان تحت عنوان "دوافع واساليب ارتكاب الجرائم الالكترونية".

اما الفصل الثاني للدراسة فهو بعنوان "سبل مكافحة الجرائم الالكترونية "والي قسمناه الى ثلاثة مباحث حيت تطرقنا في المبحث الاول الى "التدابير الوقائية والتقنية "اما المبحث الثاني فكان تحت عنوان "الاجراءات الجنائية والتحقيقية " لنتطرق في المبحث الثالث والاخير حول "التحديات المعاصرة والمقترحات التطويرية "

وختمنا هذه الدراسة بخاتمة عامة تطرقنا فيها لنتائج البحث وتوصياته.

أهمية الدراسة

يُعد موضوع الجرائم الإلكترونية من المواضيع ذات الحساسية المتزايدة في عصرنا الراهن، بالنظر إلى التوسع في استخدام الوسائل التكنولوجية في شتى المجالات، سواء على المستوى الفردي أو المؤسساتي. ومع تزايد الاعتماد على الفضاء الرقمي في تبادل المعلومات وتسيير العمليات، أصبحت المجتمعات أكثر عرضة لهجمات رقمية تهدد الأمن العام والخصوصية والسلامة الاقتصادية.

وتنبع أهمية هذه الدراسة من كونها تتناول جانبًا معقدًا ومتشابكًا من الظواهر الإجرامية المعاصرة، يتمثل في العلاقة بين التكنولوجيا الحديثة كأداة حضارية، وبين استغلالها كوسيلة لارتكاب الجرائم. إذ أن الكشف عن هذه العلاقة وتحليلها يساعد على فهم الأسس التقنية والاجتماعية التي تؤطر الجرائم الإلكترونية، وبالتالي يساهم في تقديم رؤى واقعية يمكن أن تُوظف في تحسين الاستراتيجيات الوقائية والتشريعية.

أهداف الدراسة

انطلاقًا من الطابع التحليلي والواقعي للدراسة، تهدف هذه المقاربة إلى الإحاطة الشاملة بمختلف جوانب موضوع الجرائم الإلكترونية، ليس فقط عبر عرض ملامحها العامة، بل من خلال تحليل عوامل

نشأتها، وتطور أدواتها، ومجالات تأثيرها، وسبل الحد منها. ومن ثمّ، فإن الدراسة تسعى إلى تحقيق مجموعة من الأهداف، نوجزها فيما يلي:

1. **تحليل العلاقة بين التقدم التكنولوجي وظهور أنماط جديدة من الجرائم الرقمية.**
2. **التعرف على أبرز أشكال الجرائم الإلكترونية المنتشرة في السياقات المعاصرة.**
3. **استكشاف الوسائل التقنية المستخدمة في تنفيذ هذه الجرائم، وكيفية تطورها.**
4. **تسليط الضوء على الإطار القانوني الوطني والدولي في التعامل مع الجريمة الإلكترونية.**
5. **اقتراح سبل عملية وفنية لمكافحة هذه الظاهرة، من خلال تعزيز الحماية الرقمية، والتكوين المتخصص، والتعاون المؤسساتي.**
6. **تنمية الوعي العام بمخاطر الاستخدام غير الآمن للتكنولوجيا.**

أسباب اختيار الموضوع

إن اختيار موضوع "دور التكنولوجيا الحديثة في ارتكاب الجرائم الإلكترونية وسبل مكافحتها" لم يكن اعتباريًا، بل جاء نتيجة لمجموعة من الأسباب الموضوعية والعلمية التي تعكس وعي الباحث بأهمية التطرق إلى هذا المجال في الظرف الراهن، ومن أبرز هذه الأسباب:

1. **الطابع المستجد والديناميكي للموضوع،** إذ تُعد الجريمة الإلكترونية من الظواهر التي لا تزال في طور التوسع والتعقيد، ما يجعل دراستها ضرورة علمية وأمنية.
2. **نقص المعالجة الأكاديمية المتخصصة،** خاصة في السياقات المحلية، رغم الانتشار الواسع للجرائم الإلكترونية، ما يستدعي تقديم إسهام بحثي جاد في هذا المجال.
3. **الدافع الشخصي المعرفي،** حيث يمثل الموضوع اهتمامًا خاصًا للباحث نظرًا لتقاطعاته مع مجالات متعددة كالقانون، والتكنولوجيا، والأمن، والمجتمع.
4. **الحاجة المجتمعية المتزايدة لفهم الظاهرة،** من أجل تحصين وتوعية الأفراد والمؤسسات من مخاطرها، وتقديم مقترحات واقعية للحد منها.
5. **الرغبة في دعم المجهودات الأكاديمية الوطنية والدولية،** من خلال إثراء الأدبيات المتعلقة بالجريمة الإلكترونية ومكافحتها.

الدراسات السابقة :

1 .دراسة الدكتور نسيم دردور: جرائم المعلوماتية على ضوء القانون الجزائري والمقارن

تناولت هذه الدراسة الإشكالية المتزايدة لجرائم المعلوماتية في ظل تسارع وتيرة التطورات التكنولوجية، وسعت إلى تحليل الإطار القانوني الجزائري المنظم لها مقارنة بالتشريعات الأجنبية. اعتمد الباحث على المنهج الوصفي والتحليل القانوني، متتبعًا نصوص القانون الوطني ذات الصلة، إلى جانب مقارنتها مع التشريعات المتقدمة في هذا المجال، وذلك بهدف تحديد أوجه النقص والفراغ القانوني الذي قد يسمح بمرور بعض الجرائم دون عقاب واضح.

وقد أظهرت الدراسة أن التشريع الجزائري ما يزال يفتقر إلى تغطية شاملة لبعض الأشكال الجديدة للجرائم الإلكترونية، مثل الجرائم التي تُرتكب عبر مواقع التواصل الاجتماعي والتي تستغل الثغرات التقنية والقانونية في النظام القانوني الحالي. كما بيّنت الدراسة أن هذا النقص في التجريم الصريح لبعض الأفعال أدى إلى اتساع هامش المناورة لدى الجناة الذين يستفيدون من تأخر المشرع في التحديث القانوني.

خلصت الدراسة إلى ضرورة إعادة النظر في المنظومة القانونية من خلال استحداث مواد جديدة تواكب جرائم العصر الرقمي، مع وضع تعريف موحد وشامل لجرائم المعلوماتية يُراعى فيه التطور المستمر في طرق وأساليب ارتكاب هذه الجرائم. كما أوصى الباحث بتعزيز التعاون الدولي القضائي وتكوين وحدات أمنية متخصصة في التحقيق في هذه الجرائم لتضييق الخناق على مرتكبيها.

2 .دراسة النقيب سعيداني نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري

ركزت هذه الدراسة على الجانب الإجرائي للجرائم الإلكترونية، حيث سعى الباحث إلى تحليل الكيفية التي تعتمدها الأجهزة الأمنية والقضائية في الجزائر لتتبع مرتكبي الجرائم المعلوماتية. ومن خلال المنهج الوصفي التحليلي، استعرض الباحث أدوات التحقيق التقليدية المعمول بها في القانون الجزائري، وقارنها بالوسائل المستحدثة والمعتمدة في بعض الدول المتقدمة مثل الاستنساخ الرقمي، والتحليل الجنائي الرقمي، والتتبع السيبراني.

كشفت الدراسة عن عدة نقاط ضعف تعيق فعالية التحقيقات، أهمها بطء تبني الأجهزة الأمنية للتكنولوجيا الحديثة في جمع الأدلة الرقمية، وضعف التكوين المتخصص، فضلاً عن محدودية التنسيق بين الجهات الأمنية والسلطة القضائية، مما يؤثر سلبًا على سرعة ودقة تعقب المجرمين.

أوصت الدراسة بضرورة إنشاء مراكز بيانات متخصصة تُعنى بحفظ وتحليل الأدلة الرقمية، بالإضافة إلى تطوير مهارات المحققين من خلال تكوينات متخصصة في علم الأدلة الرقمية. كما شددت على أهمية وضع تشريعات صريحة تنظم عملية جمع البيانات الرقمية بطريقة قانونية تُعزز من شرعية الأدلة أمام القضاء، وتُسهم في رفع جودة و نجاعة التحقيقات الإلكترونية.

3 .دراسة الدكتور صغير يوسف: الجريمة المرتكبة عبر الإنترنت

هدفت هذه الدراسة إلى تقديم فهم شامل لجرائم الإنترنت من خلال مقاربة وصفية تحليلية، تم فيها التطرق إلى مفاهيم الجريمة الإلكترونية وأشكالها المختلفة، مع تحليل حالات واقعية توضّح كيفية تنفيذ هذه الجرائم باستخدام أدوات تكنولوجية متطورة. كما أجرى الباحث مقابلات ميدانية مع بعض الخبراء الأمنيين والقانونيين لتقييم واقع التطبيق العملي للنصوص القانونية في هذا المجال.

كشفت النتائج عن وجود فجوة ملحوظة بين ما تنص عليه القوانين وبين الممارسات الفعلية لأجهزة الأمن، حيث تعاني الأخيرة من محدودية في الوسائل التقنية المتوفرة مقارنة بسرعة تطور أدوات الجريمة الإلكترونية. كما أن غياب الكوادر المتخصصة وتحديث النصوص القانونية يجعل من الصعب مجاراة طبيعة هذه الجرائم التي تتغير باستمرار.

خلصت الدراسة إلى ضرورة تحديث البنية التشريعية المحلية بما يضمن مسايرتها للتطور التكنولوجي السريع، وأوصى الباحث بإحداث وحدات متخصصة لتحسين القدرة على رصد وتحري الجرائم الإلكترونية، إلى جانب تعزيز التكوين والتدريب في المجال القانوني والتقني لمختلف الفاعلين في المجال الأمني والقضائي.

4 .دراسة الدكتور إي. سي. لونجينوس: التقنيات الناشئة والجريمة الإلكترونية

اهتمت هذه الدراسة بتقييم التهديدات السيبرانية الناجمة عن استخدام الذكاء الاصطناعي ومنصات التواصل الاجتماعي، مع التركيز على كيفية انتشار المعلومات المضللة واستغلالها لأغراض إجرامية. اعتمد الباحث على منهج مختلط جمع بين الاستبيانات الميدانية وتحليل أدبيات حديثة، مما أتاح له تصنيف أنواع الجرائم الإلكترونية والتعرف على أدواتها المستحدثة.

أظهرت النتائج أن الغالبية ترى في الجرائم الإلكترونية خطرًا يمتد أثره إلى المؤسسات العامة والخاصة، وليس فقط الأفراد. كما أن الأنظمة الرقمية المترابطة تخلق بيئة خصبة لانتقال الهجمات والتضليل بشكل سريع، مما يصعّب احتوائها باستخدام الوسائل التقليدية. وأكدت الدراسة على أن مواجهة هذا النوع من الجرائم لا يمكن أن يتم إلا من خلال نهج شامل يشمل تطوير التشريعات، وتكثيف حملات التوعية الرقمية، وتعزيز التعاون بين الجهات الأمنية وشركات التكنولوجيا.

انتهت الدراسة إلى ضرورة تبني بروتوكولات عمل مشتركة تستند إلى معايير دولية للحد من الانتشار السريع للمعلومات المضللة، إلى جانب تبني سياسات استباقية في مجال الأمن السيبراني تأخذ بعين الاعتبار الطبيعة الديناميكية للفضاء الرقمي.

❖ اولا: اوجه التشابه في الدراسات السابقة

-معظم الدراسات السابقة تشير الى ان التقدم التكنولوجي ساهم في توفير تقنيات جديدة اي انه كلما تطورت التكنولوجيا زادت فرص ارتكاب الجرائم الالكترونية مع تعقد الاساليب

-عدم نجاعة انظمة الحماية التقليدية لمواجهة الجرائم الالكترونية الحديثة مما يتطلب تحديث يتماشى مع التطور التقني

-اختلاف الجرائم الالكترونية وتعدد اشكالها(الاختراق الابتزاز الاحتيال الفيروسات)

-اهمية التوعية وهي من الحلول التي تساهم في القضاء على الجريمة الالكترونية

-توفر الانترنت وسهولة الوصول اليها ساهم في ارتكاب الجرائم حتى مع انعدام الخبرة الاجرامية

❖ ثانيا: أوجه الاختلاف في الدراسات السابقة

-الاختلاف في تعريف مفهوم الجريمة الالكترونية حيت التعريف الشامل هو كل استخدام غير مشروع للتكنولوجيا على عكس هناك دراسات تركز على انواع محددة مثل الاحتيال المالي او الاختراقات الامنية

-الاختلاف في ربط علاقة التكنولوجيا بالجريمة بحيث اغلب الدراسات رات ان التكنولوجيا سبب اول ورئيسي بينما هناك دراسات ترى ان الدافع الحقيقي يعود الى عوامل نفسية او اجتماعية او اقتصادية

-الاختلاف في تقدير حجم و ثاتير الجرائم الالكترونية

-اختلاف الجرائم الالكترونية بالنسبة للموقع الجغرافي بحيث في الدول المتقدمة مثلا يكون باستهداف البنية التحتية اما بالنسبة للدول النامية يكون عبر الاحتيال عبر مواقع التواصل والابتزاز

الفصل الأول

الإطار النظري للجرائم الإلكترونية

تمهيد :

شهد العالم في العقود الأخيرة ثورة تكنولوجية غير مسبوقة شملت مختلف مجالات الحياة، وكان من أبرز مظاهرها الانتشار الواسع لتكنولوجيا المعلومات والاتصال، التي أسهمت في تسهيل التواصل وتبادل المعلومات والمعاملات. غير أن هذه التطورات رافقها ظهور نوع جديد من التهديدات، تتمثّل في الجرائم الإلكترونية، التي أصبحت تشكّل تحديًا حقيقيًا للأمن الوطني والدولي على حد سواء. فقد باتت الفضاءات الرقمية ساحة مفتوحة لممارسات إجرامية تتسم بالتعقيد ولا محدودية الجغرافية، ما جعل مواجهة هذه الظاهرة تتطلب إعادة نظر شاملة في مفاهيم الجريمة التقليدية، وتكييف الأطر القانونية والأمنية لمجاراتها

المبحث الأول: مفاهيم الجرائم الالكترونية

إن الجرائم الإلكترونية ليست مجرد امتداد للجرائم التقليدية عبر وسائط رقمية، بل هي ظاهرة متمايزة في طبيعتها ووسائلها وأطرافها، إذ تعتمد على تقنيات متطورة وتستغل الثغرات القانونية والتقنية لتحقيق أهدافها، وهو ما يفرض دراسة دقيقة لمفاهيمها الأساسية، وتحديد ماهيتها وتمييزها عن المفاهيم المجاورة كالجريمة المعلوماتية أو الجريمة السيبرانية. كما أن الوقوف على خصائص هذه الجرائم وتصنيفاتها يُعد خطوة أساسية لفهم السياق القانوني والاجتماعي الذي تتحرك فيه، وبناء قاعدة صلبة لمناقشة سبل الوقاية والمكافحة لاحقًا.

في هذا المبحث، سيتم التطرق إلى أهم المفاهيم المرتبطة بالجرائم الإلكترونية، مع بيان خصائصها وأشكالها المختلفة، سعياً إلى بناء أرضية معرفية واضحة تؤسس لما سيأتي لاحقًا من تحليل قانوني وإجرائي لهذه الظاهر

المطلب الأول: تعريف التكنولوجيا الحديثة وأنماطها

الفرع الأول: مفهوم التكنولوجيا الحديثة

يرى محمد باشا أن التكنولوجيا الحديثة "تمثل تطبيقًا عمليًا للمعرفة العلمية في مختلف مجالات الحياة، من خلال استخدام الأدوات والآلات والأنظمة المتطورة لتحقيق نتائج ملموسة". وهذا التعريف يسلط الضوء على الجانب التطبيقي للتكنولوجيا، حيث يُنظر إليها كحلقة وصل بين العلم النظري واحتياجات الحياة الواقعية. من خلال هذا المفهوم، تصبح التكنولوجيا وسيلة لتحقيق التقدم وتحويل الأفكار النظرية إلى حلول عملية ملموسة[1].

يشير باشا إلى أن التكنولوجيا الحديثة لا تقتصر على المجال الصناعي أو التقني فقط، بل تمتد لتشمل الزراعة، والتعليم، والصحة، والإعلام، والإدارة، وغيرها من الميادين. فكلما تطورت المعرفة

[1]محمد باشا، مفهوم التكنولوجيا والتقنيات، دار النشر غير محددة، الطبعة الأولى، القاهرة، مصر، 2018، ص22.

العلمية، وُجدت الحاجة إلى ترجمتها إلى تطبيقات عملية تفيد الفرد والمجتمع. ويعني ذلك أن التكنولوجيا هي الحامل الحقيقي لتطور المجتمعات، لأنها تجعل العلم نافعًا وسهل الاستخدام[1].

وترى ضمراوي أن التكنولوجيا أصبحت ملازمة لكل تفاصيل الحياة اليومية، بدءًا من أبسط العمليات المنزلية، مثل الطبخ والتنظيف، ومرورًا بخدمات الاتصالات والنقل، ووصولًا إلى مجالات معقدة مثل الجراحة الطبية الدقيقة والتخطيط العمراني. فكل ما يستخدمه الإنسان اليوم لتحقيق راحته، يعتمد بدرجة كبيرة على تطور التكنولوجيا[2].

وتضيف ضمراوي أن التكنولوجيا تساهم أيضًا في تقليص الفجوة بين الطبقات الاجتماعية، حيث تتيح للجميع فرصًا متساوية في الوصول إلى المعلومات والخدمات، بشرط أن يتم تعميم استخدامها بشكل عادل. وهذا ما يعزز من قيم المساواة والعدالة الاجتماعية في ظل مجتمعات رقمية متقدمة[3].

كما يشير إلى أن التكنولوجيا لها تأثيرات متشعبة، تشمل المجال الصحي من خلال تطوير الأجهزة الطبية، والمجال البيئي من خلال ابتكار حلول صديقة للبيئة، والمجال الإداري من خلال الرقمنة والحوسبة. ولذلك، فإن التكنولوجيا الحديثة أصبحت ضرورة وليست ترفًا، وهي ركيزة أساسية في بناء مستقبل المجتمعات[4].

الفرع الثاني: أنماط التكنولوجيا الحديثة

اولا: تكنولوجيا المعلومات والاتصالات:(ICT)

تكنولوجيا المعلومات والاتصالات تعد من أبرز أنماط التكنولوجيا الحديثة التي دخلت في جميع جوانب الحياة البشرية. تشمل هذه التكنولوجيا الأدوات الرقمية التي تستخدم في معالجة المعلومات وتخزينها ونقلها. من أبرز هذه الأدوات الحواسيب، الإنترنت، الهواتف الذكية، والشبكات. فهي توفر وسائل تفاعلية تساهم في تسهيل التواصل وتبادل المعرفة بين الأفراد والمؤسسات.

[1] محمد باشا، المرجع نفسه ،ص 23

[2] محمد باشا ، المرجع السابق ص 25

[3] بانا ضمراوي، *تعريف التكنولوجيا* ، دار النشر غير محددة، الطبعة الأولى، 2017، ص10.

[4] عبده سمير ، *العرب والتكنولوجيا* ، دار الآفاق الجديدة، الطبعة الأولى، بيروت، لبنان، 1981، ص120.

يمكن اعتبار تكنولوجيا المعلومات والاتصالات بمثابة العمود الفقري للتحول الرقمي في المجتمع المعاصر، حيث إنها تمكن المؤسسات من تحسين أدائها وزيادة إنتاجيتها من خلال الاستفادة من البيانات وتحليلها. في الحياة اليومية، تساهم هذه التكنولوجيا في تسهيل الأعمال اليومية مثل التسوق عبر الإنترنت، التواصل عبر البريد الإلكتروني أو الرسائل النصية، وإجراء المحادثات الفيديوية، وحتى في التعليم عن بُعد[1].

ثانيا: التكنولوجيا الحيوية:(Biotechnology)

التكنولوجيا الحيوية هي واحدة من أهم فروع العلوم التطبيقية التي تستخدم الكائنات الحية أو أجزاء منها في تطوير منتجات أو عمليات تهدف إلى تحسين حياة الإنسان. تعتمد هذه التكنولوجيا بشكل أساسي على فهم الآليات البيولوجية والوراثية للكائنات الحية، واستخدام هذا الفهم في تطوير حلول عملية في مجالات عدة مثل الطب، الزراعة، والصناعة.

من أبرز التطبيقات التكنولوجية الحيوية هي الهندسة الوراثية، التي تُستخدم لتعديل جينات الكائنات الحية بهدف تحسين خصائصها أو إنتاج مواد جديدة مفيدة للبشر. على سبيل المثال، يمكن استخدام الهندسة الوراثية في إنتاج محاصيل زراعية مقاومة للأمراض أو تحمل ظروف بيئية قاسية، مما يسهم في تحسين الأمن الغذائي العالمي[2].

ثالثا: تكنولوجيا النانو:(Nanotechnology)

تكنولوجيا النانو هي مجال علمي يهتم بتصميم وتصنيع مواد وأجهزة على مقياس النانومتر، وهو مقياس يعادل جزءًا من مليار جزء من المتر. وتُستخدم هذه التكنولوجيا في العديد من المجالات مثل الطب، الإلكترونيات، والطاقة، حيث تسهم في تطوير تقنيات مبتكرة تسهم في تحسين حياة الإنسان.

[1] عبد الرحيم بشبر، *التكنولوجيا في عملية التعلم والتعليم*، دار الشروق للنشر، الطبعة الأولى، عمان، الأردن، 1988، ص113.
[2] حسين حمدي، *وسائل الاتصال والتكنولوجيا في التعليم*، دار القلم، الطبعة الأولى، الكويت، 1994، ص46.

أما في قطاع الطاقة، فإن تكنولوجيا النانو تساهم في تحسين كفاءة الخلايا الشمسية، من خلال زيادة قدرتها على امتصاص الضوء وتحويله إلى طاقة. كما تساهم في تطوير بطاريات وأجهزة تخزين طاقة أكثر كفاءة، مما يسهم في تحقيق استدامة الطاقة والحد من الاعتماد على الوقود الأحفوري[1].

رابعا: الذكاء الاصطناعي:(Artificial Intelligence)

الذكاء الاصطناعي هو مجال من مجالات علوم الكمبيوتر يهدف إلى تطوير أنظمة قادرة على أداء مهام تتطلب ذكاءً بشريًا، مثل التعلم، التحليل، واتخاذ القرار. يُستخدم الذكاء الاصطناعي اليوم في العديد من المجالات، بما في ذلك الطب، المالية، النقل، والتسويق.

في الطب، تُستخدم أنظمة الذكاء الاصطناعي لتشخيص الأمراض وتحليل الصور الطبية بطريقة دقيقة وسريعة، مما يساعد الأطباء في تقديم العلاج المناسب بشكل أكثر فعالية. كما تُستخدم هذه الأنظمة في تطوير الروبوتات الجراحية التي تساعد في إجراء العمليات المعقدة بشكل دقيق ودون الحاجة لتدخل بشري مباشر[2].

وفي مجالات أخرى، مثل التجارة الإلكترونية والخدمات المالية، يساهم الذكاء الاصطناعي في تحسين تجربة العملاء من خلال التوصيات الذكية، وتحليل سلوك المستهلكين، وإجراء عمليات التنبؤ بالأسواق المالية[3].

خامسا: تكنولوجيا الطاقة المتجددة:

تكنولوجيا الطاقة المتجددة تشمل التقنيات التي تُستخدم لتوليد الطاقة من مصادر طبيعية ومتجددة، مثل الشمس، الرياح، والمياه. الهدف من هذه التقنيات هو تقليل الاعتماد على الوقود الأحفوري وتقليل الانبعاثات الكربونية الملوثة للبيئة.

من أهم التطبيقات في هذا المجال هي محطات الطاقة الشمسية، التي تُستخدم لتوليد الكهرباء من أشعة الشمس. هذه التقنية تعتبر من أكثر الحلول فعالية في المناطق ذات الإضاءة الشمسية الوفيرة، حيث

[1]علي عبد العزيز، *تكنولوجيا التعليم في تطوير المواقف التعليمية*، مكتبة الفلاح للنشر والتوزيع، الطبعة الأولى، بيروت، لبنان، 1996، ص41.
[2]كارول فاجان، دان لونلي، *التخطيط للتقنية: دليل لقادة المدارس*، سكولاستيك إنك، الطبعة الأولى، نيويورك، الولايات المتحدة الأمريكية، 1995، ص8–9.
[3]علي عبد العزيز، *مرجع سابق*، ص53.

يمكنها توفير طاقة نظيفة ومستدامة. كما يتم استخدام تكنولوجيا الرياح لتوليد الكهرباء من الرياح، وهي مصدر آخر للطاقة النظيفة التي تساهم في تقليل التلوث البيئي[1].

المطلب الثاني : مفهوم الجريمة الإلكترونية وخصائصها

الفرع الاول: تعريف الجريمة الإلكترونية

تُعد الجريمة الإلكترونية من أخطر مظاهر الانحراف المعاصر، نظرًا لتطور وسائط ارتكابها وتعدد صورها وتجاوزها للحدود الجغرافية، فضلًا عن ارتباطها المباشر بالبنية التحتية المعلوماتية التي باتت تمثل العمود الفقري لمؤسسات الدولة والمجتمع.

إن طبيعة الجريمة الإلكترونية التقنية والمعقدة جعلت من الصعب وضع تعريف قانوني موحّد لها، ولذلك فإن أغلب التعريفات جاءت من خلال جهود فقهية أو قانونية تحليلية، تحاول الإحاطة بعناصر الجريمة الحديثة دون الإخلال بجوهرها.

فقد عرّفها **الدكتور خالد القاضي** بأنها:

" كل فعل أو امتناع عن فعل يتم باستخدام الحاسب الآلي أو شبكات الاتصال بهدف التعدي على الأموال أو الأفراد أو المؤسسات، ويشكل انتهاكًا لنصوص قانونية[2]."

أما **الدكتور عبد المجيد محمد** فقد ركز في تعريفه على البعد السلوكي والأهداف الإجرامية، معرفًا الجريمة الإلكترونية بأنها:

" سلوك غير مشروع يقوم به الجاني عبر الوسائل الإلكترونية الحديثة، مثل الإنترنت أو الحواسيب، بهدف تحقيق مكاسب غير قانونية، أو إلحاق ضرر بالغير ماديًا أو معنويًا[3]."

أما **الباحثة نهى شكري** فقد ركزت على الأثر الناتج عن الجريمة الرقمية، معرفةً إياها بأنها:

---

[1] علي عبد العزيز، *مرجع سابق*، ص59.

[2] خالد القاضي، الجرائم الإلكترونية – المفهوم وسبل المواجهة، دار الفكر الجامعي، الطبعة الثانية، الإسكندرية، مصر، 2016، ص45.

[3] عبد المجيد محمد، الجرائم الإلكترونية والبيانات الرقمية، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، مصر، 2018، ص32.

"أي استخدام غير قانوني لوسائل تكنولوجيا المعلومات يؤثر سلبًا على المصالح الفردية أو الجماعية المحمية قانونًا، سواء تعلق ذلك بالمعلومات أو المعاملات أو الخصوصية أو الأمن العام[1]."

ويضيف **الدكتور عبد الله العوضي** عنصرًا بالغ الأهمية، يتمثل في توسع دائرة الاستهداف، مؤكدًا أن الجريمة الإلكترونية لا تستهدف الأفراد فحسب، بل قد تمس الكيانات السياسية والاقتصادية، مهددةً الأمن العام للدول[2]

الفرع الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بجملة من الخصائص التي تميزها عن الجرائم الكلاسيكية، وتجعل من مكافحتها وتحديد مرتكبيها مهمة معقدة تتطلب أدوات قانونية وفنية متقدمة:

اولا: الطابع غير المادي

على خلاف الجرائم التقليدية التي تترك آثارًا فيزيائية كأدوات الجريمة أو الجثث أو الأضرار الملموسة، فإن الجريمة الإلكترونية تُرتكب في بيئة رقمية مجردة يصعب لمس آثارها، ما يضعف من وسائل الإثبات ويعقّد إجراءات التحقيق. كما يشير إلى ذلك **الدكتور محمد الفايد** بقوله:

"إن اختفاء الآثار المادية للجريمة يضعف من قوة الإثبات ويزيد من التحديات القانونية في ملاحقة الجناة .[3]."

ثانيا: الامتداد عبر الحدود

الطبيعة العالمية للإنترنت تجعل من السهل ارتكاب الجريمة من دولة أخرى، ما يطرح إشكاليات قانونية في تحديد الاختصاص القضائي وسرعة التعاون الدولي. فقد تتم الجريمة في ظرف ثوانٍ بين عدة دول دون أن تترك أدلة فيزيائية[4]

[1] نهى شكري، الأمن السيبراني ومكافحة الجرائم الإلكترونية، دار الكتاب الحديث، الطبعة الأولى، القاهرة، مصر، 2019، ص19.
[2] عبد الله العوضي، الجريمة الإلكترونية: تحديات الواقع والمستقبل، دار المطبوعات الجامعية، الطبعة الأولى، بيروت، لبنان، 2020، ص61.
[3] محمد الفايد، الجرائم الرقمية في التشريع الجزائري، دار الخلدونية، الطبعة الأولى، الجزائر، 2021، ص98.
[4] أحمد عماد الدين، الجرائم العابرة للحدود في الفضاء الإلكتروني، دار الفكر، الطبعة الثانية، دمشق، سوريا، 2020، ص72.

ثالثا: سرعة التنفيذ : أغلب الجرائم الإلكترونية تُرتكب في لحظات، حيث يمكن اختراق حساب مصرفي أو تسريب بيانات أو تدمير نظم تشغيل خلال وقت وجيز. هذه السرعة تفوق قدرات أجهزة الأمن التقليدية، وتفرض أنظمة رقابة واستجابة فورية[1].

رابعا: تعدد الأشكال والأنماط

تأخذ الجريمة الإلكترونية صورًا متنوعة يصعب حصرها، مثل: الاحتيال المالي، سرقة الهوية، التشهير، التحرش الإلكتروني، اختراق الأنظمة، سرقة البيانات، وغيرها. كما أنها تتطور بتطور البرمجيات والخوارزميات[2].

خامسا: صعوبة التتبع

يتم ارتكاب الجرائم الرقمية باستخدام وسائل تعمية مثل الشبكات الخاصة الافتراضية (VPN) أو أدوات التخفي في الشبكة المظلمة، مما يجعل تحديد موقع وهوية الجاني مسألة تقنية وقانونية بالغة الصعوبة.

سادسا: الاحتياج إلى خبرات فنية متقدمة

تستوجب التحقيقات في الجرائم الإلكترونية معرفة معمقة بلغات البرمجة، تحليل الأدلة الرقمية، علوم البيانات، التشفير، الأمن السيبراني، ما يفرض على الدول تدريب فرق مختصة ورفدها بالتقنيات الحديثة.

سابعا: التهديد المزدوج: فردي ومجتمعي

لا تنحصر خطورة هذه الجرائم في الأفراد المتضررين، بل تتعدى لتشمل أنظمة حساسة كالمؤسسات المصرفية، القطاعات الصحية، البنى التحتية الحيوية، ما يرفع من مستوى الخطورة إلى تهديد شامل للأمن القومي[3].

[1] فاطمة الزهراء السالمي، الجريمة الإلكترونية في التشريع المقارن، دار الأكاديميون، الطبعة الأولى، عمان، الأردن، 2020، ص134.
[2] زياد حمود، تقنيات التشفير والأمن السيبراني، دار ابن خلدون، الطبعة الأولى، تونس، 2022، ص147.
[3] هشام مراد، الأمن الرقمي في ظل التهديدات الإلكترونية، دار الرشاد الحديثة، الطبعة الأولى، المغرب، 2022، ص57.

المطلب الثالث: التطور التاريخي للجرائم الإلكترونية

يُعد التطور التاريخي للجرائم الإلكترونية مرآة عاكسة لمسار تطور التكنولوجيا نفسها، فمنذ اللحظات الأولى التي ارتبط فيها الإنسان بالآلة الرقمية، بدأت تبرز محاولات استخدام هذه الأدوات لأغراض غير مشروعة. ومع تحول المجتمع من الاقتصاد التقليدي إلى الاقتصاد الرقمي، تغيرت طبيعة الجريمة، وتوسعت رقعتها، حتى أصبحت الجرائم الإلكترونية أحد أهم التهديدات العالمية اليوم، يتجاوز خطرها حدود الدول ويطال البنى التحتية الحيوية، والمؤسسات المالية، والأمن المجتمعي، وحتى السيادة الوطنية.

الفرع الاول: المرحلة الأولى

البدايات (من الستينيات إلى نهاية السبعينيات (في هذه المرحلة، بدأ مفهوم الجريمة الإلكترونية بالتشكل على نحو بسيط وغير منظم، متأثرًا بالتطور التكنولوجي المحدود آنذاك. فمع استخدام الحواسيب الكبيرة في المؤسسات الحكومية والبحثية في الولايات المتحدة وأوروبا، بدأ بعض الأفراد في استكشاف تلك الأنظمة بهدف اختبار القدرات الفنية دون نية إجرامية بالضرورة[1].

يُشير المؤرخون إلى أن بعض المهندسين في شركات مثل IBM كانوا يستخدمون معرفتهم لاختراق الأنظمة الداخلية، ليس بدافع السرقة أو التخريب، بل لاستعراض المهارات أو تسهيل أعمالهم. ومع ذلك، فإن أول جريمة إلكترونية موثقة تعود إلى سنة 1969، حيث قام مهندس بتحويل مبالغ مالية بسيطة من نظام الرواتب إلى حسابه الشخصي دون أن يُكتشف لفترة من الزمن[2].

الفرع الثاني: المرحلة الثانية

ظهور الفيروسات (الثمانينيات (شهدت الثمانينيات ولادة الجرائم الإلكترونية بمعناها الواضح، مع ظهور أول فيروس إلكتروني معروف باسم Brainعام 1986، والذي برمجه شقيقان من باكستان بدافع ما وصفاه بـ"الرد على القرصنة"، إلا أن تأثيره تخطى النية الأصلية ليؤسس لمرحلة جديدة من الجريمة الرقمية[3].

---

[1]أحمد عبده، *الجرائم الإلكترونية بين الواقع والتحديات*، دار الفجر للنشر والتوزيع، الطبعة الأولى، القاهرة، مصر، 2019، ص44.
[2]سفيان دربال، *الجرائم السيبرانية: قراءة قانونية ومعلوماتية*، دار الهدى، الطبعة الثانية، الجزائر، 2021، ص62.
[3]كمال راجي، *التعاون الدولي في مكافحة الجريمة المعلوماتية*، دار الكتب القانونية، الطبعة الأولى، بيروت، لبنان، 2020، ص83.

كما ظهرت خلال هذه المرحلة أولى الحالات التي لفتت انتباه السلطات، منها اختراق شبكة ARPANET(النواة التي تطورت لاحقًا إلى الإنترنت) مما أثار مخاوف حول الأمن القومي الأمريكي، ودفع إلى تأسيس أول وحدات مختصة بالأمن السيبراني في الوكالات الفيدرالية[1].

الفرع الثالث: المرحلة الثالثة – عصر الإنترنت وانتشار التجارة الإلكترونية (التسعينيات (تعتبر هذه المرحلة واحدة من أهم التحولات في تاريخ الجريمة الإلكترونية، فقد انتشر الإنترنت بسرعة، وأصبح في متناول الأفراد والمؤسسات، وظهرت الحواسيب الشخصية في كل بيت ومكتب، مما أدى إلى انفتاح العالم الرقمي على الملايين من المستخدمين.

في هذا السياق، بدأت الجرائم الإلكترونية تأخذ طابعًا اقتصاديًا بحتًا، إذ ظهرت عمليات الاحتيال عبر البريد الإلكتروني، وسرقة بيانات بطاقات الائتمان، وانتحال الهوية الرقمية. كما استُخدمت الصفحات المزيفة للإيقاع بالمستخدمين وسرقة معلوماتهم الشخصية والمالية[2].

الفرع الرابع : المرحلة الرابعة – العصر الرقمي المتقدم (2000–2010)دخلت الجريمة الإلكترونية في هذه المرحلة مستوىً أكثر تقدمًا، من حيث الأدوات والأساليب والتأثير. فقد أصبح الإنترنت جزءًا لا يتجزأ من البنية التحتية للدول، ودخلت الشركات الكبرى في سباق رقمي يتطلب حماية معلوماتها بكل الوسائل.

ظهرت أساليب جديدة مثل التصيد الاحتيالي، والهندسة الاجتماعية، وهي تقنيات تقوم على استغلال العنصر البشري بدلًا من الثغرات التقنية. فأصبح بإمكان المخترق أن يخدع الموظف ليحصل على كلمة المرور.

دون الحاجة إلى اختراق النظام مباشرة[3].

بدأ الحديث في هذه المرحلة عن الأمن السيبراني كجزء من الأمن القومي، وأنشأت الدول وحدات متخصصة، وأصبحت الاستثمارات في الحماية الرقمية تتجاوز مليارات الدولارات سنويًا[4].

---

[1]حسن الطيب، *الأمن السيبراني ومخاطر الفضاء الرقمي*، دار المسيرة، الطبعة الأولى، عمان، الأردن، 2021، ص104.
[2]ليلى محمود، *الجريمة الإلكترونية والذكاء الاصطناعي*، دار الكتاب الحديث، الطبعة الأولى، القاهرة، مصر، 2023، ص141.
[3]عادل عبد الله، *الجريمة الإلكترونية وأمن المعلومات في التشريعات العربية*، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، مصر، 2020، ص77.
[4]ناصر العزاوي، التحقيق في الجرائم المعلوماتية: أصوله وإجراءاته، *دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، الأردن، 2021، ص99.*

الفرع الخامس: المرحلة الخامسة – الجرائم الإلكترونية المعقدة (2010 – إلى اليوم (في العقد الأخير، دخلت الجريمة الإلكترونية مرحلة غير مسبوقة من التعقيد والتنظيم. لم تعد هذه الجرائم تنفذها مجموعات صغيرة أو أفراد فقط، بل باتت بعض الدول تنشئ جيوشًا رقمية لأغراض التجسس، والتخريب، والتأثير السياسي.

كما كشفت الانتخابات الأمريكية لعام 2016 حجم الخطر الذي تشكله القرصنة المعلوماتية في التأثير على الديمقراطية، بعد اتهام روسيا بشن هجمات على البريد الإلكتروني للحزب الديمقراطي، ونشر معلومات مسيئة للتأثير على الناخبين[1].

ومع انتشار الذكاء الاصطناعي، وتقنيات التعلم الآلي، وإنترنت الأشياء، أصبحت الهجمات أكثر تعقيدًا، واستهدافًا، وذات طبيعة هجومية ودفاعية في آن واحد.

المطلب الرابع: تصنيف الجرائم الإلكترونية حسب الأساليب والأهداف

شهدت الجرائم الإلكترونية تطورًا متسارعًا من حيث الكم والنوع خلال العقود الأخيرة، متأثرة بالثورة الرقمية والتحولات العميقة في بنية المجتمع ألمعلوماتي. ولم تعد هذه الجرائم مقتصرة على محاولات بدائية للاختراق أو سرقة معلومات بسيطة، بل تحوّلت إلى أنماط إجرامية ممنهجة ومعقدة تشارك فيها أحيانًا جهات دولية أو منظمات عابرة للحدود. ويمثّل تصنيف الجرائم الإلكترونية خطوة أساسية لفهم طبيعتها وتحديد الإطار القانوني الأنسب لمواجهتها، خاصة مع ما تطرحه من تحديات جديدة على مستوى الإثبات، والاختصاص القضائي، والتعاون الدولي.

الفرع الاول : التصنيف حسب الأساليب التقنية

يمكن القول إن الوسائل والأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية ترتبط بشكل وثيق بالتطورات التقنية المتلاحقة. فكلما ظهرت تقنية جديدة، ظهرت بالمقابل محاولات لاستغلالها إجراميًا. من هنا، تتعدد الأدوات والأساليب التي يعتمدها المجرمون السيبرانيون، بدءًا من عمليات الاختراق التقليدية ووصولًا إلى تقنيات متقدمة تستخدم الذكاء الاصطناعي والخوارزميات المعقدة. ويُعد **الاختراق**

[1] *عماد الدين مصطفى*، الجرائم الإلكترونية في ظل القانون الجنائي المغربي والمقارن، *مطبعة النجاح الجديدة، الطبعة الأولى، الدار البيضاء، المغرب، 2022، ص55.*

(Hacking)أكثر الأساليب التقنية شيوعًا، ويتم من خلال الدخول غير المشروع إلى الأنظمة الرقمية بغرض الاطلاع أو التلاعب أو التدمير أو حتى الاستيلاء على البيانات. هذه العمليات قد تستهدف أفرادًا، شركات، أو حتى مؤسسات حكومية. ويعتمد الهاكر عادة على ثغرات في البرمجيات، أو ضعف في التكوين الأمني، أو حتى كلمات مرور سهلة. وفي كثير من الأحيان، يترافق الاختراق مع زراعة برامج تجسس (Spyware) أو برمجيات خبيثة (Malware) تكون بمثابة أدوات لمراقبة النظام أو تعطيله لاحقًا.

وتأتي **البرمجيات الخبيثة** بأنواعها المختلفة في صلب النشاط الإجرامي الإلكتروني؛ إذ تشمل فيروسات قادرة على إتلاف الملفات، أو ديدان (Worms) تنتشر تلقائيًا داخل الشبكة، أو أحصنة طروادة (Trojans)التي تبدو برامج مفيدة لكنها تحتوي على برامج خفية مدمرة، أو برامج الفدية (Ransomware)التي تقوم بتشفير بيانات المستخدم والمطالبة بفدية مقابل فك التشفير. وتشير التقارير الأمنية الحديثة إلى أن هجمات الفدية قد أصبحت من أكثر الأشكال ربحًا للجريمة الإلكترونية[1].

الفرع الثاني : التصنيف حسب الأهداف

لا يقل تصنيف الجرائم الإلكترونية حسب أهداف مرتكبيها أهمية عن تصنيفها وفق الأساليب التقنية، إذ يسمح بفهم النوايا الكامنة وراء الهجوم، وتحديد مدى خطورته وأبعاده الاجتماعية والاقتصادية وحتى السياسية. ففي السياق المالي، تتصدر **الغايات الاقتصادية والمالية** قائمة الدوافع الإجرامية، وتشمل مجموعة واسعة من الأفعال مثل: سرقة أرقام بطاقات الائتمان، القرصنة المصرفية، الاحتيال عبر الإنترنت، الاستيلاء على حسابات مصرفية، اختراق حسابات تداول العملات الرقمية، وتوزيع برامج الفدية. هذه الأنشطة عادة ما تكون مدفوعة بالجشع المالي، وقد تشترك فيها شبكات دولية إجرامية تعمل بطريقة منظمة. والأخطر أن هذه الشبكات تستغل السوق السوداء الرقمية لتصريف المسروقات، عبر ما يُعرف بالـ"دارك ويب[2]."

هناك أيضًا فئة من الجرائم ترتكب بدافع **الانتقام أو الدوافع الشخصية** .ففي بعض الحالات، يقوم موظف سابق أو زميل ساخط أو حتى شريك سابق باختراق حسابات أو أنظمة شخصية أو مهنية بهدف

[1]نوال الشيباني، الفضاء السيبراني والتحولات الإجرامية، دار أسامة للنشر، الطبعة الأولى، الجزائر، 2019، ص67
[2]سلوى عواد، *الجرائم الإلكترونية ومواجهة التشريعات العربية لها*، دار النهضة العربية، الطبعة الأولى، بيروت، لبنان، 2018، ص95.

الإضرار بالضحية. وتتراوح هذه الأفعال بين التشهير، تسريب البيانات، تخريب الملفات، أو حتى ابتزاز الضحية بمعلومات خاصة. وتشير الأبحاث إلى أن هذه الحالات، وإن بدت فردية، إلا أن آثارها قد تكون مدمرة نفسيًا ومهنيًا .[1].

الفرع الثالث: التصنيف من وجهة نظر قانونية

تبنّت العديد من التشريعات الوطنية والعربية تصنيفات قانونية واضحة للجرائم الإلكترونية، تساعد في تحديد الركن المادي والمعنوي للجريمة، وتسهّل توجيه التهم ومباشرة الإجراءات القضائية. وعمومًا، يمكن تقسيم الجرائم الإلكترونية إلى ثلاث فئات رئيسية من حيث طبيعة الاعتداء القانوني:

اولا: جرائم ضد الأفراد:وتشمل كل فعل إلكتروني يمس بحياة الأشخاص، سمعتهم، أو حرياتهم الخاصة، مثل: الابتزاز الإلكتروني، التشهير عبر الإنترنت، التحرش الرقمي، سرقة الهوية الإلكترونية، أو استغلال الأطفال عبر الإنترنت. وقد اعترف المشرع الجزائري بخطورة هذه الجرائم، فخصص لها نصوصًا واضحة في قانون العقوبات وكذلك في قانون 09-04 المتعلق بالجرائم الإلكترونية[2].

ثانيا: جرائم ضد الممتلكات:وتشمل كل هجوم إلكتروني يهدف إلى التعدي على الأموال المنقولة أو غير المنقولة أو البيانات الرقمية التي لها قيمة اقتصادية. من أبرز الأمثلة: الاحتيال المالي، سرقة البطاقات المصرفية، التلاعب في المعاملات الإلكترونية، والتخريب المعلوماتي الذي يؤدي إلى خسائر مادية.

ثالثا:جرائم ضد الدولة:وهي الأكثر حساسية، وتشمل محاولات اختراق أنظمة الدولة، التجسس على مؤسسات حساسة، نشر أخبار كاذبة تخلّ بالأمن العام، أو تعطيل البنى التحتية الحيوية كالماء، الكهرباء، المواصلات، أو حتى نظم التصويت الإلكتروني. ويدخل في هذا الإطار أيضًا الإرهاب السيبراني الذي يستهدف أمن الدولة ومواطنيها[3].

الفرع الرابع: تصنيفات أخرى معاصرة

[1]فؤاد منصور، *الجريمة الإلكترونية وتحديات التشريع الجزائي المعاصر*، دار الثقافة للنشر، الطبعة الأولى، عمان، الأردن، 2021، ص106.
[2]عماد حسين، *مرجع سابق*، ص121.
[3]عماد حسين، *مرجع سابق*، ص124.

مع تطور التكنولوجيا الرقمية وظهور تقنيات غير مسبوقة مثل الذكاء الاصطناعي، البلوك تشين، الواقع الافتراضي، والميتافيرس، بدأت تظهر تصنيفات جديدة للجرائم الإلكترونية تتجاوز التصنيفات التقليدية. من بين هذه التصنيفات[1]:

- **الجرائم السيبرانية المعتمدة على الذكاء الاصطناعي:**حيث يتم استخدام برامج ذكية قادرة على التعلم والتفاعل مع الأنظمة لاختراقها أو التلاعب بها دون تدخل بشري مباشر. وتشكل هذه الجرائم تحديًا كبيرًا نظرًا لقدرتها على التطور الذاتي والتخفي.
- **الجرائم المعتمدة على العملات الرقمية:**مثل البيتكوين وغيرها من العملات المشفرة، والتي تُستخدم لتبييض الأموال، تمويل الأنشطة غير المشروعة، أو تنفيذ عمليات احتيال مالي يصعب تتبعها نظرًا لطبيعة المعاملات غير المركزية.

المبحث الثاني: الأطر التشريعية الوطنية والدولية لمكافحة الجرائم الالكترونية

إن التطور السريع الذي شهدته تكنولوجيا المعلومات والاتصال خلال العقود الأخيرة قد ساهم في إيجاد بيئة رقمية جديدة غيّرت من أنماط الحياة البشرية، إلا أن هذا التحول الرقمي صاحبه وجهٌ مظلم تمثل في تصاعد الجرائم الإلكترونية وتنوعها، وهو ما شكّل تحديًا كبيرًا أمام الأنظمة القانونية على المستوى الوطني والدولي. فقد أصبحت الجريمة الإلكترونية عابرة للحدود، لا تعترف بالجغرافيا أو السيادة، وتُرتكب في بيئة افتراضية تفتقر إلى القواعد القانونية المستقرة، مما أوجد فراغًا تشريعيًا كبيرًا خصوصًا في الدول النامية، وأدى إلى الحاجة الملحة لتأطيرها قانونيًا ضمن نصوص واضحة وصريحة. [2].

المطلب الأول: المعاهدات والاتفاقيات الدولية في مكافحة الجرائم الإلكترونية

عدّ الجرائم الإلكترونية من أبرز التحديات التي تواجه الأمن القانوني والرقمي على المستوى العالمي، نظرًا لطبيعتها العابرة للحدود، وسرعة تطورها، وتعدد أشكالها وأساليبها. لقد ولّدت الثورة التكنولوجية واقعًا جديدًا بات فيه من السهل ارتكاب الجريمة دون الحاجة إلى الحضور الجسدي في مسرح الجريمة، مما أفرز إشكاليات قانونية دولية معقدة، أبرزها مسألة الاختصاص القضائي، وطرق الإثبات، وآليات الملاحقة، والتعاون الدولي في تنفيذ الأحكام. في هذا السياق، لم تعد التشريعات الوطنية وحدها قادرة على

[1]فؤاد منصور، مرجع سابق، ص110
[2]كمال راجي، التعاون الدولي في مكافحة الجريمة المعلوماتية، دار الكتب القانونية، الطبعة الأولى، بيروت، لبنان، 2020، ص110

التصدي لهذا النوع من الجرائم المتطورة، حيث يمكن للمجرم أن ينفذ جريمته من دولة معينة، بينما تقع آثارها في دولة أخرى، وهو ما يعقّد من مهام ملاحقته ومحاسبته.

الفرع الاول: اتفاقية بودابست لمكافحة الجريمة الإلكترونية (2001)

تُعد اتفاقية بودابست من أهم الاتفاقيات الدولية في ميدان مكافحة الجرائم الإلكترونية، بل يمكن اعتبارها المرجع القانوني الأول والأكثر شمولًا في هذا السياق. تم توقيع الاتفاقية سنة 2001 ودخلت حيّز التنفيذ سنة 2004، وقد وُضعت تحت إشراف مجلس أوروبا لكنها فُتحت للتوقيع أمام الدول من خارج أوروبا، وهو ما منحها بُعدًا دوليًا. تهدف الاتفاقية إلى توحيد التشريعات الجنائية المتعلقة بالجرائم المعلوماتية، وتوفير آليات فعّالة للتعاون الدولي في التحقيقات المرتبطة بالجرائم التي تُرتكب عبر الإنترنت، وتعزيز القدرات القانونية للدول لمجابهة هذه الأنماط الجديدة من الجريمة[1].

الفرع الثاني :البروتوكول الثاني المكمّل لاتفاقية بودابست (2022)

صدر البروتوكول الثاني كملحق تكميلي لاتفاقية بودابست لمكافحة الجريمة الإلكترونية، ويُعد تطويرًا محوريًا لمجال التعاون الدولي في التحقيقات الرقمية، خصوصًا في ظل تطورات التكنولوجيا الحديثة، كاستخدام السحابة الإلكترونية وخدمات التخزين عبر الإنترنت. تم تبني البروتوكول سنة 2022 بهدف معالجة التحديات الجديدة التي نشأت بفعل التغيرات السريعة في المجال السيبراني، وخصوصًا ما يتعلق بإمكانية الحصول على بيانات رقمية موجودة في بلد أجنبي بدون إجراءات قضائية معقدة قد تُبطئ التحقيقات الجنائية[2].

الفرع الثالث: اتفاقية الأمم المتحدة لمكافحة الجريمة الإلكترونية (2024)

تُعد اتفاقية الأمم المتحدة لمكافحة الجريمة الإلكترونية، المُعتمدة سنة 2024، نقلة نوعية في التعاون الدولي لمجابهة التحديات الرقمية، باعتبارها أول معاهدة عالمية تُنظم المكافحة الشاملة للجرائم السيبرانية من منظور الأمم المتحدة، بما يشمل كل الدول الأعضاء، بصرف النظر عن انتمائها القانوني أو الجغرافي. تم التفاوض حول هذه الاتفاقية بين أكثر من 150 دولة على مدار سنوات، وتهدف إلى وضع

[1]. كمال راجي ، المرجع السابق ، ص112

[2]صفاء نجم، *الجريمة المنظمة في ظل العولمة*، دار صفاء للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2018، ص77

إطار شامل وموحد يُعزز الأمن الرقمي الدولي، ويُمكّن الدول، خاصة النامية منها، من حماية فضائها السيبراني [1].

الاتفاقية الجديدة تختلف عن سابقتها (بودابست) بكونها أكثر شمولًا ومرونة، وتستجيب للتحديات المستجدة مثل الذكاء الاصطناعي، العملات الرقمية، والميتافيرس، كما تُركّز على بناء الثقة بين الدول، وحثّها على تقاسم الموارد والخبرات. إنها تمثل جهدًا جماعيًا غير مسبوق لتنظيم الفضاء الرقمي، وتُثبت أن العالم، رغم انقساماته السياسية، قادر على الاتفاق عندما يتعلق الأمر بمواجهة التهديدات الرقمية العابرة للحدود[2].

المطلب الثاني: القوانين والتشريعات الوطنية: النموذج الجزائري

مع التحول الرقمي الذي يشهده العالم المعاصر، ظهرت أشكال جديدة من الجريمة تُعرف بالجرائم الإلكترونية، وهي جرائم تتطلب تدخلًا قانونيًا خاصًا نظرًا لطبيعتها المعقدة والعابرة للحدود. في هذا السياق، لم تكن الجزائر بمنأى عن هذه الظاهرة، فقد عرفت تصاعدًا في وتيرة هذه الجرائم، مما دفع المشرع الجزائري إلى اعتماد جملة من القوانين والإصلاحات التشريعية التي تهدف إلى الوقاية من الجرائم الإلكترونية ومكافحتها، وتوفير الحماية القانونية للأفراد والمؤسسات. ويتجلى هذا المسعى من خلال إصدار قوانين خاصة، وتعديل بعض القوانين القائمة، مع محاولة تكييف المنظومة التشريعية الوطنية مع المعايير الدولية

الفرع الاول: القانون رقم 09-04 المؤرخ في 5 أغسطس 2009

يُعتبر القانون رقم 09-04 المؤرخ في 5 أغسطس 2009 حجر الأساس في السياسة الجنائية الجزائرية الخاصة بمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.[3]وقد تم سن هذا القانون في ظل تزايد استعمال تكنولوجيا المعلومات في مختلف مناحي الحياة، وازدياد حالات الاستغلال السيئ لهذه الوسائل لأغراض إجرامية. وقد سعى المشرع من خلال هذا القانون إلى وضع إطار قانوني واضح ومحدد يضمن الوقاية من هذه الجرائم ومكافحتها، مع احترام حقوق الإنسان والحريات الأساسية.

---

[1] فادي البشير، *مرجع سابق*، ص95

[2] فادي البشير، *مرجع سابق*، ص99

[3] نمديلي رحيمة، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة"، مجلة جيل الأبحاث القانونية المعمقة، العدد 12، 2014، ص 43

الفرع الثاني: تعديل قانون العقوبات الجزائري (المواد من 394 مكرر إلى 394 مكرر 7)

بموازاة صدور القانون الخاص بمكافحة الجرائم الإلكترونية، قام المشرع الجزائري بتعديل قانون العقوبات من خلال إدراج فصل جديد تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، تضمن جملة من المواد (394 مكرر إلى 394 مكرر 7) التي تهدف إلى تجريم الأفعال الإجرامية المرتبطة باستخدام الوسائل المعلوماتية.

الفرع الثالث: التحديات والآفاق المستقبلية

تحتاج الجزائر إلى وضع إستراتيجية وطنية متكاملة للأمن السيبراني، تشمل البعد القانوني والتقني والتوعوي، من خلال برامج وطنية للتثقيف الرقمي، ومناهج تعليمية موجهة للأطفال والشباب لتعزيز السلوك الآمن في الفضاء الإلكتروني[1].

المطلب الثالث: مؤسسات الدولة والهيئات المتخصصة في مكافحة الجرائم الإلكترونية

أمام التحولات الرقمية المتسارعة والانفجار المعلوماتي الكبير، بات الفضاء السيبراني ميدانًا مفتوحًا للتهديدات والجرائم المستحدثة التي تمس بأمن الأفراد، المؤسسات، بل وبأمن الدولة ككل.

الفرع الاول: الهيئات الأمنية المختصة

اولا: المركز الوطني للأدلة الرقمية(CNED)

يُعتبر المركز الوطني للأدلة الرقمية من أهم الهيئات المتخصصة التابعة للمديرية العامة للأمن الوطني، حيث أنشئ استجابة للحاجة المتزايدة إلى التعامل مع الأدلة الرقمية التي أصبحت حاضرة في أغلب الجرائم، لا سيما الإلكترونية منها. ويضم هذا المركز طاقمًا من الكفاءات الوطنية المختصة في مجالات الإعلام الآلي، الأمن المعلوماتي، الجنائيات الرقمية، وتحليل البيانات. ويُعنى المركز بجمع

[1] فضيلة عاقلي، "الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"، مجلة جيل الأبحاث القانونية المعمقة، العدد 12، 2014، ص 55.

وحفظ وتحليل الأدلة الرقمية التي يتم استخراجها من أجهزة الحاسوب، الهواتف المحمولة، وسائط التخزين، والكاميرات الرقمية، وغير ذلك من الوسائل التقنية[1]. .

ثانيا: فرقة مكافحة الجرائم المعلوماتية

الفرع الثاني: الهيئات الإدارية والمؤسسات الرسمية

أولا: الهيئة الوطنية لحماية المعطيات الشخصية

في ظل التوسع اللامحدود في جمع البيانات الرقمية وتداولها عبر مختلف المنصات الإلكترونية، برزت الحاجة إلى كيان مؤسساتي يسهر على حماية الحياة الخاصة للمواطنين من الاستغلال غير المشروع للمعطيات الشخصية. ومن هنا جاءت الهيئة الوطنية لحماية المعطيات الشخصية، التي تأسست بموجب القانون رقم 18-07 المؤرخ في 10 يونيو 2018. وتكمن مهمة الهيئة في مراقبة مدى التزام المؤسسات الحكومية والخاصة بالقواعد القانونية المتعلقة بحماية البيانات الشخصية، لاسيما في الفضاء الرقمي.[2]

ثانيا: مركز الاستجابة لطوارئ الحاسوب(CERT-Algeria)

يعد هذا المركز الذراع التقنية الأولى للدولة في مجال رصد الهجمات السيبرانية والاستجابة السريعة للحوادث الرقمية. ويعمل تحت إشراف مركز البحث في الإعلام العلمي والتقني(CERIST) ، ويقوم بمجموعة من المهام الحيوية مثل: التحليل الفني للبرمجيات الخبيثة، إصدار التحذيرات الأمنية، التنسيق بين الهيئات الحكومية في حال وقوع اختراقات، وتوفير دعم تقني للمؤسسات العمومية والخاصة.

وقد أصبح CERT-Algeria حلقة وصل مهمة بين الجزائر والهيئات الإقليمية والدولية المختصة بالأمن السيبراني مثل فريق "FIRST" العالمي، والمراكز التابعة للاتحاد الإفريقي، مما يعزز من جاهزية الدولة لمواجهة التهديدات العابرة للحدود[3].

[1] لعروسي كريمة، الجرائم الإلكترونية في الجزائر ودور الشرطة العلمية في مكافحتها، دار الخلدونية، ط1، الجزائر، 2021، ص 136.

[2] بوكاف عبد الكريم، حماية المعطيات الشخصية في القانون الجزائري، دار الفضيلة، الجزائر، 2019، ص 84.

[3] مزياني سفيان، الأمن السيبراني في الجزائر: تحديات وآفاق، دار هومة، ط1، الجزائر، 2020، ص 112.

ثالثا: الوكالة الوطنية للأمن السيبراني

تم إحداث الوكالة الوطنية للأمن السيبراني بموجب المرسوم التنفيذي رقم 20-408 المؤرخ في 26 ديسمبر 2020، لتكون الهيئة العليا المعنية بتنسيق وتنفيذ السياسة الوطنية للأمن السيبراني. ومن بين أهم إنجازات الوكالة: إعداد خارطة رقمية للتهديدات السيبرانية في الجزائر، إطلاق منصة رقمية للإبلاغ عن الحوادث الإلكترونية، والمشاركة في تدريبات ومحاكاة إلكترونية مع دول ومنظمات شريكة. ويُنتظر من الوكالة أن تلعب دورًا محوريًا في بناء ثقافة أمن رقمي مؤسسي وشعبي في آنٍ واحد[1].

المطلب الرابع: العقوبات المقترنة بالجرائم الإلكترونية ومدى فاعليتها

تُعد العقوبات الجنائية من الركائز الأساسية في النظام القانوني لأي دولة، إذ تمثل الوسيلة الفعلية لفرض احترام القواعد القانونية، وصيانة النظام العام، وحماية مصالح الأفراد والمجتمع. ولا شك أن تطور الجريمة الإلكترونية بوصفها أحد أخطر مظاهر الإجرام المعاصر، قد فرض تحديات كبيرة على المنظومات القانونية، لما تتسم به من خصائص فريدة تجعل مكافحتها أمرًا بالغ التعقيد. فهذه الجرائم تنفذ بوسائل تقنية متطورة يصعب أحيانًا اكتشافها.

الفرع الاول: العقوبات الجزائية في قانون العقوبات الجزائري

إن إدراج نصوص قانونية خاصة بمكافحة الجريمة الإلكترونية في قانون العقوبات يُعد خطوة متقدمة في سبيل توفير الحماية القانونية للمجتمع الرقمي، وقد تحقق ذلك من خلال الأمر رقم 06-23 المؤرخ في 20 ديسمبر 2006، الذي أدرج فصولًا جديدة ضمن القانون الجزائري، تُعنى بالتصدي للأفعال الماسة بنظم المعالجة الآلية للمعطيات. هذه النصوص شكلت إطارًا قانونيًا عامًا يجرم ويعاقب سلوكيات محددة مثل الدخول غير المشروع، وعرقلة النظام، وتزوير البيانات الإلكترونية، وهو ما يدل على وعي تشريعي بأهمية مكافحة هذه الجرائم[2].

أولا: جريمة الدخول غير المشروع

[1] زواوي مروان، الحوكمة الرقمية والأمن السيبراني في الجزائر، دار الكتاب الحديث، الجزائر، 2021، ص 147.

[2] جفال أحمد، **الجرائم الإلكترونية في القانون الجزائري**، دار الفجر، ط1، الجزائر، 2018، ص 92.

تعتبر هذه الجريمة من أبسط صور الجرائم الإلكترونية وأكثرها انتشارًا، إذ يتمثل سلوك الجاني في الولوج غير المصرح به إلى نظام معلوماتي، سواء بقصد الاستطلاع، أو لجمع معلومات، أو تمهيدًا لارتكاب جرائم أخرى. وقد نصت المادة 394 مكرر من قانون العقوبات على أنه: "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنتين (2) وبغرامة من 50.000 دج إلى 200.000 دج، كل من يدخل عمدًا، وبصفة غير مشروعة، إلى كل أو جزء من نظام للمعالجة الآلية للمعطيات". هذه المادة تُؤسس لمفهوم "الاختراق" غير المصرح به، حتى وإن لم يترتب عليه ضرر مادي أو معنوي، مما يعكس نية المشرع في وضع حاجز قانوني منيع أمام أي محاولة عبثية أو استكشافية للنظم المعلوماتية. كما أن هذه الجريمة غالبًا ما تكون بوابة لجرائم أخطر، مثل سرقة الهوية الرقمية، أو تدمير الأنظمة، أو ابتزاز الأشخاص. وبالتالي، فإن معاقبتها بشكل مستقل أمر ضروري لتحقيق الردع العام[1].

ثانيا: جريمة المساس بالمعطيات

يُعتبر التلاعب بالبيانات الرقمية من الجرائم الخطيرة التي يمكن أن تؤدي إلى نتائج كارثية، خصوصًا إذا تعلقت ببيانات مصرفية، أو سجلات صحية، أو معلومات أمنية. وفي هذا الإطار، شدد المشرع الجزائري العقوبات على كل من يقوم بتعديل أو حذف أو إدخال بيانات في نظام معلوماتي دون إذن مسبق، حيث تصل العقوبات إلى خمس سنوات حبس. هذا التشديد يعكس وعي المشرع بخطورة مثل هذه الأفعال، التي لا تمس فقط خصوصية الأفراد، بل تهدد كذلك سلامة المؤسسات الاقتصادية والإدارية. وتجدر الإشارة إلى أن المادة 394 مكرر 3، تتضمن عقوبات مشددة في حال أدى الفعل إلى تدمير النظام، أو إذا ارتُكب في إطار جماعة منظمة. وهذا التوجه يعكس تطورًا نوعيًا في السياسة العقابية، من خلال مراعاة الظروف المشددة وخصوصيات الجريمة الإلكترونية[2].

الفرع الثاني: العقوبات في القوانين الخاصة

لم يكتف المشرع الجزائري بتعديل قانون العقوبات فحسب، بل ذهب أبعد من ذلك من خلال سن قوانين قطاعية خاصة، تُعنى بتنظيم جوانب معينة من الحياة الرقمية،

أولا: قانون حماية المعطيات ذات الطابع الشخصي

[1] خليف عبد الحق، **قانون العقوبات: القسم الخاص – الجرائم الحديثة**، دار هومه، الجزائر، ط2، 2020، ص 183.
[2] مسعودي أمينة، **حماية الحياة الخاصة والمعطيات الشخصية في القانون الجزائري**، دار الهدى، الجزائر، ط1، 2020، ص 105.

يُعد القانون رقم 18-07 المؤرخ في 10 جوان 2018، من القوانين الحديثة التي تُجسد رغبة الدولة في الانخراط في مسار حماية الحياة الخاصة للمواطنين في البيئة الرقمية. وقد نص على عقوبات مشددة في حال تم تجميع أو نقل أو معالجة بيانات شخصية دون إذن من المعني، خاصة إذا تم استعمال هذه البيانات في أغراض تجارية، أو بغرض الابتزاز، أو التشهير.[1].

ثانيا: قانون البريد والاتصالات الإلكترونية

نظم القانون رقم 18-04 المؤرخ في 10 ماي 2018، المسائل المتعلقة باستغلال شبكات الاتصالات والبريد، وحدد أفعالًا جرمية ترتبط باستخدام هذه الشبكات في أغراض غير مشروعة. فالمواد من 86 إلى 90 من هذا القانون، تُعاقب بصرامة على أفعال قرصنة الاتصالات، واعتراض المراسلات، والتجسس على الشبكات، حيث تتراوح العقوبات بين الحبس لعدة سنوات، وغرامات تتجاوز مليون دينار جزائري. وقد تضمن هذا القانون نصوصًا تعكس تطور الفكر التشريعي، حيث لم يكتف بتجريم الأفعال، بل فرض على مقدمي خدمات الاتصالات التزامًا بضمان سرية المراسلات، واتخاذ تدابير الحماية الأمنية، تحت طائلة المسؤولية الجنائية والإدارية[2].

الفرع الثالث: مدى فاعلية هذه العقوبات في الحد من الجريمة الإلكترونية

اولا: صعوبة إثبات الجريمة

الإثبات في مجال الجريمة الإلكترونية يطرح تحديات هائلة، إذ تعتمد هذه الجرائم على تقنيات معقدة يصعب تتبعها، وتتم عبر شبكات محمية وأدوات تشفير. وكثيرًا ما يعجز أعوان الضبطية القضائية عن جمع الأدلة الرقمية بطريقة قانونية تُراعي قواعد الإثبات، مما يجعل العديد من القضايا تُطوى دون محاسبة. كما أن طبيعة الدليل الإلكتروني تتطلب وجود خبرات تقنية عالية، وتعاونًا وثيقًا بين الجهات الأمنية والقضائية، ومخابر رقمية مؤهلة، وهو ما لا يتوفر دائمًا في الواقع الجزائري، مما يضعف من فاعلية العقوبات حتى وإن كانت شديدة[3].

ثانيا: ضعف التعاون الدولي

[1]بلحاج أحمد، **قانون الاتصالات الإلكترونية وحماية المستهلك الرقمي**، دار المحيط، الجزائر، ط1، 2021، ص 77
[2]قادة بن عيسى، **إثبات الجرائم الإلكترونية في التشريع الجزائري**، دار المعرفة، الجزائر، ط1، 2019، ص 164.
[3]شتوح سمية، **السياسة العقابية في مواجهة الجريمة الإلكترونية**، دار الكتاب الجامعي، الجزائر، ط1، 2022، ص 90.

الجريمة الإلكترونية تتجاوز الحدود الجغرافية للدول، ومن ثم فإن مواجهتها تتطلب تعاونًا دوليًا وثيقًا، سواء عبر الاتفاقيات، أو من خلال تبادل المعلومات، أو تنفيذ أوامر القبض الدولية. غير أن الجزائر تعاني من ضعف نسبي في هذا الجانب، نتيجة غياب شراكات قوية مع الدول المتقدمة تكنولوجيًا، وغياب آليات تنسيق فورية. هذا الضعف يجعل من الصعب ملاحقة مجرمين يتخذون من دول أجنبية ملاذًا لهم، أو يستخدمون خوادم خارجية لإخفاء آثارهم، وبالتالي تضعف فاعلية العقوبة[1].

ثالثا: عدم التناسب أحيانًا بين الجرم والعقوبة

يرى العديد من الخبراء أن بعض العقوبات المنصوص عليها لا ترتقي إلى حجم الخطر الذي تُشكله الجريمة، خاصة في ما يتعلق بالجرائم التي تستهدف النظام المصرفي، أو البيانات الحساسة للدولة. ففي حين أن بعض الدول تفرض عقوبات سالبة للحرية تتجاوز العشر سنوات على جرائم مماثلة، نجد أن العقوبات في الجزائر ما تزال في حدود 3 إلى 5 سنوات في الغالب، مع غرامات لا تُحدث أثرًا ردعيًا كبيرًا. هذا التفاوت يُظهر الحاجة إلى إعادة تقييم السياسة العقابية، وإعادة ضبط سلم العقوبات بما يتناسب مع خطورة الفعل[2].

المبحث الثالث: دوافع وأساليب ارتكاب الجرائم الإلكترونية

مع التقدم المتسارع في تكنولوجيا المعلومات والاتصالات، أصبحت الجرائم الإلكترونية تمثل تهديدًا متزايدًا لأمن الأفراد والدول على حد سواء، حيث تجاوزت هذه الجرائم في طبيعتها وتعقيدها الحدود التقليدية للجريمة، واتسمت بأساليب متطورة ودوافع متعددة تختلف باختلاف السياقات النفسية والاجتماعية والاقتصادية والسياسية للمجرم الإلكتروني.

المطلب الأول: الدوافع الاقتصادية والاجتماعية للجناة

تُعد الجرائم الإلكترونية من أبرز التحديات التي تواجه المجتمعات الحديثة، نظرًا لتنوع دوافعها وتعدد أساليبها وتطورها السريع الذي يسبق أحيانًا قدرة القانون على مجاراته. وقد شهد العالم خلال العقود الأخيرة تحولاً كبيرًا في طريقة ارتكاب الجرائم، حيث بات الفضاء الإلكتروني بيئة خصبة لنمو سلوكيات

[1] شتوح سمية، **مرجع سابق**، ص 95.
[2] صديقي عبد المجيد، **مكافحة الجريمة الإلكترونية من خلال السياسة الجنائية الجزائرية**، دار اليقين، الجزائر، ط1، 2021، ص 127.

إجرامية متنوعة ومعقدة. ويُعد فهم الدوافع الاقتصادية والاجتماعية لمرتكبي هذه الجرائم أمرًا أساسيًا لوضع سياسات فعالة للوقاية والمكافحة. ويُسهم التحليل العميق لهذه الدوافع في بناء استراتيجية شاملة تتجاوز البُعد الزجري إلى الأبعاد الوقائية والتربوية[1].

الفرع الاول: الدوافع الاقتصادية

1. السعي وراء الربح السريع :لقد أصبح الربح السريع هاجسًا يلاحق الكثير من الشباب في ظل الأوضاع الاقتصادية الهشة، خاصة في الدول التي تعاني من ضعف التنمية وانتشار الفقر. ويستغل بعض الأفراد مهاراتهم التكنولوجية لأغراض غير مشروعة، فيمارسون الاحتيال المالي عبر الإنترنت، مثل إنشاء مواقع وهمية، إرسال رسائل تصيد، أو تنفيذ هجمات الفدية التي تُجبر الضحية على دفع مبالغ ضخمة لاستعادة بياناته. فالعائد السريع والمخاطرة المنخفضة – مقارنة بالجرائم التقليدية – يجعلان من الجريمة الإلكترونية بديلاً مغريًا للكثيرين[2].
2. البطالة والضغوط الاقتصادية :تُعد البطالة من العوامل الاقتصادية الأكثر تأثيرًا في سلوك الأفراد، خاصة فئة الشباب. فالشخص الذي يعاني من انعدام الدخل وغياب فرص العمل قد يلجأ إلى البحث عن بدائل غير مشروعة لتأمين حاجياته الأساسية أو لتحقيق طموحاته. ومع اتساع انتشار الإنترنت، أصبحت الجريمة الإلكترونية خيارًا متاحًا لأولئك الذين يمتلكون الحد الأدنى من المهارات التقنية. فغياب الأمل في تحسين الوضع الاقتصادي، والشعور بالتهميش والإقصاء من المجتمع، يجعل بعض الأفراد أكثر عرضة للانحراف.[3].
3. الفجوة الرقمية :تشير الفجوة الرقمية إلى التفاوت في الوصول إلى التكنولوجيا والإنترنت بين مختلف الفئات الاجتماعية أو الجغرافية، وقد تكون هذه الفجوة محفزًا للجريمة الإلكترونية.[4].

الفرع الثاني: الدوافع الاجتماعية

[1]زيوش عبد الرؤوف، زغيشي مصطفى، "الجرائم الإلكترونية الاقتصادية: المفهوم والدوافع"، مجلة الدراسات القانونية والاقتصادية، العدد 07، 2024، ص 390

[2] زيوش عبد الرؤوف، زغيشي مصطفى ، المرجع السابق ، ص400.

[3]وفاء محمد علي محمد، "الأبعاد الاجتماعية للجرائم الإلكترونية: دراسة تحليلية لمضمون عينة من القضايا في محكمة سوهاج"، مجلة جامعة سوهاج، 2021، ص 25.

[4] عبد السلام محمد المايل، عادل محمد الشربجي، "الجريمة الإلكترونية في الفضاء الإلكتروني: المفهوم، الأسباب، سبل المكافحة"، جامعة المرقب، ليبيا، 2022.، ص 59

1. التفكك الأسري وضعف الرقابة :تلعب الأسرة دورًا محوريًا في تشكيل سلوك الفرد وتوجيهه، غير أن التفكك الأسري أو غياب أحد الوالدين أو انشغالهم الزائد قد يُفضي إلى غياب الرقابة الأسرية، مما يُتيح للأطفال والمراهقين وقتًا طويلاً أمام الإنترنت دون توجيه[1].
2. الرغبة في التحدي وإثبات الذات :يسعى كثير من الشباب، خاصة أولئك الذين يفتقدون للاعتراف الاجتماعي أو النجاح الدراسي، إلى إثبات قدراتهم بأي وسيلة.
3. التأثير السلبي لوسائل الإعلام :تلعب وسائل الإعلام، التقليدية والرقمية على حد سواء، دورًا كبيرًا في تشكيل التصورات والسلوكيات، وقد يكون لهذا الدور جانب سلبي. فبعض الأفلام والمسلسلات تُصور المخترقين الإلكترونيين كأبطال[2].

الفرع الثالث: التداخل بين الدوافع الاقتصادية والاجتماعية

من المهم الإشارة إلى أن الدوافع الاقتصادية والاجتماعية لا تعمل بمعزل عن بعضها، بل تتداخل بشكل معقد. فالشاب الذي يعاني من البطالة قد يكون في نفس الوقت ضحية لتفكك أسري، ويعيش في بيئة إعلامية مشبعة بالمغريات الرقمية. كما أن الشعور بالإقصاء الاجتماعي قد يُترجم في صورة تمرّد رقمي على شكل اختراقات أو أعمال تخريب إلكتروني. ويؤكد ذلك الحاجة إلى تدخلات متعددة المستويات، تشمل السياسات العمومية، التربية، الإعلام، والعدالة الجنائية[3].

إن فهم الدوافع الاقتصادية والاجتماعية لمرتكبي الجرائم الإلكترونية يُعد حجر الأساس في بناء مقاربة فعالة وشاملة لمكافحة هذه الظاهرة..[4].

المطلب الثاني: دوافع الجريمة السياسية والإيديولوجية

تُعد الجرائم الإلكترونية ذات الطابع السياسي والإيديولوجي من أخطر التحديات التي تواجه المجتمعات الحديثة، خاصة في ظل الانفتاح الرقمي والتطور التكنولوجي السريع، حيث أضحت الجرائم لا تُقترف فحسب بدافع الحصول على مكاسب مادية، وإنما أيضًا بدوافع فكرية وأيديولوجية وسياسية عميقة، تعكس صراعات داخلية أو إقليمية أو دولية.

---

[1]دياب البداحنة، "الجرائم الإلكترونية: المفهوم والأسباب"، مجلة البحوث الأمنية، 2018، ص 20.
[2]دياب البداحنة، مرجع سابق، ص 31
[3]زوبيري حسين، "الدوافع الاجتماعية للجرائم الإلكترونية"، جريدة بركة نيوز، 2023.، ص 101
[44]دياب البداحنة، مرجع سابق، ص 37

الفرع الاول: الدوافع السياسية

لقد أصبحت السياسة من أكثر المجالات اختراقًا عبر الوسائط الرقمية، حيث باتت التكنولوجيا الرقمية أداة مركزية في التعبير عن المواقف السياسية وتنفيذ المخططات ذات البعد الاستراتيجي. وتتمثل أبرز الدوافع السياسية فيما يلي[1]:

1. **الاحتجاج على السياسات الحكومية**
2. **نشر الفكر المعارض عبر الإنترنت**

يُعتبر الإنترنت ساحة مفتوحة أمام الحركات المعارضة، خاصة تلك التي لا يُسمح لها بالعمل بحرية في الفضاء الواقعي. وهنا تلجأ هذه الحركات إلى خلق منصات رقمية بديلة، سواء مواقع إلكترونية أو حسابات على شبكات التواصل الاجتماعي أو منتديات رقمية مغلقة، لنشر خطاباتها، وانتقاد السياسات القائمة، وتوجيه الجماهير. ويُلاحظ أن كثيرًا من هذه الحركات تتخذ طابعًا تنظيميًا مُحكمًا، وتستخدم تقنيات متقدمة لإخفاء هويات أفرادها ومصادرها، مما يزيد من صعوبة مواجهتها تقنيًا وأمنيًا.

3. **الهجمات السيبرانية بين الدول (الحروب الإلكترونية)**

في إطار الصراع بين القوى الدولية، أصبحت الهجمات السيبرانية جزءًا من استراتيجية الحرب غير المباشرة. تقوم بعض الدول أو أجهزتها الاستخباراتية بشن هجمات على البنية التحتية الحيوية لدول أخرى (شبكات الكهرباء، أنظمة النقل، قواعد البيانات الحكومية...)، بهدف إرباك العدو، أو التجسس، أو حتى توجيه رسائل سياسية. المثال الأبرز على ذلك هو فيروسStuxnet، الذي تم اكتشافه عام 2010، والذي يُعتقد أن هدفه كان تخريب البرنامج النووي الإيراني. هذه الهجمات لا تترك بالضرورة آثارًا مادية ملموسة، لكنها قد تُحدث خللًا كبيرًا في توازنات القوة بين الدول، وتثير توترات دبلوماسية حادة[2].

الفرع الثاني: الدوافع الإيديولوجية والفكرية

[1]محمد عبد الرحمن حسن، **الجريمة الإلكترونية في ضوء أحكام الشريعة والقانون**، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص 15
[2]محمد عبد الرحمن حسن، المرجع السابق ، ص 17

تُعد الدوافع الفكرية من بين أخطر المحفزات للجريمة الإلكترونية، نظرًا لما تنطوي عليه من ارتباط بعقائد راسخة أو تصورات متطرفة حول العالم والمجتمع، تجعل مرتكبي هذه الجرائم ينظرون إلى أنفسهم كمناضلين أو مجاهدين في سبيل قضية يعتبرونها عادلة، ما يمنحهم دافعًا معنويًا قويًا[1].

ظهر مصطلح «الجهاد الإلكتروني» ليُعبّر عن تحول في طبيعة النشاطات الجهادية من الميدان الواقعي إلى الفضاء الافتراضي. وتقوم به جماعات إرهابية منظمة مثل «داعش» أو «القاعدة»، حيث تعتمد على تقنيات التشفير، وتطبيقات التواصل المشفّرة (مثل تيليغرام)، والبريد الإلكتروني المجهول، وغيرها من الوسائل، لنشر التعليمات وتنسيق العمليات. كما تعتمد هذه الجماعات على مواقع تعليمية تُدرّس فنون الاختراق الإلكتروني، واستخدام المتفجرات، والتمويه الرقمي، مما يُحيل الإنترنت إلى ساحة تدريب افتراضية[2].

3. الدعاية المضادة وتزييف الوعي

من أخطر أشكال الجريمة الفكرية استخدام أدوات الإعلام الرقمي لبث الدعاية المضللة، ونشر الأخبار الكاذبة، وصناعة محتوى يوهم الجماهير بواقع غير حقيقي. وقد ازداد خطر هذه الظاهرة مع انتشار تقنيات الذكاء الاصطناعي، وتحديدًا ما يُعرف بـ«التزييف العميقDeepfake «، الذي يمكن من خلاله تركيب صور وفيديوهات لأشخاص حقيقيين وهم يقولون أو يفعلون أمورًا لم تحصل في الواقع. تستخدم بعض الجماعات هذه الوسائل لتشويه سمعة الخصوم، أو تأليب الرأي العام ضد فئات معينة، أو خلق حالة من الهلع الجماعي، وهو ما يُعرف بـ«الحرب النفسية الرقمية"[3]

الفرع الثالث: الجريمة السياسية/الإيديولوجية كأداة للتمرد أو العصيان الرقمي

بدأت تظهر في السنوات الأخيرة حركات رقمية تستغل الفضاء السيبراني للتعبير عن تمردها السياسي أو الأخلاقي على النظام العالمي، مثل جماعة «أنونيموسAnonymous «، التي شنت مئات الهجمات السيبرانية على مواقع حكومية وعسكرية واقتصادية كبرى في العالم، بهدف فضح الفساد أو الدفاع عن قضايا مثل حرية التعبير وحقوق الإنسان. ما يميز هذه الجماعات هو عدم ارتباطها بأيديولوجية تقليدية، بل تعتمد على ما يُعرف بالأخلاقيات الرقمية أو «الهاكتيفيزم»، وتستخدم الهجمات

[1]محمود عبد الفضيل، **الجرائم السياسية والانقلابات في العالم العربي**، دار الشروق، القاهرة، مصر، الطبعة الثانية، 2017، ص 120
[2]عبد الجبار سعد الله، **الحروب السيبرانية: المفهوم والتأثير السياسي**، دار الفكر الجامعي، الجزائر، 2021، ص 87
[3]سامية فوزي إبراهيم، **الجريمة الإلكترونية والإرهاب الرقمي**، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، الطبعة الأولى، 2020، ص 210

كأداة ضغط معنوية وسياسية. وهذه الحركات لا تسعى بالضرورة للسلطة، بل لتحريك الضمائر العالمية، وقد حققت في بعض الحالات نتائج ملموسة مثل إجبار شركات على تغيير سياساتها، أو فضح ملفات حساسة للرأي العام[1].

الفرع الرابع: السياق الدولي والإقليمي كبيئة محفزة لهذه الجرائم

تتغذى الجريمة السياسية والإيديولوجية الإلكترونية من البيئة الدولية المضطربة، حيث تعيش العديد من الدول أوضاعًا سياسية هشة، أو أزمات هوية، أو صراعات طائفية، وهو ما يُشكل أرضًا خصبة لنشأة التيارات المتطرفة أو المعارضة الراديكالية. كما أن فشل بعض الأنظمة في احتواء التنوع الأيديولوجي، أو قمع حرية التعبير، يدفع المعارضة نحو التعبير الرقمي المتطرف. من جهة أخرى، فإن الحروب الأهلية أو التوترات الإقليمية (مثل الصراع الفلسطيني الإسرائيلي، أو الحرب في سوريا) قد تدفع أطرافًا داخلية أو خارجية إلى استخدام الإنترنت كساحة لصراع موازٍ. ولا ننسى أن بعض القوى العالمية تستخدم الجماعات الرقمية كأذرع غير رسمية في صراع النفوذ العالمي[2].

الفرع الخامس: ضعف المواجهة التشريعية والإعلامية

رغم خطورة هذه الجرائم، فإن أغلب الأنظمة القانونية لا تملك حتى اليوم أدوات قانونية فعّالة لمواجهتها، إذ غالبًا ما تُصنّف الجرائم حسب آثارها المباشرة، لا حسب دوافعها. فالاختراق السياسي قد يُعامل كأنه مجرد اختراق معلومات، دون أخذ الخلفية الإيديولوجية بعين الاعتبار، مما يضعف من الردع والعقاب. كما أن الإعلام، في كثير من الدول، إما خاضع لرقابة أو يفتقر للخبرة التكنولوجية، فلا يستطيع تفكيك الخطابات الرقمية المتطرفة أو فضح أهدافها الحقيقية. كما أن الإعلام أحيانًا يتحول إلى أداة تضليل بدل أن يكون أداة كشف، مما يُفاقم أزمة الوعي العام[3].

المطلب الثالث: الأساليب التقنية الفيروسات الاختراق التصيد الاحتيالي

أصبحت الجريمة الإلكترونية تمثل تهديدًا عالميًا حقيقيًا، ليس فقط بسبب عددها المتزايد، ولكن أيضًا بسبب تنوع الأساليب التقنية المعتمدة في تنفيذها. فمع تزايد الاعتماد على الإنترنت في كل مناحي الحياة،

[1] أحمد بن عبد العزيز الشدوخي، **الجرائم المعلوماتية في المملكة العربية السعودية: دراسة مقارنة**، مكتبة الرشد، الرياض، السعودية، الطبعة الأولى، 2018، ص 75-

[2] عبد الحفيظ غريبة، **الجرائم السياسية والإرهاب في القانون الجزائري**، منشورات المجمع العلمي الجزائري، الجزائر، 2020، ص 34

[3] عبد الله بوجلال، "الهاكتيفيزم والمقاومة الرقمية: رؤية في الأيديولوجيا الإلكترونية"، مجلة العلوم الإنسانية، جامعة بسكرة، العدد 17، 2022، ص 221

أصبحت الفيروسات، وبرمجيات الاختراق، والتصيد الاحتيالي من الأدوات الرئيسة التي يوظفها المجرمون الإلكترونيون من أجل تحقيق أهدافهم. إنّ فهم هذه الأساليب، وآلياتها التقنية، ودورها في زعزعة أمن المعلومات، يُعدّ مدخلًا أساسيًا لمواجهة التحديات المرتبطة بالأمن السيبراني. سنفصل في هذا المطلب كل أداة على حدة، لنبيّن مدى خطورتها وتطوّرها، وآليات التصدي لها.

الفرع الاول: الفيروسات والبرمجيات الخبيثة:(Malware)

تُعتبر البرمجيات الخبيثة من أقدم وأكثر الأدوات المستخدمة في تنفيذ الجرائم الإلكترونية، وتعود جذورها إلى بدايات استخدام الحواسيب الشخصية، لكنها تطورت تطورًا مذهلًا، لتصبح أدوات دقيقة ومعقّدة قادرة على تنفيذ عمليات تخريبية وتجسسية على نطاق واسع. الفيروسات هي نوع من هذه البرمجيات الخبيثة، حيث تُصمّم لتنتقل بين الأجهزة، مستغلة الثغرات الأمنية، أو عن طريق تصرّف المستخدم نفسه دون علمه. هناك أنواع متعددة من هذه الفيروسات، أبرزها فيروسات التدمير، التي تستهدف حذف أو إتلاف الملفات، وفيروسات الدودة التي تنتشر عبر الشبكات وتسبب بطئًا عامًا أو توقفًا كاملاً عن العمل. من أشهر هذه الأنواع أيضًا، حصان طروادة الذي يُخفي نفسه داخل برامج تبدو شرعية، ويؤدي وظائف خفية لصالح المهاجم[1].

الفرع الثاني: الاختراق الإلكتروني:(Hacking)

يُعد الاختراق من أكثر الأساليب شهرة في الجرائم الإلكترونية، ويعني الوصول غير المشروع إلى أنظمة أو بيانات أو شبكات، باستخدام أدوات تقنية متخصصة. المهاجم في هذه الحالة يكون إما فردًا أو مجموعة من القراصنة السيبرانيين المدربين، وقد يكون الدافع من وراء الاختراق سرقة المعلومات، أو التخريب، أو حتى التجسس لصالح جهات أجنبية. توجد أنواع متعددة من الاختراق، منها ما يُعرف بالاختراق الأخلاقي، الذي يُستخدم لاختبار فعالية الأنظمة الأمنية، وغالبًا ما يتم بموافقة مُلاك النظام. بينما الاختراق الإجرامي هو ما يتم خلسة، ويستهدف تحقيق مكاسب غير شرعية. [2].

الفرع الثالث: التصيّد الاحتيالي:(Phishing)

[1]هالة عبد المنعم، **الجرائم الإلكترونية: التحديات والحلول**، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى، 2021، ص 132
[2]محمود سالم، **الجرائم الإلكترونية وأساليب مكافحتها**، دار الفكر العربي، القاهرة، مصر، الطبعة الثالثة، 2020، ص 189

التصيّد الاحتيالي هو أحد أكثر الأساليب خداعًا في الجريمة الإلكترونية، ويعتمد بشكل كبير على خداع الضحية وليس فقط على استغلال الثغرات التقنية. يقوم المهاجمون بإرسال رسائل مزيفة إلى الضحايا، تتظاهر بأنها قادمة من مصادر موثوقة مثل البنوك، أو منصات التواصل، أو مواقع التجارة الإلكترونية. الهدف هو إقناع الضحية بإدخال بياناته السرية، مثل كلمات المرور، أو أرقام الحسابات البنكية، أو معلومات الهوية. التصيّد يتم بعدة أشكال: التصيد التقليدي باستخدام البريد الإلكتروني، والتصيّد الموجه الذي يستهدف أشخاصًا معينين عبر معلوماتهم الخاصة، والتصيّد الصوتي عبر الهاتف (Vishing)، والتصيّد عبر الرسائل النصية[1].(Smishing)

وقد تكون نتائج التصيّد كارثية: من سرقة الهوية، إلى خسائر مالية جسيمة، بل وقد تمتد لاختراق شبكات مؤسسات بأكملها[2].

الفرع الرابع: العلاقة التفاعلية بين هذه الأساليب

من الخطأ الشائع تصور أن الجريمة الإلكترونية تعتمد على أسلوب واحد فقط، إذ غالبًا ما تكون هناك تداخلات تقنية بين الفيروسات، والاختراق، والتصيّد. فقد يبدأ المهاجم بتصيّد ضحية عبر رسالة بريد إلكتروني مقنعة، تحتوي على رابط يُحمّل ملفًا خبيثًا يحتوي فيروسًا، يمهّد الطريق للاختراق الكامل للنظام. هذه الديناميكية المركبة تزيد من فعالية الهجمات، وتُصعّب مهمة الاكتشاف المبكر. الجمع بين أكثر من أداة يجعل من الهجوم أكثر تطورًا، خصوصًا عندما يتم استخدام أدوات الذكاء الاصطناعي والتعلم الآلي في مراحل التخطيط والتنفيذ.

الفرع الخامس: تطور الأساليب التقنية مع الذكاء الاصطناعي:

مع ظهور تقنيات الذكاء الاصطناعي، دخلت الجريمة الإلكترونية مرحلة جديدة من الاحترافية. فقد أصبح بإمكان المهاجمين استخدام نماذج لغوية متقدمة لصياغة رسائل تصيّد احترافية، أو لتوليد برمجيات خبيثة تتغير تلقائيًا لتفادي برامج الحماية، أو لتحليل سلوك الضحايا على الإنترنت واستهدافهم برسائل مخصصة. كما أصبح من الممكن توليد محتوى مزيف باستخدام تقنيات التزييف العميق (Deepfake)

[1]سامي خليل، **أمن المعلومات والجرائم المعلوماتية**، مكتبة الرشد، الرياض، السعودية، الطبعة الأولى، 2019، ص 101
[2]فاطمة الزهراء بن عيسى، "التطور التقني للجريمة الإلكترونية: دراسة مقارنة"، *مجلة دراسات قانونية وسياسية*، جامعة قسنطينة، العدد 27، 2022، ص 250

لتوريط الضحايا أو ابتزازهم. التطور الهائل في تقنيات الذكاء الاصطناعي، إن لم يُواكَب بتقنيات دفاعية موازية، سيكون له أثر خطير على أمن الأفراد والدول على حد سواء[1].

المطلب الرابع: استخدام الأدوات والبرمجيات الخبيثة وتحليل سلسلة الهجوم

في العصر الرقمي الحديث، تزايدت بشكل ملحوظ التهديدات الإلكترونية التي تستهدف الأفراد والمؤسسات على حد سواء. وتلعب البرمجيات الخبيثة (Malware) دورًا محوريًا في تنفيذ هذه الهجمات، حيث أصبحت من الأدوات الأساسية للمجرمين الإلكترونيين في جميع أنحاء العالم. وتتميز هذه البرمجيات بمرونتها الكبيرة وإمكانية تخصيصها لتناسب أهدافًا متعددة، مثل سرقة المعلومات الحساسة، تعطيل الأنظمة، أو تنفيذ عمليات ابتزاز إلكتروني. وتكمن خطورتها في قدرتها على أن تكون جزءًا من سلسلة هجوم إلكتروني متكاملة، تبدأ من مرحلة الاستطلاع وحتى تحقيق الهدف النهائي.

الفرع الاول: مفهوم البرمجيات الخبيثة

البرمجيات الخبيثة هي برامج تم تصميمها خصيصًا لإحداث ضرر متعمد بالمستخدم أو النظام الذي تعمل عليه. تختلف أشكال هذه البرمجيات باختلاف الأهداف والوسائل، لكنها تشترك في السلوك العدائي تجاه الأنظمة أو البيانات أو الشبكات. وقد تطورت هذه البرمجيات مع تطور التكنولوجيا، فأصبحت أكثر تعقيدًا وأصعب في الكشف عنها. ومن بين خصائصها الأساسية قدرتها على الانتشار السريع، والتخفي، واستغلال الثغرات سواء التقنية أو الاجتماعية لتحقيق أهدافها[2].

اولا: أنواع البرمجيات الخبيثة

تتنوع البرمجيات الخبيثة وفقًا لأساليبها وأهدافها، ومن أبرز أنواعها[3]:

1 **الفيروسات:(Viruses)** تصيب ملفات شرعية وتقوم بالانتشار من خلال نسخ نفسها داخل نظام التشغيل. وغالبًا ما تحتاج إلى تفاعل المستخدم لنشرها.

[1]وسيم فريد، "برامج الفدية والتهديد الجديد لأمن المعلومات"، *مجلة الفكر المعلوماتي*، العدد 18، 2023، ص 112

[2]عبد الرحمن حجازي، **الهجمات الإلكترونية الحديثة: دراسة تحليلية وتقنية**، دار الفكر المعاصر، بيروت، لبنان، الطبعة الأولى، 2021، ص 88

[3]رامي عبد الله، "تحليل سلسلة الهجوم السيبراني وفق نموذج"Cyber Kill Chain ، *مجلة الأمن السيبراني العربي*، العدد 5، 2022، ص 59

2 **الديدان:(Worms)** تنتشر ذاتيًا دون الحاجة إلى ملفات مرفقة أو تدخل بشري، وتُعد من أخطر الأنواع من حيث سرعة الانتشار.

3 **أحصنة طروادة:(Trojans)** تخدع المستخدم بأنها برامج مفيدة بينما تؤدي مهامًا ضارة كفتح ثغرات خلفية.

4 **برمجيات الفدية:(Ransomware)** تقوم بتشفير بيانات المستخدم وتطلب فدية مالية لفك التشفير.

5 **برمجيات التجسس:(Spyware)** تراقب نشاط المستخدم دون علمه، وغالبًا تُستخدم لجمع كلمات المرور أو بيانات حساسة.

6 **برمجيات التعدين غير الشرعي:(Cryptojacking)** تستغل موارد جهاز الضحية (كالطاقة والمعالج) لتعدين العملات الرقمية دون علمه.

الفرع الثاني: الأدوات التقنية المستخدمة في الهجوم

يعتمد المهاجمون الإلكترونيون على ترسانة من الأدوات البرمجية المتخصصة التي تُستخدم في مراحل مختلفة من الهجوم السيبراني، نذكر منها[1]:

- **أدوات الاستطلاع:(Reconnaissance Tools)** تُستخدم لجمع معلومات أولية عن الهدف، مثل المنافذ المفتوحة والخدمات المشغلة، ومن أبرزها "Nmap" و."Shodan"
- **أدوات استغلال الثغرات:(Exploitation Kits)** مثل"Metasploit" ، تتيح استغلال ثغرات معروفة في الأنظمة أو التطبيقات بهدف تنفيذ كود خبيث.
- **برامج التحكم عن بعد:(RATs)** مثل"DarkComet" ، تتيح للمهاجم التحكم الكامل بجهاز الضحية كما لو كان أمامه.
- **برامج تسجيل النقرات:(Keyloggers)** تُستخدم لالتقاط كل ما يكتبه المستخدم، مما يسهل سرقة كلمات المرور والبيانات الشخصية.
- **Rootkits:**وهي أدوات خبيثة تُستخدم لإخفاء وجود المهاجم داخل النظام لفترات طويلة دون أن تُكتشف من قبل أنظمة الحماية.

[1]عبد الرحمن حجازي، **مرجع سابق**، ص 98

الفرع الثالث: تحليل سلسلة الهجوم السيبراني

تُعرف سلسلة الهجوم السيبراني باسم **Cyber Kill Chain**، وهي إطار مفاهيمي يوضح تسلسل المراحل التي يعتمدها المهاجم الإلكتروني للوصول إلى هدفه. وتتمثل مراحلها فيما يلي[1]:

1. **مرحلة الاستطلاع:(Reconnaissance)** تبدأ بجمع معلومات دقيقة عن الضحية، مثل بيانات الأجهزة والبريد الإلكتروني والعناوين الشبكية، باستخدام أدوات مثل Google Dorking أو تقنيات الهندسة الاجتماعية.
2. **مرحلة التسلح:(Weaponization)** يتم خلالها تجهيز البرمجية الخبيثة المناسبة وإقرانها بوسيلة توصيل، مثل مستند يحتوي على كود خبيث.
3. **مرحلة الإرسال:(Delivery)** يُرسل الكود الخبيث إلى الضحية من خلال البريد الإلكتروني، أو رابط مصاب، أو ناقل USB.
4. **مرحلة الاستغلال:(Exploitation)** يُنفذ الكود الخبيث على الجهاز المستهدف عبر استغلال ثغرة في النظام أو التطبيق.
5. **مرحلة التثبيت:(Installation)** يتم تنصيب البرمجية بشكل دائم في النظام حتى بعد إعادة التشغيل.
6. **مرحلة القيادة والسيطرة:(C2)** يتصل الجهاز المصاب بخادم خارجي يسيطر عليه المهاجم لإعطاء الأوامر أو استقبال البيانات.
7. **مرحلة تحقيق الأهداف:(Actions on Objectives)** يُنفذ فيها المهاجم هدفه النهائي، مثل سرقة البيانات أو تدمير النظام أو تشفير الملفات.

الفرع الرابع: أمثلة تطبيقية من الواقع

التاريخ الرقمي مليء بأمثلة عن الهجمات السيبرانية التي استخدمت برمجيات خبيثة بطريقة متطورة، من أبرزها[2]:

[1] عبد الرحمن حجازي، **مرجع سابق**، ص 105
[2] سامي أبو زيد، **أمن المعلومات ومواجهة البرمجيات الخبيثة**، دار الشروق، عمان، الأردن، الطبعة الثالثة، 2020، ص 133

- **هجوم:(2017) WannaCry**استهدف هذا الهجوم العالمي ثغرة في أنظمة Windows تُعرف باسم"EternalBlue" ، وانتشر بسرعة مذهلة مشفرًا بيانات آلاف المؤسسات، وطالب بفدية مالية لفك التشفير.
- **هجوم:Stuxnet**يُعد أول هجوم سيبراني معروف صُمم لإحداث أضرار مادية، حيث استهدف أجهزة الطرد المركزي النووية الإيرانية من خلال برمجية خبيثة متقدمة للغاية.
- **حملة التصيد ضد:(2022) Gmail** استخدم المهاجمون صفحات مزورة تحاكي صفحة تسجيل الدخول لجوجل، وأرفقواKeyloggersلسرقة بيانات المستخدمين.

الفرع الخامس: مكافحة البرمجيات الخبيثة

تتطلب مواجهة البرمجيات الخبيثة نهجًا متعدد الأبعاد يجمع بين التقنيات والتوعية البشرية، وتشمل أهم الوسائل[1]:

- **استخدام مضادات الفيروسات:**تحديث برامج الحماية بشكل منتظم يساعد في اكتشاف البرمجيات المعروفة وحذفها.
- **مراقبة السلوكيات:(BehavioralAnalysis)** وهي تقنيات تعتمد على تحليل سلوك التطبيق بدلًا من الاعتماد فقط على التوقيعات.
- **التحديث المستمر:**سد الثغرات في الأنظمة والبرمجيات يعد خط الدفاع الأول ضد الاستغلال.
- **التدريب والتوعية:**تمثل نقطة ضعف بشرية مهمة، لذا من الضروري تدريب الموظفين على كيفية التعرف على الرسائل الخبيثة.
- **تقسيم الشبكات:(Network Segmentation)** يساعد على تقليل التأثير في حال حدوث اختراق، ويمنع انتشار البرمجيات داخل المؤسسة.

[1]عبد الرحمن حجازي، **مرجع سابق**، ص 114

الفصل الثاني:

سبل مكافحة الجرائم الإلكترونية

تمهيد:

مع التقدم التكنولوجي المتسارع الذي يشهده العالم، ازدادت التحديات المرتبطة بالأمن الرقمي، وبرزت الجرائم الإلكترونية كأحد أخطر التهديدات التي تواجه الأفراد، المؤسسات، والحكومات على حد سواء. فهذه الجرائم، التي تتنوع بين الاختراقات، الاحتيال الإلكتروني، الابتزاز، والاعتداء على الخصوصية، تتميز بطابعها غير التقليدي وصعوبة تتبع مرتكبيها، مما يفرض ضرورة إعادة النظر في آليات المكافحة التقليدية.

لقد أظهرت الدراسات الحديثة أن الوقاية من الجريمة الإلكترونية لا تقتصر على الجوانب الأمنية التقنية فحسب، بل تتطلب تكاملاً في الجهود القانونية، المؤسساتية، والاجتماعية، فضلاً عن تعزيز وعي المستخدمين وتطوير أطر التعاون الدولي. ولهذا، أصبح لزامًا على الدول أن تبلور سياسات وطنية متكاملة لمكافحة الجريمة الإلكترونية، تشمل سنّ تشريعات حديثة، تحديث البنى التحتية الرقمية، وإنشاء أجهزة متخصصة في التحري الرقمي الجنائي.

في ضوء ما سبق، يتناول هذا الفصل أبرز السبل المعتمدة في مكافحة الجرائم الإلكترونية، من خلال التطرق إلى الإطار القانوني والمؤسساتي، الوسائل التقنية الحديثة، دور التوعية والتثقيف، والتعاون الدولي. كما يسعى إلى إبراز أهمية تفعيل هذه السبل بشكل متكامل للحد من تفشي هذا النوع من الجرائم في البيئة الرقمية المعاصرة.

المبحث الأول: التدابير الوقائية والتقنية

تُعد التدابير الوقائية والتقنية حجر الأساس في منظومة مكافحة الجرائم الإلكترونية، إذ تمثل خط الدفاع الأول في مواجهة التهديدات الرقمية المتزايدة. فمع تطور أساليب القراصنة وتعدد أشكال الهجمات الإلكترونية، بات من الضروري اعتماد مقاربات وقائية متقدمة ترتكز على أدوات التكنولوجيا الحديثة، وأنظمة الحماية الذكية، والتحديث المستمر للبنية التحتية للمعلومات.

وتكمن فعالية هذه التدابير في قدرتها على رصد الهجمات قبل وقوعها، والتقليل من آثارها حال حدوثها، من خلال مجموعة من الوسائل كجدران الحماية، برامج مكافحة الفيروسات، أنظمة كشف التسلل، وتقنيات التشفير. كما تتكامل هذه الإجراءات مع سياسات أمن المعلومات وإدارة المخاطر التي تعتمدها المؤسسات لحماية بياناتها ومواردها الرقمية.

لذا، يعالج هذا المبحث أبرز التدابير الوقائية والتقنية المعتمدة لمجابهة الجرائم الإلكترونية، موضحًا أبعادها وأهميتها، ومؤكدًا على ضرورة تكاملها مع وعي المستخدم وسياسات الأمن السيبراني الشاملة.

المطلب الأول: التوعية والتثقيف السيبراني لدى الأفراد والمؤسسات

في ظل التحولات الرقمية المتسارعة التي يشهدها العالم، أصبحت مسألة التوعية والتثقيف السيبراني من القضايا الجوهرية التي يجب أن تتصدر أولويات الأفراد والمؤسسات على حد سواء. إذ أن الاعتماد على التكنولوجيا لم يعد خيارًا، بل ضرورة فرضتها طبيعة الحياة المعاصرة، بما تحمله من تعاملات رقمية، وتبادل معلوماتي، واتصال دائم عبر الشبكات، مما أفرز تحديات أمنية غير مسبوقة، يتصدرها خطر الهجمات السيبرانية. هذه الأخيرة لم تعد مقتصرة على استهداف الأنظمة الحكومية أو المؤسسات الكبرى، بل باتت تطال الأفراد والمؤسسات الصغيرة، ما يجعل من نشر الثقافة السيبرانية أمرًا لا يقبل التأجيل.

الفرع الأول: أهمية التوعية السيبرانية

تبرز هنا أهمية التوعية كأداة وقائية تسبق العلاج، إذ تساعد على بناء مناعة معلوماتية داخل المجتمع.

ويُفهم من التوعية السيبرانية تلك الأنشطة التربوية والإعلامية التي تستهدف تغيير سلوكيات الأفراد الرقمية، وتعزيز وعيهم بخطورة التهديدات السيبرانية، وتمكينهم من تبني ممارسات آمنة في حياتهم التكنولوجية اليومية. فالمعرفة وحدها لا تكفي، بل يجب أن تتحول إلى سلوك راسخ، وهذا هو جوهر التثقيف السيبراني. تبدأ التوعية من أبسط الأمور، مثل كيفية اختيار كلمة مرور قوية، أو التعرف على رسائل البريد الإلكتروني المشبوهة، لكنها تتدرج لتشمل فهم أعمق لمفاهيم أمن المعلومات، وإدراك قيمة البيانات الشخصية والمؤسساتية، وكيفية التصرف السليم عند وقوع اختراق أو تسريب. ولا شك أن التنشئة التربوية، سواء في المدارس أو البيئات المهنية، تلعب دورًا محوريًا في ترسيخ هذا الفهم[1].

إن الأفراد يمثلون الخط الدفاعي الأول في مواجهة الهجمات الإلكترونية. فمهما بلغت كفاءة النظم التقنية، فإن خطأً بسيطًا ناتجًا عن جهل أو تهاون بشري قد يتسبب في كارثة معلوماتية. وهنا تتجلى أهمية تثقيف الأفراد وتمكينهم من أدوات الحماية الذاتية. على سبيل المثال، يُمكن لمستخدم بسيط أن يكون بوابة لاختراق نظام بأكمله من خلال النقر على رابط مشبوه، أو تحميل ملف خبيث. لذلك، فإن التثقيف لا يقتصر على موظفي الأقسام التقنية، بل يجب أن يشمل جميع الشرائح. فالوعي يجب أن يكون عامًا، شاملاً، ومُتدرجًا بحسب الفئة المستهدفة.

وقد بات واضحًا أن أحد أبرز التحديات التي تواجه استراتيجيات الأمن السيبراني هو التغافل عن العامل البشري. فغالبًا ما يُنظر إلى الأمن من زاوية تكنولوجية فقط، متناسين أن التقنية لا تحمي ذاتها، بل تحتاج إلى مستخدم واعٍ ومؤهل. إن الوقاية من الهجمات تبدأ من وعي الفرد، فكلما ارتفع مستوى

[1] **أحمد خالد الزبيدي**، *مدخل إلى الأمن السيبراني: المبادئ والتطبيقات*، دار صفاء للنشر والتوزيع، الطبعة الأولى، الأردن، 2021، ص. 65.

الوعي، تقلصت فرص النجاح أمام محاولات الاختراق. وقد أشار القزاز (2022)[1] إلى أهمية إدماج المواطن كطرف فاعل في منظومة الحماية المعلوماتية، وهو ما يعني ضرورة توسيع قاعدة التوعية لتشمل المواطنين العاديين، لا فقط النخب التقنية أو العاملين في قطاع التكنولوجيا. وهذا يتطلب استثمارًا مستدامًا في برامج التعليم الرقمي والتدريب العملي، وتوظيف وسائل الإعلام والمنصات الاجتماعية لنشر رسائل توعوية بلغة بسيطة وسهلة الفهم.

وفي السياق المؤسسي، تزداد أهمية التوعية السيبرانية مع تعقيد البُنى الرقمية وتنوع مصادر التهديد. فالمؤسسات، بخلاف الأفراد، تدير قواعد بيانات ضخمة، وتتعامل مع معلومات حساسة قد تكون سرية أو تجارية أو مالية. وفي حال اختراق هذه البيانات، فإن الأضرار لا تقتصر على خسائر مادية، بل تمتد إلى السمعة المؤسسية، وثقة العملاء، وقد تؤدي إلى تبعات قانونية وتنظيمية. لذا، من الضروري أن تعتمد المؤسسات برامج توعية شاملة ومستمرة، تُدمج ضمن السياسات الإدارية والهيكل التنظيمي. ومن الممارسات المثلى في هذا المجال، تدريب الموظفين بشكل دوري على أحدث أساليب الاحتيال السيبراني، وإشراكهم في محاكاة لهجمات افتراضية، وتوفير أدلة إرشادية توضح كيفية التصرف في حال حدوث طارئ. كما أن إعداد سياسات أمنية واضحة، وتفعيل القوانين الداخلية المتعلقة باستخدام البريد الإلكتروني، وتحديث كلمات السر، من شأنها أن تخلق بيئة رقمية آمنة.

ولقد أكدت دراسة أنديجانيوفلمبان (2022)[2] على الدور المتنامي للمؤسسات التعليمية في نشر الوعي السيبراني، خاصة في منطقة الخليج العربي، حيث بدأت الجامعات والمدارس تعتمد نماذج تدريبية تفاعلية تجمع بين النظرية والتطبيق، وتسعى لتكوين ثقافة أمنية لدى الطلاب والعاملين على حد سواء. إن هذه التجربة تُعد نموذجًا يحتذى به، خصوصًا إذا ما تم دعمها من طرف السياسات الحكومية، وإدماجها

[1] **توفيق محمود محمد القزاز**، *الأمن السيبراني لمصادر المعلومات Cyber Security* ، مؤسسة طيبة للنشر والتوزيع، الطبعة الأولى، مصر، 2022، ص. 87.

[2] **دلال صالح أنديجاني، فدوى ياسين نور الدين فلمبان**، *ممارسات تعزيز الوعي بثقافة الأمن السيبراني في المؤسسات التعليمية*، مجلة العلوم التربوية والنفسية، المجلد 6، العدد 4، الخليج العربي، 2022، ص. 47.

في المناهج التربوية الرسمية. وفي الوقت ذاته، لا بد أن تتواكب هذه الجهود مع حملات إعلامية ذكية، تستثمر أدوات الإعلام الرقمي، مثل الفيديوهات التوضيحية القصيرة، والرسائل المصورة، والنصائح اليومية، التي يمكن نشرها عبر شبكات التواصل الاجتماعي، لتصل إلى أوسع شريحة ممكنة.

وفيما يتعلق باستراتيجيات التوعية الفعّالة، فإنها لا تقتصر على مجرد نقل المعرفة، بل تتطلب توظيف تقنيات تعليمية حديثة تركز على التفاعل والمشاركة. فالتجربة أثبتت أن التلقي السلبي للمعلومات لا يؤدي إلى نتائج مُستدامة، بينما تُحقق المحاكاة والتدريب العملي نتائج أفضل في ترسيخ السلوك الأمني. وهنا يأتي دور السيناريوهات التفاعلية التي تحاكي الهجمات الحقيقية، مما يُمكن المتدربين من اكتساب الخبرة بطريقة آمنة. كما ينبغي أن تُصمم البرامج التدريبية وفقًا للفئة المستهدفة، بحيث تراعي خلفيتها المعرفية ومستوى تعاملها مع التكنولوجيا. فالموظف التقني يختلف عن الإداري، والطالب يختلف عن الأستاذ، مما يتطلب تخصيص المحتوى ليتناسب مع كل فئة.

وقد نبهت بادة وساس (2019) إلى أن العديد من حملات التوعية تفشل لأنها تركز على الجانب النظري فقط، وتهمل البعد العملي، مما يجعل المعلومات المُكتسبة عرضة للنسيان، ولا تؤدي إلى تغيير حقيقي في السلوك. لذلك فإن التوعية السيبرانية الناجحة هي تلك التي تتغلغل في الثقافة المؤسسية، وتُصبح جزءًا من هوية المؤسسة، وليست مجرد نشاط عابر أو موسمي. ويجب أن تكون التدريبات إلزامية، ويُعاد تقييمها بصفة دورية، مع تحفيز الموظفين على الالتزام بالسلوكيات الآمنة، وربط هذا الالتزام بتقييم الأداء الوظيفي عند الإمكان[1].

لكن رغم وضوح هذه الرؤية، إلا أن التحديات لا تزال قائمة. فالكثير من المؤسسات، خاصة في الدول النامية، تُعاني من نقص الكفاءات المتخصصة في الأمن السيبراني، مما يُعيق تنفيذ برامج توعية فعالة. كما أن بعض الموظفين يُبدون مقاومة للتغيير، إما بدافع الكسل أو الخوف من المجهول، مما

[1] **ماريا بادة، أنجيلا إم ساس، جيسون آر سي نيرس**، *حملات التوعية بالأمن السيبراني: لماذا تفشل في تغيير السلوك؟*، أرشيفarXiv، الولايات المتحدة الأمريكية، 2019، ص. 5.

يتطلب جهودًا مضاعفة في الإقناع والتحفيز. كذلك، فإن ضعف التمويل المخصص للتوعية يُعتبر من العقبات الكبرى، إذ غالبًا ما يُنظر إلى الأمن السيبراني كمجال ثانوي لا يستحق الاستثمار الجاد، وهو تصور خاطئ قد يُكلف المؤسسة مستقبلها.

أما على المستوى المجتمعي، فإن الاستجابة الجماعية للتهديدات لا تزال بطيئة، ولا تتناسب مع سرعة انتشار الهجمات. فالثقافة الرقمية لدى الكثيرين تفتقر إلى الحس الأمني، ويغلب عليها الاستخدام العشوائي وغير الواعي للتكنولوجيا. لذلك، فإن نشر الوعي يتطلب تظافر الجهود بين المؤسسات التعليمية، والإعلام، والمجتمع المدني، والدولة، لتشكيل جبهة توعوية متماسكة. فالمعركة ضد الجريمة السيبرانية لا تُربح بالتقنيات فقط، بل بعقل بشري واعٍ، قادر على التمييز، والتصرف، والتعاون[1].

وهكذا، فإن التوعية والتثقيف السيبراني يمثلان حجر الزاوية لأي نظام أمن رقمي مستدام. فمن دون وعي، تصبح أكثر الحلول التقنية عرضة للفشل. ومن دون ثقافة أمنية، تظل المجتمعات عرضة للاستغلال. إننا بحاجة إلى نشر الوعي باعتباره مسؤولية جماعية، تبدأ من البيت، وتُرسخ في المدرسة، وتُمارس في العمل، ليُصبح السلوك الآمن عادةً لا تحتاج إلى تذكير.

الفرع الثاني:دور العامل البشري في التصدي للجرائم الالكترونية

إن الأفراد يمثلون الخط الدفاعي الأول في مواجهة الهجمات الإلكترونية. فمهما بلغت كفاءة النظم التقنية، فإن خطأً بسيطًا ناتجًا عن جهل أو تهاون بشري قد يتسبب في كارثة معلوماتية. وهنا تتجلى أهمية تثقيف الأفراد وتمكينهم من أدوات الحماية الذاتية. على سبيل المثال، يُمكن لمستخدم بسيط أن يكون بوابة لاختراق نظام بأكمله من خلال النقر على رابط مشبوه، أو تحميل ملف خبيث. لذلك، فإن

[1] **محمد عبد الحميد النجار**، *الأمن السيبراني وحماية نظم المعلومات*، دار الفكر الجامعي، الطبعة الثانية، مصر، 2020، ص. 102.

التثقيف لا يقتصر على موظفي الأقسام التقنية، بل يجب أن يشمل جميع الشرائح. فالوعي يجب أن يكون عامًا، شاملاً، ومُتدرجًا بحسب الفئة المستهدفة.

وقد بات واضحًا أن أحد أبرز التحديات التي تواجه استراتيجيات الأمن السيبراني هو التغافل عن العامل البشري. فغالبًا ما يُنظر إلى الأمن من زاوية التكنولوجيا فقط، متناسين أن التقنية لا تحمي ذاتها، بل تحتاج إلى مستخدم واعٍ ومؤهل. إن الوقاية من الهجمات تبدأ من وعي الفرد، فكلما ارتفع مستوى الوعي، تقلصت فرص النجاح أمام محاولات الاختراق

أما على مستوى المجتمع، فإن الاستجابة الجماعية للتهديدات لا تزال تسير بوتيرة بطيئة، ولا تتناسق مع سرعة انتشار الهجمات. فالثقافة الرقمية لدى الكثيرين تتسم بالامبالاة، ويغلب عليها الاستخدام العشوائي للتكنولوجيا.

فالمعركة ضد الجريمة السيبرانية لا تُربح بالتقنيات فقط، بل بعقل بشري واعٍ، قادر على التمييز، والتصرف، والتعاون

المطلب الثاني: بروتوكولات أمن المعلومات وأدوات الحماية التقنية

الفرع الأول: بروتوكولات أمن المعلومات

أولاً: بروتوكولTLS

يُعد بروتوكول TLS (أمن طبقة النقل) من أكثر البروتوكولات شيوعًا في تأمين الاتصالات عبر الإنترنت، ويُستخدم لحماية البيانات المتبادلة بين العميل (المستخدم) والخادم (الموقع). يعمل TLS على تشفير البيانات بشكل يضمن الخصوصية وعدم التلاعب أو الاطلاع عليها أثناء انتقالها. يتميز بإجراء مصافحة أولية بين الطرفين تُعرف بـ"TLS Handshake"، يتم فيها التفاوض على خوارزميات التشفير وتبادل المفاتيح العامة، ومن ثم يتم إنشاء مفتاح مشترك يُستخدم في التشفير المتناظر. أحدث إصدار له، TLS 1.3، تم تحسينه بشكل كبير لتقليل زمن الاتصال وتعزيز الأمان عبر تقليل عدد خطوات

المصافحة واعتماد خوارزميات تشفير متقدمة. من أهم خصائص TLS دعمه للتشفير من طرف إلى طرف، المصادقة المتبادلة، والتكامل البياني للبيانات المنقولة[1].

ثانياً: بروتوكولIPsec

يعتبرIPsecمجموعة من البروتوكولات التي تؤمن حركة البيانات على مستوى طبقة الشبكة. يُستخدمIPsecفي الشبكات الافتراضية الخاصة (VPN) ويؤمّن الاتصال بين موقعين أو جهازين عبر شبكة غير آمنة كشبكة الإنترنت. يعتمدIPsecعلى مكونين رئيسيين: رأس المصادقة (AH) الذي يضمن مصداقية البيانات وسلامتها، وحمولة التغليف الأمني (ESP) التي توفر التشفير الكامل للبيانات. كما يستخدمIPsecبروتوكولات تبادل المفاتيح الآمنة مثل IKE و IKEv2لضمان إعداد العلاقة الأمنية بين الطرفين. من مزاياه أنه يعمل في الخلفية دون تدخل المستخدم، ويوفر أمانًا قويًا على مستوى الشبكة بالكامل[2].

ثالثاً: بروتوكولSSH

SSH أو Secure Shell هو بروتوكول يُستخدم لتأمين الجلسات عن بُعد، ويتيح للمستخدمين التحكم الكامل في الأجهزة الطرفية عبر الشبكات غير الآمنة. يُعد SSH بديلًا آمنًا عن بروتوكولات غير مشفّرة مثل .Telnet يعمل على إنشاء قناة اتصال مشفّرة باستخدام خوارزميات تبادل المفاتيح مثل-Diffie Hellmanوتشفير الجلسات باستخدام خوارزميات مثل .AES. كما يعتمد على المصادقة الثنائية (مفتاح عام/خاص أو كلمة سر)، ويوفر نقلًا آمنًا للملفات وتنفيذ أوامر عن بُعد، ما يجعله أداة لا غنى عنها في إدارة الخوادم[3].

[1] **محمد عبد الحميد النجار**، *مرجع سابق*، ص. 111.
[2] **عبد الحميد النجار**، *مرجع نفسه*، ص. 113.
[3] **الطاهر، محمد علي**،*أمن الشبكات وتقنيات الحماية*.دار الفكر العربي، الطبعة الأولى، مصر، 2019، ص. 102.

رابعاً: بروتوكولDNSSEC

يمثّل DNSSEC امتدادًا لبروتوكول DNS الأصلي، ويهدف إلى تأمين نظام أسماء النطاقات عبر إضافة آليات تحقق رقمية تعتمد على التوقيعات الرقمية. تُستخدم مفاتيح عامة وخاصة لضمان أن الاستجابات من خوادم DNS لم يتم تعديلها أو تزويرها. كما يُمكّن المستخدم من التحقق من صحة أصل البيانات وتجنب هجمات تزوير DNS مثل ."DNS Spoofing" يُعد من الأدوات الجوهرية لتعزيز الثقة في البنية التحتية للإنترنت[1].

الفرع الثاني: أدوات الحماية التقنية

أولاً: الجدران النارية(Firewalls)

الجدار الناري هو أول خط دفاع في بنية أمن الشبكات، يُستخدم للتحكم في تدفق الحزم بين الشبكات بناءً على قواعد محددة مسبقًا. تتنوع أنواعه بين تصفية الحزم البسيطة، والجدران النارية ذات الحالة (Stateful Inspection)، وبوابات التطبيقات التي تفحص المحتوى على مستوى الطبقات العليا. يعمل الجدار الناري على منع الاتصالات غير المرغوب فيها، ويسمح فقط بالحركة المرخصة وفقًا للسياسات الأمنية المعتمدة. ومن الضروري تحديث قواعد الجدار الناري باستمرار وفق تحليل المخاطر والتهديدات الجديدة.

ثانياً: نظم كشف ومنع التسلل(IDS/IPS)

تُستخدم نظم كشف التسلل (IDS) لمراقبة الشبكات والنظم من أجل رصد الأنشطة غير الطبيعية أو الهجمات المحتملة، وتنبه المسؤولين بوجود تهديدات. بينما تتخذ نظم منع التسلل (IPS) خطوة إضافية من خلال تنفيذ إجراءات تلقائية مثل منع الاتصال المشبوه أو حظر عناوين IP ضارة. هذه النظم تعتمد

[1] **عبد السلام، أحمد**،*بروتوكولات الأمان في شبكات الإنترنت*.دار الأشجار للنشر، الطبعة الثانية، الأردن، 2018، ص. 78.

على قواعد سلوك، أو نماذج تعلم آلي، أو تحليل التواقيع لرصد الهجمات المعروفة والمجهولة. يُعد استخدامها ضروريًا لتقليل زمن الاستجابة للهجمات ورفع درجة أمان الشبكة[1].

ثالثاً: أنظمة إدارة المعلومات والأحداث الأمنية(SIEM)

SIEMهو نظام مركزي لجمع وتحليل السجلات والبيانات الأمنية من مختلف أجهزة الشبكة. يُساعد على اكتشاف الأنماط المشبوهة وتحليل الحوادث الأمنية في الزمن الحقيقي. يدمج SIEM بين تقنيات جمع الأحداث(Log Collection) ، وتوحيد التنبيهات، والتحليل السياقي، ما يتيح للمؤسسات رؤية شاملة على حالة الأمن السيبراني، وتحقيق الامتثال للمعايير التنظيمية، وتحسين سرعة الاستجابة للحوادث.

رابعاً: برامج مكافحة البرمجيات الخبيثة(Anti-Malware/AV)

برامج الحماية من الفيروسات والبرمجيات الخبيثة تمثّل خط الدفاع الأساسي للمستخدم النهائي. تقوم بفحص الملفات والسلوكيات على الأجهزة لاكتشاف البرمجيات الضارة مثل الفيروسات، وRansomware، والديدان، وأحصنة طروادة. تعتمد هذه البرامج على قواعد بيانات تواقيع تُحدث باستمرار، كما تستخدم خوارزميات الذكاء الاصطناعي لتحديد البرمجيات غير المعروفة بناءً على السلوك. توفر أيضًا خاصيات متقدمة مثل العزل التلقائي، والتحليل السحابي، والمراقبة في الزمن الحقيقي[2].

خامساً: أنظمة منع فقدان البيانات(DLP)

تُستخدم أنظمة منع فقدان البيانات (DLP) لرصد البيانات الحساسة والتحكم في طرق استخدامها وانتقالها. تقوم بتحليل المحتوى والسياق لمنع نسخ أو إرسال البيانات الحساسة إلى خارج الشبكة سواء عبر البريد الإلكتروني، أو وحداتUSB ، أو الشبكة السحابية. تُعد DLP ضرورية للامتثال للسياسات

[1] **الزهيري، خالد**.*تقنيات الأمن السيبراني*.دار الجامعات للنشر، الطبعة الأولى، السعودية، 2020، ص. 145.
[2] **الياس، يوسف**.*الجدران النارية وأنظمة الحماية*.دار المعرفة، الطبعة الأولى، لبنان، 2017، ص. 64.

القانونية والمعايير الصناعية مثل GDPR أوHIPAA ، كما تساعد على تقليل المخاطر المرتبطة بالتسريب الداخلي أو الأخطاء البشرية.

سادساً: الشبكات الخاصة الافتراضية(VPN)

VPNتوفر وسيلة آمنة لإنشاء قناة اتصال مشفّرة بين مستخدم أو فرع بعيد وخوادم المؤسسة، عبر شبكة الإنترنت العامة. تستخدم بروتوكولات تشفير مثلIPSecأو SSL/TLS لضمان سرّية البيانات، وتوفر طبقة إضافية من الحماية للمستخدمين أثناء تصفح الإنترنت أو الوصول إلى الموارد الحساسة عن بُعد. كما تسمح VPN بإخفاء عنوان IP الحقيقي للمستخدم، وتوفر حماية من التنصت أو اعتراض الاتصالات، ما يجعلها خيارًا أساسيًا في البيئات المرنة والعمل عن بُعد[1].

المطلب الثالث: دور القطاع الخاص مزودي الأنظمة وشركات الأمن السيبراني

يلعب القطاع الخاص دورًا حيويًا في تعزيز الأمن السيبراني من خلال تطوير البنى التحتية الأمنية، توفير الحلول التقنية المتخصصة، تقديم خدمات الكشف عن التهديدات والاستجابة للحوادث، تقديم الاستشارات والتدقيق الأمني، توفير التدريب وبناء القدرات، وتعزيز الشراكات بين القطاعين العام والخاص.

الفرع الأول:دور الشركات في تعزيز القدرات الحكومية في التصدي للتهديدات السيبرانية

تعمل الشركات المتخصصة مثل Cisco و Palo Alto Networksو Fortinetعلى تطوير حلول متقدمة للجدران النارية وأنظمة التشفير والنقل الآمن، مما يعزز من قدرة الشبكات الحكومية والمؤسساتية على التصدي للتهديدات السيبرانية .تستخدم هذه الشركات تقنيات مثل التفتيش العميق للحزم والذكاء

[1] **صالح، منى**.*كشف ومنع التسلل في الشبكات*.دار النهضة العربية، الطبعة الأولى، تونس، 2018، ص. 89.

الاصطناعي لتحليل السلوكيات الشبكية، مما يساهم في تحسين أداء الشبكات وزيادة فعاليتها في مواجهة الهجمات الإلكترونية [1]

كما تقدم شركات الاستشارات مثل Deloitte وPwC و KPMG خدمات استشارية متخصصة في مجال الأمن السيبراني، بما في ذلك التوافق مع المعايير العالمية مثل ISO 27001 وNIST CSF، وتنفيذ اختبارات الاختراق وتقييم الثغرات، مما يساعد المؤسسات على تحسين وضعها الأمني والتأكد من التزامها بالمتطلبات التنظيمية [2].

توفر الشركات أيضًا برامج تدريبية متخصصة في مجال الأمن السيبراني، بما في ذلك ورش العمل والدورات التدريبية في أمن الشبكات، تأمين التطبيقات، وتحليل البرمجيات الخبيثة، مما يساهم في رفع مستوى وعي الأفراد والفرق التقنية وقدرتهم على التعامل مع التهديدات السيبرانية.

تعزز الشراكات بين القطاعين العام والخاص من خلال تبادل المعلومات والتعاون في مجال الأمن السيبراني، مما يساهم في تحسين الاستجابة الجماعية للتهديدات السيبرانية وتعزيز الحماية على مستوى الاقتصاد الرقمي الوطني .

الفرع الثاني: تحديات الشركات في مجال الأمن السيبراني

على الرغم من التحديات التي تواجهها الشركات الصغيرة والمتوسطة في مجال الأمن السيبراني، مثل نقص الموارد والقدرات الفنية،

إلا أن التوقف عن العمل وفقدان الإنتاجية هي أكبر مصادر القلق بين مشاكل الأعمال الناجمة عن عدم فعالية أمن تكنولوجيا المعلومات. ويعود السبب الأساسي لمواجهة الشركات لهذه المشكلة هو الوقت الطويل الذي تحتاجه لاكتشاف التهديدات ومعالجتها.

[1] **الصياد، كوثر**.*أساسيات التشفير في بروتوكولات الأمان*.دار الحكمة، الطبعة الأولى، العراق، 2019، ص. 131.
[2] **منصور، إبراهيم**.*إدارة المعلومات والأحداث الأمنية (SIEM)*. دار الرائد الجامعي، الطبعة الأولى، مصر، 2021، ص. 57.

إلا أن هناك فرصًا لتطوير حلول محلية وتشجيع الابتكار في هذا المجال، مما يساهم في تقليل الاعتماد على التكنولوجيا الأجنبية وتعزيز القدرات المحلية [1] .

يلعب القطاع الخاص دورًا لا غنى عنه في بناء منظومة أمنية متكاملة وقابلة للتطور مع تقادم التهديدات .ويعتمد نجاح هذا الدور على تعميق الشراكات مع القطاع الحكومي، وتحفيز الابتكار المحلي، وتوسيع برامج التدريب وبناء القدرات .هكذا تتبلور العلاقات التكاملية اللازمة لحماية الفضاء السيبراني للدول والمؤسسات على السواء.

المطلب الرابع: آليات التعاون الدولي في تبادل المعلومات والإنذار المبكر

في ظل الطبيعة المتغيرة والمتسارعة للتهديدات السيبرانية، لم تعد أي دولة قادرة على حماية فضائها الرقمي بشكل منفرد، حيث أضحت التهديدات تتخطى الحدود الجغرافية وتستهدف البنى التحتية الحيوية والشبكات السيادية باستخدام تقنيات متطورة ومنصات مجهولة المصدر، يصعب تعقب مصدرها أو تحديد الجهات الفاعلة بدقة. وقد باتت هذه التهديدات تمثل خطرًا عابرًا للحدود، يهدد ليس فقط الأمن الرقمي للدول، وإنما أيضًا استقرارها السياسي والاقتصادي. من هنا، لم يعد التعاون الدولي في هذا المجال خيارًا تكتيكيًا، بل ضرورة إستراتيجية لا غنى عنها لضمان الأمن السيبراني على الصعيدين الوطني والعالمي. فالهجمات التي طالت أكثر من دولة، مثل هجوم "Stuxnet" الذي استهدف البنية التحتية النووية، أو هجوم "SolarWinds" الذي اخترق سلاسل التوريد البرمجية وأصاب شبكات حكومية وشركات متعددة الجنسيات، تُعد دلائل قاطعة على أن الحلول الأحادية لم تعد مجدية، وأن المواجهة الفاعلة تتطلب استجابة جماعية منسقة[2].

الفرع الأول:الإنذار المبكر السيبراني

[1] **صالح، منى**،مرجع *سابق*، ص. 91.

[2] **الجبوري، فلاح حسن**، *الأمن السيبراني ومجتمع المعلومات*، دار الثقافة للنشر، الطبعة الأولى، الأردن، 2020، ص. 91

برز مفهوم "الإنذار المبكر السيبراني" بوصفه إحدى أهم الأدوات الوقائية في مواجهة الهجمات الإلكترونية. يشير هذا المفهوم إلى منظومة مؤسسية متكاملة تعتمد على رصد المؤشرات الأولية للتهديدات، وتشارك هذه المعلومات مع الشركاء المحليين والدوليين بشكل فوري، بما يسمح بالتعامل السريع مع الخطر قبل أن يتفاقم. وتُدار هذه المنظومة عادة من خلال مراكز الاستجابة للحوادث الأمنية المعروفة باسمCSIRTsأوCERTs، وهي كيانات وطنية أو قطاعية متخصصة في تحليل التهديدات والتصدي للحوادث السيبرانية. وتعتمد هذه الفرق على مصادر استخبارية متقدمة، مثل قواعد بيانات الهجمات السابقة، تحليل البرمجيات الخبيثة، وأنماط حركة الشبكة غير الاعتيادية، لرصد التهديدات المستقبلية والاستعداد لها بشكل استباقي. كما تسهم في تفعيل خطط الطوارئ، وتحليل نقاط الضعف، وعزل الأنظمة المصابة، ومنع امتداد الهجوم إلى شبكات أوسع[1].

الفرع الثاني:آليات التعاون الدولي

تأخذ آليات التعاون الدولي أشكالًا متعددة، أبرزها **الاتفاقيات الثنائية** أو المتعددة الأطراف، التي تُوقعها الدول بهدف تنظيم تبادل المعلومات وتنسيق الجهود. وتُدرج هذه الاتفاقيات بنودًا تتعلق بتوحيد تعريف الجرائم الإلكترونية، وتحديد آليات التبليغ المشترك الفوري، وحفظ سرية البيانات المتبادلة، والتعاون القضائي في التحقيقات العابرة للحدود. وتُعد "اتفاقية بودابست" حول الجرائم السيبرانية، الصادرة عن مجلس أوروبا عام 2001، من أهم النماذج العالمية في هذا الصدد، إذ جمعت أكثر من 65 دولة حول معايير موحدة للتعامل مع الجريمة الرقمية، وساهمت في إنشاء شبكات تعاون فعالة بين أجهزة إنفاذ القانون والمؤسسات التقنية.

إلى جانب الاتفاقيات، تلعب الشبكات المتخصصة ومراكز التنسيق الإقليمية والدولية دورًا جوهريًا في تيسير التعاون المعلوماتي، لا سيما في لحظات الأزمات السيبرانية. ومن بين هذه الشبكات نذكر

[1] **صالح، منى محمد،** *التهديدات الإلكترونية والتعاون الأمني الدولي*، دار اليازوري العلمية، الطبعة الثانية، الأردن، 2021، ص. 135

منتدى فرق الاستجابة للحوادث الأمنيةFIRST ، الذي يضم أكثر من 600 فريق حول العالم، ويُعد منصة ديناميكية لتبادل المؤشرات الفنية والتحذيرات في الوقت الفعلي، مما يُعزز من سرعة الاستجابة ويقلل من آثار الهجمات. كما يُعتبر الاتحاد الأوروبي من أبرز الفاعلين في هذا المجال، حيث يدير عبر وكالة ENISA منصةCyber Europe ، وهي تمرين دوري لمحاكاة الهجمات السيبرانية الكبرى واختبار جاهزية الأنظمة الأوروبية. وعلى الصعيد العربي، خطت بعض الدول خطوات مهمة، حيث أنشأ الاتحاد الدولي للاتصالات "المركز الإقليمي للأمن السيبراني" في سلطنة عمان، ليعمل كمنصة تدريب واستجابة للحوادث على المستوى العربي، ويوفر قاعدة لتنسيق الجهود بين الفرق الوطنية[1].

ويُعد تبادل المعلومات الاستخبارية المتعلقة بالتهديدات أحد أبرز جوانب التعاون المتقدم، حيث يتيح للدول والمؤسسات الاطلاع على مؤشرات الاختراق المعروفة(IoCs) ، والأدوات والتقنيات التي يستخدمها المهاجمون(TTPs) ، وأحيانًا تحديد الجهات الفاعلة التي تقف وراء الهجمات. وتُستخدم في هذا المجال منصات معيارية مثل STIX و TAXIIالتي تسمح بتبادل المعلومات بشكل آلي وآمن بين الأطراف. إلا أن هذا النوع من التعاون يظل حساسًا للغاية، نظرًا لما يتطلبه من مستوى عالٍ من الثقة الرقمية بين الدول، بالإضافة إلى وجود ضمانات قانونية تقي من استخدام المعلومات في غير أهدافها الأمنية، أو توظيفها سياسيًا أو استخباراتيًا ضد الدول المشاركة.

وقد ظهرت خلال السنوات الماضية عدة نماذج تطبيقية ناجحة تؤكد فعالية التعاون الدولي في هذا المجال. فحلف شمال الأطلسي "الناتو"، على سبيل المثال، أنشأ مركز الامتياز للدفاع السيبراني في إستونيا بعد تعرضها لهجوم واسع النطاق عام 2007، ليكون منصة لتنسيق وتبادل الإنذار المبكر بين دول الحلف. ويُعتبر هذا المركز حاليًا من أبرز مؤسسات البحث والتدريب وتبادل البيانات السيبرانية على المستوى الدولي. وفي المنطقة الخليجية، وقعت دول مجلس التعاون الخليجي اتفاقية مشتركة لتبادل

[1] **أحمد، سامر عبد الله**، نظم الإنذار المبكر في الأمن السيبراني، مكتبة المجتمع العربي، مصر، 2019، ص. 45

البيانات والمعلومات الأمنية، بدعم من المركز الإقليمي في مسقط، وأسست منظومة موحدة لفرق الاستجابةCSIRT ، تهدف إلى تعزيز الجاهزية والاستجابة السريعة في حال وقوع هجمات إقليمية. وعلى المستوى الآسيوي، يربط مشروع APCERT فرق الاستجابة لدول آسيا والمحيط الهادئ، ضمن آلية تقنية موحدة لتبادل الإنذارات والردود على الحوادث، مع التركيز على الهجمات عابرة الحدود وسرعة التنسيق الإقليمي[1].

ورغم التقدم الكبير في بناء هذه المنظومات، إلا أن التعاون الدولي في مجال الأمن السيبراني لا يزال يواجه تحديات كبيرة، أولها غياب الثقة بين بعض الدول، خصوصًا تلك التي تعيش توترات جيوسياسية أو تتنافس في الفضاء السيبراني. كما أن تباين السياسات الوطنية المتعلقة بالخصوصية، وحماية البيانات، وحرية التعبير، يمثل عائقًا أمام التوافق على معايير موحدة. ومن جهة أخرى، لا تزال هناك فجوة في توحيد المصطلحات التقنية، والبروتوكولات التشغيلية، الأمر الذي يعقد من فهم مشترك لطبيعة التهديدات وأساليب الاستجابة. وتخشى بعض الدول من الإفصاح عن الهجمات التي تتعرض لها خشية فقدان هيبتها أو الاعتراف بوجود ثغرات في بنيتها التحتية الحيوية.

وبناءً على ما سبق، فإن تعزيز فعالية التعاون الدولي في مجال تبادل المعلومات والإنذار المبكر يتطلب اتخاذ جملة من التوصيات العملية. أولًا، ينبغي إنشاء منصة عربية موحدة تُعنى برصد وتبادل الإنذارات السيبرانية، وتربط بين فرق الاستجابة في الدول العربية بشكل آمن وسريع. ثانيًا، يجب تطوير آلية موحدة لتصنيف الحوادث السيبرانية وتقييم درجة خطورتها وفق إطار إقليمي يسمح بمقارنة البيانات وتحليل الاتجاهات. ثالثًا، من المهم تعزيز تبادل الخبرات التقنية بين الفرق الوطنية، عبر تنظيم تدريبات وتمارين محاكاة دورية، ترفع من مستوى الجاهزية وتبني الثقة المتبادلة. وأخيرًا، يجب تفعيل التشبيك

[1] *CCDCOE, National Cyber Security Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence, 2021.

المستمر بين مراكز الأمن السيبراني الوطنية، عبر بروتوكولات تشغيل موحدة وأطر قانونية شفافة، لتوحيد الجهود ومواجهة التهديدات العابرة بشكل متكامل.

المبحث الثاني: الإجراءات الجنائية و التحقيقية

في ظل التنامي المتسارع للجريمة السيبرانية وتعدد صورها وتطور أدواتها، لم تعد النظم القانونية التقليدية قادرة وحدها على ملاحقة الجناة وتحقيق الردع، الأمر الذي استدعى إعادة النظر في الإجراءات الجنائية والتحقيقية، سواء من حيث الآليات أو المفاهيم أو التشريعات. فالجريمة المعلوماتية تتسم بخصوصية تكنولوجية معقدة، تتطلب جهات إنفاذ القانون والمحققين المتخصصين القادرين على التعامل مع الأدلة الرقمية، وفهم آليات الاختراق والتشفير والتزوير الإلكتروني. كما أن التحقيق في هذا النوع من الجرائم يتطلب توازنًا دقيقًا بين احترام الحريات العامة والخصوصية من جهة، وفعالية الإجراءات الجنائية من جهة أخرى. وعليه، تتجه الأنظمة القانونية الحديثة إلى تطوير مسارات جنائية جديدة تتماشى مع هذه التحديات المستجدة، تشمل على وجه الخصوص تجريم الأفعال الإلكترونية، وضبط آليات التحري الرقمي، وتعزيز التعاون القضائي مع جهات إنفاذ القانون الدولية، بما يحقق الفعالية المطلوبة في مواجهة هذه الجرائم المتطورة.

المطلب الأول: استراتيجيات جمع الأدلة الرقمية وتحليلها(Digital Forensics)

يُعد جمع الأدلة الرقمية وتحليلها من أبرز التحديات التي تواجه أجهزة العدالة الجنائية في العصر الرقمي، إذ أصبحت الحواسيب والشبكات ومختلف الأجهزة الذكية ساحةً افتراضية لاقتراف الجرائم، مما يستدعي تطوير أدوات وتقنيات دقيقة لاكتشاف الأثر الرقمي وتتبع الفاعلين. إن التحقيق في الجرائم السيبرانية يختلف عن نظيره التقليدي؛ فالأدلة هنا غير ملموسة، سريعة الزوال، وقد تكون موزعة عبر خوادم موجودة في دول متعددة، وهو ما يفرض على المحققين امتلاك كفاءات تقنية ومعرفية متقدمة. كما

أن عملية جمع الأدلة الرقمية تخضع لإجراءات دقيقة تحكمها قواعد قانونية وتقنية لضمان سلامتها ومصداقيتها أمام القضاء، ذلك أن أي خلل في سلسلة الحيازة أو أدنى تلاعب قد يؤدي إلى استبعاد الدليل أو الطعن فيه.

الفرع الأول: تقنيات جمع وتحليل الجريمة الالكترونية

تبدأ عملية التحري الرقمي منذ لحظة الاشتباه في وقوع الجريمة الإلكترونية، حيث يعمل فريق مختص على تأمين مكان الجريمة الافتراضي دون المساس بسلامة الأدلة الرقمية، باستخدام أدوات تقنية متخصصة مثل برامج تصوير القرص الصلب (Disk Imaging) وتقنيات تحليل الذاكرة الحية (Live Memory Analysis). الهدف من هذه المرحلة هو المحافظة على بيئة البيانات كما هي، والتقاط صورة دقيقة لنظام التشغيل والبرمجيات المستخدمة، وسجلات الدخول، وكلمات السر المحفوظة، وحتى الملفات المحذوفة أو المشفرة. يتم ذلك وفق تسلسل زمني صارم يضمن ما يسمى بـ "سلسلة الحيازة (Chain of Custody)"، وهي التي تُوثق من خلالها جميع مراحل التعامل مع الدليل، بدءًا من مصادرته مرورًا بتخزينه وتحليله، وانتهاءً بتقديمه أمام المحكمة[1].

الفرع الثاني: ضوابط احترام خصوصية الأشخاص والبيانات

من الناحية القانونية، تُلزم غالبية التشريعات بضرورة احترام خصوصية الأفراد وحرمة البيانات أثناء جمع الأدلة، مما يفرض على الجهات المختصة الحصول على إذن قضائي مسبب قبل الدخول إلى الأجهزة أو تفتيش حسابات البريد الإلكتروني أو تخزين الخدمات السحابية. وقد أقر التشريع الجزائري، بموجب القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، الخاص بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بآليات خاصة للتفتيش الإلكتروني وفق ضوابط تحمي الحق في السرية من جهة، وتكفل فعالية الإجراءات من جهة أخرى. كما نصت المادة 60 مكرر

[1] بدر، حسن عبد الفتاح، **التحقيق الجنائي الرقمي**، دار الفكر الجامعي، الطبعة الأولى، مصر، 2018، ص. 22

من قانون الإجراءات الجزائية على إمكانية إجراء تفتيش إلكتروني بواسطة أعوان مختصين، شريطة صدور إذن مسبق عن وكيل الجمهورية أو قاضي التحقيق[1].

وتجدر الإشارة إلى أن أهمية الأدلة الرقمية في الإثبات لم تعد تقتصر على قضايا الجرائم الإلكترونية البحتة، بل امتدت إلى مختلف أنواع الجرائم، مثل الإرهاب، والجرائم المالية، والتحرش الإلكتروني، والتشهير، والابتزاز، مما يجعلها اليوم عنصراً جوهرياً في بنية الإثبات الجنائي المعاصر. ولذلك، أصبحت معظم الدول تؤسس وحدات تحقيق رقمية داخل الشرطة أو النيابة، وتُدخل في مناهج تكوين القضاة وأعوان الضبط القضائي مواد متخصصة في علوم الأدلة الرقمية وأساليب استخراجها وتحليلها.

أما على الصعيد الدولي، فقد ساهمت اتفاقية بودابست بشأن الجريمة السيبرانية في توحيد المبادئ العامة المتعلقة بجمع الأدلة الرقمية وتبادلها، ووفرت إطاراً قانونياً لتسهيل التعاون القضائي بين الدول في هذا المجال، لاسيما في ظل التحديات التقنية المرتبطة بتخزين البيانات عبر الحدود، وهو ما يتطلب في كثير من الحالات استجابة فورية عبر قنوات رسمية بين الدول لمنع ضياع الأدلة أو فقدان أثر الجناة[2].

المطلب الثاني: إجراءات الضبط والحجز الإلكتروني

مع تطور التكنولوجيا وظهور فضاء الإنترنت كبيئة خصبة لارتكاب الجرائم، ظهرت الحاجة الملحة إلى تكييف إجراءات الضبط والحجز الجنائي مع طبيعة الجريمة السيبرانية، التي تختلف جوهريًا عن الجرائم التقليدية. ذلك أن أدوات الجريمة الرقمية غالبًا ما تكون غير مادية، مثل البرمجيات، البيانات، الرسائل الإلكترونية، أو المواقع الإلكترونية، وبالتالي فإن عملية الضبط في هذا السياق تتطلب وسائل تقنية خاصة، وتدخلاً سريعًا للحفاظ على الدليل الرقمي الذي يمكن أن يُمحى أو يُعدل في ثوانٍ معدودة. إن الضبط الإلكتروني يشير إلى تلك العملية التي تقوم بها السلطات المختصة برصد، وتحديد، وتجميع،

[1] بن لطرش، رشيد، **الجريمة المعلوماتية في القانون الجزائري**، دار هومة للنشر، الطبعة الثانية، الجزائر، 2020، ص. 143
[2] سليم، عبد الحكيم، **قانون الإجراءات الجزائية الجزائري: شرح وتحليل**، دار الهدى، الطبعة الرابعة، الجزائر، 2021، ص. 202

وتأمين الأدلة الرقمية المتعلقة بجريمة محتملة من أجهزة إلكترونية أو شبكات رقمية، دون المساس بمحتواها أو إفساد خصائصها التقنية.

الفرع الأول:شرعية الضبط الالكتروني للجريمة الالكتروني

في السياق الإجرائي، يُعد الضبط الإلكتروني إجراءً تمهيديًا بالغ الحساسية، ويخضع في أغلب التشريعات لمبدأ الشرعية، بحيث لا يجوز تنفيذه إلا بناءً على إذن قضائي، أو في حالات التلبس المنصوص عليها قانونًا. وقد نص القانون الجزائري، من خلال المادة 60 مكرر من قانون الإجراءات الجزائية، على إمكانية إجراء تفتيش وضبط للمحتوى الإلكتروني من قبل ضباط الشرطة القضائية، شرط توفر إذن قضائي مسبق، وضمن حدود الزمان والمكان والموضوع المحددة. كما أشار القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلى أن الجهات المختصة يمكنها اللجوء إلى تقنيات الحجز الإلكتروني وفق إجراءات دقيقة تضمن شرعية العملية وسلامة الأدلة[1].

تتضمن عملية الضبط الرقمي عادةً حجز الحواسيب أو الهواتف الذكية أو وسائط التخزين الأخرى التي تحتوي على بيانات يُشتبه في صلتها بالجريمة. وتتم هذه العملية بواسطة مختصين يستخدمون أدوات دقيقة، مثل أجهزة النسخ القضائي (Forensic Imaging Tools) التي تُستخدم لأخذ صورة طبق الأصل للقرص الصلب دون التأثير على البيانات الأصلية، وهو ما يُعرف بمبدأ "النسخ دون تعديل". كما يُشترط توثيق سلسلة الحيازة (Chain of Custody) لكل جهاز أو ملف تم ضبطه، ابتداءً من لحظة اكتشافه إلى حين تقديمه كدليل أمام المحكمة، مما يُحافظ على مصداقية الأدلة الرقمية.

الفرع الثاني: صعوبات وتحديات الضبط الالكتروني

[1]سليم، عبد الحكيم، **قانون الإجراءات الجزائية الجزائري: شرح وتحليل**، دار الهدى، الطبعة الرابعة، الجزائر، 2021، ص. 205

إن من أبرز التحديات التي تواجه الضبط الإلكتروني هي طبيعة البيانات التي يمكن تخزينها في خدمات سحابية (Cloud Services) تقع خارج حدود الدولة، ما يُصعب عملية الحجز ويثير إشكالات متعلقة بالاختصاص القضائي الدولي. في مثل هذه الحالات، تلجأ الدول إلى التعاون القضائي الدولي وتفعيل الاتفاقيات الثنائية ومتعددة الأطراف لتبادل المعلومات والحصول على الأدلة الرقمية. ويُعد ذلك من المسائل التي لا تزال بحاجة إلى تطوير تشريعي واتفاقي على المستوى الدولي، خاصة في ظل السرعة الكبيرة لتطور التكنولوجيا وعدم تكافؤ القدرات التقنية بين الدول[1].

من جهة أخرى، فإن الحجز الإلكتروني يجب أن يُراعي مبدأ التناسب والضرورة، بحيث لا يُفضي إلى انتهاك خصوصيات الأفراد غير المعنيين بالجريمة، أو يشمل بيانات ليست لها علاقة مباشرة بالفعل الإجرامي. وفي هذا الإطار، يبرز دور القضاء في مراقبة مدى احترام الضبط لمبادئ العدالة وحماية الحقوق الأساسية للأشخاص، لا سيما الحق في الخصوصية وسرية المراسلات الرقمية. وتُظهر السوابق القضائية أن كثيرًا من القضايا الإلكترونية تم الطعن فيها بسبب عدم احترام هذه الإجراءات الجوهرية، ما يُؤكد على ضرورة التأهيل المتخصص للمحققين والضبطية القضائية في المجال الرقمي.

وقد أدركت الأنظمة المقارنة أهمية ضبط وتنظيم الحجز الإلكتروني بدقة، حيث نص التشريع الفرنسي مثلاً على إجراءات مفصلة في قانون الإجراءات الجنائية بشأن تفتيش الأنظمة المعلوماتية وحجز محتوياتها، بما في ذلك التحقق من صلاحيات النفاذ، وتسجيل عمليات الدخول، واستخدام خبير تقني أثناء التفتيش. أما على الصعيد العربي، فقد بدأ العديد من الدول في إدراج نصوص صريحة تنظم هذه الإجراءات، كما هو الحال في قانون مكافحة الجرائم الإلكترونية الأردني والمغربي والسعودي[2].

وتكمن أهمية الحجز الإلكتروني في كونه يسمح بالحصول على أدلة قد تكون حاسمة في إثبات الجريمة أو نفيها، خاصة عندما يتعلق الأمر بتحديد مصادر الاختراق أو مواقع الجناة أو الرسائل

[1] بن لطرش، رشيد، **مرجع سابق**، ص190

[2] الربيعي، جاسم محمد، **الإجراءات الجنائية في الجريمة المعلوماتية**، دار الثقافة للنشر، الطبعة الأولى، الأردن، 2019، ص. 112

المتبادلة المتعلقة بالواقعة. ولهذا فإن هذا الإجراء يُمثل اليوم محورًا أساسيًا في بنية التحقيق الرقمي، ويُعد من أكثر مراحل الإجراءات الجنائية التقنية التي تتطلب دقة وضمانات.

المطلب الثالث: التعاون بين قوات الأمن والقضاء

يُعد التعاون بين أجهزة الأمن والقضاء حجر الزاوية في فعالية مكافحة الجريمة الإلكترونية، نظراً للطابع المعقد والعابر للحدود الذي تتسم به هذه الجرائم. هذا التعاون يتجلى في وجود قنوات اتصال فعالة ومؤطرة قانونيًا تسمح بتبادل المعلومات بسرعة، سواء على مستوى الوقائع أو الأدلة الرقمية. فكلما كانت قنوات الاتصال واضحة ومباشرة، كانت الاستجابة الأمنية والقضائية أسرع وأكثر دقة، لا سيما في الحالات التي تتطلب تدخلاً عاجلاً مثل جرائم الابتزاز الإلكتروني أو اختراق أنظمة الدولة.

الفرع الأول: تشكيل فرق عمل مختلطة

تتمثل أولى مظاهر هذا التعاون في تشكيل فرق عمل مختلطة بين النيابة العامة ومصالح الأمن السيبراني، تكون مهمتها التنسيق المسبق حول طرق التحري، ضمانًا لاحترام الإجراءات القانونية المنصوص عليها في قانون الإجراءات الجزائية. ويسمح هذا الأسلوب بالكشف عن الجريمة الرقمية في مراحلها الأولى من خلال توظيف تقنيات التحليل الآني للبيانات(real-time data analytics) ، وهو ما يدعم فعالية الأدلة عند عرضها أمام المحكمة[1].

كما تعتمد بعض الأنظمة القانونية على إنشاء "غرف عمليات موحدة" بين الأمن والقضاء، مزودة بوسائل الاتصال المؤمنة ونظم إدارة البيانات، لتسهيل نقل المعلومات بشكل لحظي ومؤمن، لا سيما في ظل التهديدات المتزايدة المتعلقة بالاختراق أو تسريب الملفات الحساسة. ومن جهة أخرى، يُعتبر تبادل

[1]سامي الشحي، **أمن المعلومات والعدالة الجنائية**، دار جامعة الإمارات للطباعة، الطبعة الأولى، الإمارات، 2022، ص. 77.

قواعد البيانات المتعلقة بالسوابق العدلية، والمعلومات التقنية عن أدوات الجريمة الرقمية، من الآليات الجوهرية التي تساهم في تسريع مجريات التحقيق[1].

الفرع الثاني: وضع اتفاقيات وطنية ودولية

ويأخذ التعاون أحياناً شكل اتفاقيات ثنائية أو متعددة الأطراف، على الصعيدين الوطني والدولي، تسمح بتبادل المعلومات القضائية بطريقة منظمة وفعالة. وفي هذا السياق، تُبرز اتفاقية بودابست أهمية وجود أطر تشريعية وطنية تُلزم الأجهزة المعنية بالاحتفاظ بالبيانات وتبادلها عند الطلب القضائي، وفقًا للضمانات القانونية. كما أن التجربة الجزائرية بدأت تسير في هذا الاتجاه من خلال رقمنة المعاملات القضائية، وتفعيل دور الضبطيات القضائية الإلكترونية في التنسيق بين الشرطة والقضاة[2].

هذا التكامل بين الأمن والقضاء يتطلب كوادر بشرية مدربة، قادرة على التعامل مع البرمجيات الجنائية، وعلى فهم الجوانب التقنية المرتبطة بالأدلة الرقمية. ويُشترط كذلك تحديث القوانين والإجراءات لتشمل الخصوصيات الرقمية، وضمان عدم التداخل أو التعارض بين الصلاحيات الأمنية والسلطات القضائية، حتى لا يُمس بمبدأ المشروعية وحماية الحريات.

المطلب الرابع متطلبات الإثبات والمحاكمة في المنازعات الإلكترونية

تُعد مرحلة الإثبات في المنازعات الإلكترونية من أكثر المراحل تعقيدًا، وذلك بالنظر إلى طبيعة الأدلة المستعملة في هذا النوع من القضايا، والتي تكون غالبًا رقمية وغير مادية. ومن ثم، فإن إثبات الجريمة أو المسؤولية في النزاع الإلكتروني يقتضي توفر إطار قانوني دقيق، إلى جانب إمكانيات تقنية متقدمة تتيح استخراج، تأمين، وتحليل الأدلة الرقمية بطريقة تحفظ سلامتها القانونية وتضمن حجيتها أمام القضاء.

الفرع الاول: الاعتراف القانوني بالأدلة الرقمية

[1]محمد الطيب بن يسعد، **التحقيق الجنائي في الجرائم السيبرانية**، دار الخلدونية، الطبعة الثانية، الجزائر، 2021، ص. 134.
[2]نجيب الغول، **تكنولوجيا المعلومات ومكافحة الجريمة الإلكترونية**، دار اليازوري، الطبعة الأولى، الأردن، 2020، ص. 99

وهو أول متطلبات الإثبات في هذا السياق ، مثل البريد الإلكتروني، سجلات الدخول، بصمات الإنترنت، وتسجيلات كاميرات المراقبة المرتبطة بالشبكات الذكية. وتفرض هذه الأدلة ضرورة اعتماد آليات تحقق تقنيّة تضمن نسبتها إلى أطرافها، مثل استخدام التوقيع الرقمي والبروتوكولات المشفّرة التي تُثبت سلامة الوثائق وعدم تعديلها.

الفرع الثاني: احترام إجراءات جمع الأدلة الرقمية

أما ثاني المتطلبات فهو **احترام إجراءات جمع الأدلة الرقمية**، إذ يجب أن تتم عبر أشخاص مؤهلين قانونيًا وتقنيًا، كالضبطية القضائية السيبرانية أو خبراء المعلوماتية الشرعيين، ووفق إجراءات مدونة ومقننة تمنع الطعن في مشروعية الدليل. ويتعين أن تكون عملية جمع البيانات مصحوبة بمحاضر تقنية تُبيّن بدقة الأجهزة والبرامج المستعملة في التحليل الرقمي.

من جهة أخرى، تواجه المحاكمة في المنازعات الإلكترونية تحديات تتعلق ب**ضمان حقوق الدفاع**، خصوصًا عندما لا يمتلك القاضي أو الدفاع خبرات تقنية كافية لفهم طبيعة الأدلة المقدمة، مما قد يُضعف التوازن الإجرائي بين الأطراف. ويُقترح في هذا السياق الاستعانة بخبراء معلوماتيين كمساعدين قضائيين لتفسير طبيعة الأدلة وفك تشفير المعطيات المعروضة أمام المحكمة.

ومن المتطلبات الضرورية أيضًا **توفر بنى تحتية رقمية في القضاء**، مثل أنظمة إدارة الملفات الرقمية، وقاعات المحاكمة الافتراضية التي تسمح بمواصلة سير الدعوى رغم البعد الجغرافي أو الطارئ الصحي، وهي أنظمة أثبتت نجاعتها خلال جائحة كوفيد-19 في عدد من الدول[1].

كما لا يمكن تجاهل **الإطار التشريعي**، حيث تحتاج المحاكم إلى نصوص قانونية واضحة تضبط المسؤولية في الفضاء الرقمي، وتحدد وسائل الإثبات المقبولة، وشروط اعتمادها، وهذا ما تسعى إليه

[1] حسن عبيدات، **التحقيقات الإلكترونية والإثبات الجنائي**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2021، ص. 115.

العديد من التشريعات، ومنها التشريع الجزائري، من خلال التعديلات الأخيرة التي مست قانون الإجراءات الجزائية وقانون مكافحة الجرائم السيبرانية.

المبحث الثالث: دور التكنولوجيا الحديثة في مكافحة الجرائم الالكترونية وتحديات مكافحتها

المطلب الأول: دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية

تُستخدم التكنولوجيا الحديثة، وعلى رأسها شبكة الإنترنت، كوسيلة وأحيانًا كبيئة لارتكاب أفعال جرمية تمس حقوق الأفراد والمؤسسات والدول. فبفضل أدوات مثل **الهواتف الذكية، البرامج المفتوحة المصدر، الشبكات الافتراضية الخاصة(VPN) ، والتطبيقات المشفّرة،** صار من الممكن تنفيذ أفعال إجرامية عن بُعد دون الحاجة إلى الحضور المادي لمكان الجريمة.

الفرع الأول: صور إجرامية للجريمة الالكترونية

لقد أدت الثورة التكنولوجية إلى تحولات عميقة في حياة الأفراد والمجتمعات، حيث غزت الوسائل الرقمية مختلف مناحي الحياة، مما أوجد بيئة خصبة لاستغلال هذه التقنيات في ارتكاب أشكال جديدة من الجرائم، عُرفت باسم "الجرائم الإلكترونية". وتتمثل خطورة هذه الأخيرة في كونها تتسم بالخفاء وسرعة التنفيذ، مما يجعل اكتشافها وملاحقة مرتكبيها أمرًا بالغ الصعوبة.

ومن أبرز صور استخدام التكنولوجيا في الجريمة الإلكترونية[1]:

- **القرصنة المعلوماتية(Hacking)** ، حيث يتم اختراق الأنظمة للحصول على معلومات سرية أو تعديل بياناتها.
- **الاحتيال الإلكتروني،** عبر الرسائل المضللة والمواقع الوهمية التي تستهدف الضحايا بغرض سرقة بياناتهم أو أموالهم.

[1]سامي محمد عبد العزيز، **الجريمة الإلكترونية في ظل التطورات التكنولوجية**، دار الفكر الجامعي، الطبعة الأولى، مصر، 2020، ص. 54.

- **الابتزاز الإلكتروني،** من خلال الاستحواذ على صور أو معلومات خاصة ثم المطالبة بفدية مقابل عدم نشرها.
- **نشر البرمجيات الخبيثة،** كالفيروسات وأحصنة طروادة، التي تُزرع في الأجهزة لإلحاق الضرر بها أو التحكم فيها عن بُعد.

كما ساهم تطور الذكاء الاصطناعي، والطباعة ثلاثية الأبعاد، وتقنيات الواقع الافتراضي، في تعقيد صور الجريمة الإلكترونية، حيث ظهرت جرائم جديدة مثل **تزوير الصوت والفيديو(Deepfake)** ، وهجمات التجسس الصناعي، والتلاعب في المعاملات المالية عبر البورصات الرقمية والعملات المشفرة.

الفرع الثاني: الأبعاد الرئيسية في الجرائم الالكترونية

ان التطور التكنولوجي، بالرغم من فوائده الجمة، أصبح أحد أبرز الاسباب المساعدة في تطور ظاهرة الجرائم الإلكترونية وتكمن خطورة استخدام التكنولوجيا الحديثة في الجرائم الإلكترونية في **ثلاثة أبعاد رئيسية**[1]:

اولا عالمية الفضاء الرقمي، حيث يمكن تنفيذ الجريمة في قارة وتستهدف ضحية في قارة أخرى دون أن يعترضها أي حاجز جغرافي أو قانوني.

ثانيا صعوبة الإثبات، بفعل طبيعة الأدلة الرقمية القابلة للتعديل والحذف.

ثالثا إخفاء الهوية، عبر استعمال برامج التمويه والتشفير، مما يصعّب تعقب الفاعل الحقيقي.

وبالتالي، فإن التطور التكنولوجي، بالرغم من فوائده الجمة، أصبح أحد أبرز العوامل المساعدة على تنامي ظاهرة الجرائم الإلكترونية، ما يستدعي التفكير في حلول قانونية وتقنية متكاملة لمواجهتها، بالاعتماد على التعاون الدولي وتحديث النصوص القانونية باستمرار.

المطلب الثاني: التحديات التقنية و القانونية ثغرات التشريع وتأخر التحديث

[1]عمر الشريف، **التكنولوجيا الرقمية والجريمة المنظمة**، دار الثقافة للنشر والتوزيع، الطبعة الثانية، الأردن، 2021، ص. 73.

تعد الجرائم الإلكترونية واحدة من أكثر الجرائم تعقيدًا من حيث المواجهة القانونية والتقنية. إذ أن التكنولوجيا الحديثة تتيح للجرائم الإلكترونية الانتشار بشكل أسرع وأكثر فاعلية، بينما يظل العديد من الأنظمة القانونية عاجزًا عن مجاراة هذا التطور السريع. إن التحديات التقنية والقانونية المترتبة على الجرائم الإلكترونية لا تقتصر فقط على الكشف عنها، بل تمتد إلى صعوبة الإثبات، وحماية البيانات، بالإضافة إلى الثغرات القانونية التي تساهم في تفشي هذه الجرائم.

الفرع الأول : التحديات التقنية

تتمثل التحديات التقنية التي تواجه مكافحة الجرائم الإلكترونية في عدة جوانب رئيسية، منها[1]:

1. **التطور السريع للتكنولوجيا** :يتسم العالم الرقمي بالتطور المستمر والسريع، حيث تظهر تقنيات جديدة يومًا بعد يوم، سواء كانت تتعلق بالأجهزة أو البرمجيات. هذه الوتيرة السريعة تجعل من الصعب على السلطات التكنولوجية متابعة كل الجديد، ويستغل المجرمون ذلك لتنفيذ عملياتهم بشكل غير مرئي.
2. **التشفير والأدوات المجهولة** :يستخدم مجرمو الإنترنت تقنيات التشفير المتقدمة وأدوات التخفي مثل الشبكات الخاصة الافتراضية(VPN) ، والشبكات المظلمة(Dark Web) ، مما يعقد عملية تتبعهم واحتجاز الأدلة اللازمة لإثبات الجريمة. وعليه، يصبح من الصعب تحديد هوية الفاعلين بسبب إخفائهم لأنفسهم على الإنترنت.
3. **أدوات الجريمة متعددة الاستخدام** :العديد من الأدوات التكنولوجية التي تستخدم في الجرائم الإلكترونية (مثل الفيروسات وأحصنة طروادة) تستخدم في أغراض متعددة قد تكون مشروعة أيضًا. وهذا يعني أن التقنيات نفسها التي تساعد في مكافحة الجرائم يمكن أن تُستخدم بشكل غير قانوني.

الفرع الثاني: التحديات القانونية

على الجانب القانوني، يمكن تلخيص التحديات في النقاط التالية[2]:

[1]فاطمة الزهراء عبد الله، **التكنولوجيا والقانون في عصر الإنترنت**، دار الفكر العربي، الطبعة الأولى، لبنان، 2020، ص. 89.
[2]أحمد عاطف، **الجرائم الإلكترونية بين الواقع والتشريع**، دار الجامعة الجديدة، الطبعة الثانية، مصر، 2019، ص. 125.

1. **ثغرات التشريع** :لا تزال العديد من الدول تفتقر إلى قوانين واضحة وشاملة لمكافحة الجرائم الإلكترونية، حيث لم يتمكن التشريع من مجاراة التقدم التكنولوجي. غياب الإطار القانوني الموحد في العديد من البلدان يساهم في تعميق الأزمة. ففي بعض الأحيان، قد لا تعترف القوانين الحالية بالجريمة الإلكترونية بشكل كامل أو قد تُعتبر أعمالًا غير مشروعة تتعلق بتكنولوجيا معينة لم تُحدد لها عقوبات واضحة.
2. **غياب التنسيق بين الدول** :بما أن الجرائم الإلكترونية يمكن أن تتم عبر الحدود، فإن التنسيق الدولي بين الأجهزة القضائية والأمنية في مختلف الدول يعد أمرًا بالغ الأهمية. ولكن في الكثير من الحالات، تفتقر الدول إلى اتفاقات دولية مُلزِمة لمكافحة الجرائم الإلكترونية، مما يسهل على المجرمين التنقل بحرية عبر الإنترنت دون أن يكونوا معرضين للمسائلة القانونية في دول أخرى.
3. **محدودية الخبرات القانونية** :إن التعامل مع الجرائم الإلكترونية يتطلب مزيجًا من المعرفة القانونية والتقنية. ونتيجة لندرة المحامين المتخصصين في القضايا الإلكترونية، غالبًا ما يكون لدى المحاكم صعوبة في التعامل مع هذه القضايا بمهنية عالية. كما يواجه المحامون صعوبة في تقديم الأدلة الرقمية التي يصعب فهمها.
4. **التأخر في تحديث التشريعات** :عادة ما تكون التشريعات القانونية بعيدة عن التطور السريع للتكنولوجيا. إذ في العديد من الحالات، تكون القوانين القديمة التي وضعت لمكافحة الجرائم التقليدية غير قابلة للتطبيق على الجرائم الإلكترونية. على سبيل المثال، القوانين التي تتعلق بالسرقة أو التزوير قد تكون بحاجة إلى تحديثات لتعكس الأبعاد الرقمية لهذه الأفعال. كما أن تقنيات مثل **الذكاء الاصطناعي** و**الواقع الافتراضي** قد تتطلب قوانين خاصة لضبط استخدامها من الناحية القانونية.
5. **غياب التشريعات المنظمة للبيانات** :تعد حماية البيانات الشخصية من أهم القضايا القانونية في عصر الجرائم الإلكترونية. وقد أظهرت العديد من الانتهاكات في هذا السياق، مثل تسريب البيانات من الشركات الكبرى، ضرورة تطوير قوانين تحمي المعلومات الشخصية للمواطنين. ومع ذلك، فإن تشريعات حماية

البيانات لا تزال في مراحل تطويرية في العديد من البلدان، وتحتاج إلى مزيد من التحديث لمواكبة المخاطر الرقمية الحديثة.

الفرع الثالث: التأثيرات المترتبة على هذه التحديات

إن التأخر في تحديث التشريعات والقصور في تنفيذ الحلول التقنية المتكاملة لهما تأثيرات واسعة النطاق. فمن جهة، يصبح من الصعب على السلطات مكافحة الجرائم الإلكترونية بشكل فعّال. ومن جهة أخرى، يزداد قلق الأفراد والشركات حول حمايتهم من الاعتداءات الإلكترونية. علاوة على ذلك، فإن غياب التنسيق الدولي يزيد من فرص استغلال هذه الثغرات من قبل المجرمين، مما يضاعف من تعقيد المشكلة.

المطلب الثالث: التحديات الاجتماعية والثقافية

مع التقدم التكنولوجي الهائل واستخدام الإنترنت بشكل متزايد في مختلف جوانب الحياة اليومية، برزت العديد من التحديات الاجتماعية والثقافية التي تؤثر بشكل مباشر على قدرة الأفراد والمجتمعات في مواجهة الجرائم الإلكترونية. يشكل **قلة الوعي** و **ثغرات الحماية الفردية** من أبرز هذه التحديات التي تسهم في تسهيل ارتكاب الجرائم الإلكترونية.

الفرع الأول: قلة الوعي بالأخطار الرقمية

يعد **الوعي الرقمي** من أهم العوامل التي تحد من خطر الوقوع ضحية للجرائم الإلكترونية. ومع تزايد استخدام الإنترنت في التواصل الاجتماعي، التسوق الإلكتروني، التعليم عن بُعد، والخدمات المصرفية عبر الإنترنت، فإن قلة الوعي بالمخاطر الرقمية يمكن أن تضع الأفراد في مواقف خطيرة.

1. **غياب التعليم الرقمي في المناهج التعليمية** :رغم الأهمية المتزايدة للتكنولوجيا في التعليم والحياة اليومية، لا تزال الكثير من المناهج الدراسية في العديد من الدول تفتقر إلى تعليم الطلاب كيفية حماية أنفسهم من

المخاطر الرقمية. بالإضافة إلى ذلك، لا توجد برامج تعليمية كافية توضح كيفية التعامل مع المعلومات الشخصية بشكل آمن[1].

2. **الجهل بالممارسات الآمنة على الإنترنت** :يعاني العديد من الأفراد من نقص الوعي بالممارسات الأساسية للأمن السيبراني مثل استخدام كلمات مرور قوية، تجنب فتح الروابط المشبوهة، واستخدام برامج مكافحة الفيروسات. نتيجة لذلك، يكونون أكثر عرضة للوقوع ضحايا لهجمات مثل **الاحتيال الإلكتروني** و **الاختراقات**.
3. **التوعية المحدودة بشأن الخصوصية وحماية البيانات** :قلة الوعي بحقوق الخصوصية وحماية البيانات يعرض الأفراد لخطر تسريب معلوماتهم الشخصية. حيث يسهل على المهاجمين الاستفادة من عدم معرفة الأفراد لطرق حماية بياناتهم الحساسة.

الفرع الثاني: ثغرات الحماية الفردية

تعتبر **الحماية الفردية** من المخاطر الرقمية عنصرًا حاسمًا في تأمين المعلومات الشخصية. لكن هناك العديد من الثغرات التي تؤدي إلى ضعف الحماية، سواء بسبب عدم وجود أدوات حماية فعّالة أو بسبب استخدام الأفراد لأدوات غير آمنة.

1. **قلة استخدام برامج الأمان** :رغم توفر برامج مضادة للفيروسات وبرامج حماية من السرقة الإلكترونية، إلا أن الكثير من الأفراد لا يستخدمون هذه الأدوات أو يستخدمونها بشكل غير فعال. قد يكون ذلك نتيجة لقلة الوعي، أو لأنهم يعتقدون أن هذه الأدوات غير ضرورية.
2. **الاعتماد على أنظمة حماية ضعيفة** :يظل العديد من المستخدمين يعتمدون على أنظمة حماية ضعيفة أو قديمة لا تواكب التطور في أساليب الهجوم الإلكتروني. على سبيل المثال، يظل البعض يستخدم كلمات مرور بسيطة يسهل تخمينها، أو يفتقرون إلى نظام تشفير بيانات يحميهم من محاولات القرصنة.

[1]فوزي محمد، **الأمن السيبراني والتحديات الاجتماعية في العصر الرقمي**، دار الفكر العربي، الطبعة الأولى، مصر، 2021، ص. 143.

3. **استخدام أجهزة غير آمنة** :يعد استخدام الأجهزة الشخصية مثل الهواتف الذكية، والحواسيب غير المحمية بمثابة باب مفتوح أمام المهاجمين للاستفادة من الثغرات التقنية الموجودة في هذه الأجهزة. قد يتجاهل المستخدمون التحديثات الأمنية المستمرة التي تصدرها الشركات المنتجة، مما يجعل أجهزتهم أكثر عرضة للهجمات.
4. **مشاركة المعلومات الشخصية بشكل غير آمن** :الكثير من الأفراد يشاركون معلوماتهم الشخصية على الشبكات الاجتماعية دون التفكير في أبعاد هذه المشاركة على مستوى الخصوصية والأمن. قد يؤدي هذا إلى استهدافهم من قبل المحتالين الإلكترونيين، الذين يستطيعون استخدام هذه البيانات في **هجمات التصيد** أو عمليات الاحتيال.

الفرع الثالث: تأثيرات قلة الوعي وثغرات الحماية

إن قلة الوعي حول الجرائم الإلكترونية والتقنيات الأمنية، فضلاً عن الثغرات في الحماية الفردية، يؤديان إلى تداعيات اجتماعية ثقافية واسعة النطاق. تتضمن هذه التداعيات ما يلي[1]:

1. **زيادة انتشار الجرائم الإلكترونية** :كلما كان الأفراد أكثر عرضة للجرائم الإلكترونية بسبب قلة الوعي، زادت الفرص للمهاجمين الإلكترونيين للاستفادة من هذه الفجوات. وهذا بدوره يزيد من حجم الجرائم الإلكترونية ويجعل من الصعب مكافحتها.
2. **انخفاض الثقة في الأنظمة الرقمية** :يساهم نقص الوعي في إحجام الأفراد عن استخدام الخدمات الرقمية بأمان. حيث قد يتجنب البعض التعامل مع الخدمات البنكية عبر الإنترنت أو التسوق الإلكتروني بسبب مخاوف من فقدان بياناتهم الشخصية أو التعرض لعمليات احتيال.
3. **تفشي الإحساس بعدم الأمان** :يؤدي عدم وجود حماية فعالة إلى شعور الأفراد بعدم الأمان أثناء تصفح الإنترنت، مما يحد من قدراتهم على الاستفادة الكاملة من الفرص التي توفرها التكنولوجيا.

[1] ريم عبد الله، **الوعي الرقمي وأثره على حماية الأفراد من الجرائم الإلكترونية**، دار العلم للنشر، الطبعة الثانية، السعودية، 2020، ص. 91.

المطلب الرابع مقترحات لتطوير الإطار القانوني والتقني

من أجل مواجهة الجرائم الإلكترونية بفعالية، يجب تطوير الإطار القانوني والتقني في العديد من المجالات. إن سرعة تطور التكنولوجيا تجعل من الضروري تحديث التشريعات الوطنية والدولية بشكل مستمر لمواكبة هذه التغيرات السريعة. في هذا المطلب، سنقدم مقترحات لتطوير هذا الإطار، من خلال تحديث التشريعات وإنشاء وحدات متخصصة.

الفرع الاول : تحديث التشريعات لمواكبة التطور التكنولوجي

إن التطور السريع للتكنولوجيا، بما في ذلك استخدام الإنترنت وتقنيات المعلومات، قد أفرز تحديات جديدة في مجال القانون الجنائي والسيبراني. ولذلك، يجب تحديث التشريعات لمواكبة هذه التغيرات على النحو التالي[1]:

1. **تعديل القوانين الحالية لمواكبة الجرائم الإلكترونية:**

يجب على المشرعين مراجعة القوانين الجنائية لتضمين **الجرائم الإلكترونية** بشكل صريح. يتعين أن تشمل هذه التعديلات الجرائم المتعلقة بالاحتيال الإلكتروني، القرصنة، الهجمات الإلكترونية، وانتشار البرمجيات الخبيثة. على سبيل المثال، يجب وضع قوانين تعاقب بشكل محدد على **التصيد الاحتيالي** (phishing)و **الاختراقات الإلكترونية.**

2. **تطوير قوانين حماية البيانات الشخصية:**

مع تزايد الاهتمام بالبيانات الشخصية، من الضروري تطوير القوانين التي تحمي الأفراد من تسريب أو إساءة استخدام بياناتهم. ينبغي تضمين قوانين تحظر جمع البيانات الشخصية بدون موافقة، وتفرض إجراءات صارمة على الجهات التي تقوم بتخزين البيانات الشخصية والتأكد من تطبيق **المعيار الدولي لحماية البيانات** مثل **اللائحة العامة لحماية البيانات(GDPR)** التي تطبق في الاتحاد الأوروبي.

[1]حسام صالح، **الجرائم الإلكترونية والتحديات القانونية**، دار الفكر الحديث، الطبعة الأولى، مصر، 2022، ص. 234.

3. **إصدار قوانين تتعلق بالذكاء الاصطناعي:(AI)**

بما أن الذكاء الاصطناعي أصبح جزءًا أساسيًا من التكنولوجيا الحديثة، ينبغي على المشرعين وضع تشريعات خاصة بشأن **أخلاقيات الذكاء الاصطناعي** و **حقوق الأفراد** المرتبطة بالاستخدام غير المشروع لهذه التقنية، مثل المراقبة التطفلية أو القرارات المؤثرة في حياة الأفراد بناءً على الخوارزميات.

4. **مراجعة التشريعات المتعلقة بالجرائم المالية الإلكترونية:**

تعتبر الجرائم المالية عبر الإنترنت، مثل **غسيل الأموال** و **التلاعب بالأسواق المالية**، من الأنماط المتزايدة في العصر الرقمي. ينبغي أن تُضاف تشريعات جديدة تحظر**المدفوعات غير المشروعة** عبر الإنترنت، مع وضع إجراءات قانونية لملاحقة الجرائم الإلكترونية المالية التي تتم عبر العملات الرقمية أو الأنظمة المالية غير التقليدية[1].

5. **التعاون الدولي في مكافحة الجرائم الإلكترونية:**

نظرًا لأن الجرائم الإلكترونية لا تتقيد بالحدود الجغرافية، فمن المهم التعاون بين الدول لتطوير **اتفاقيات دولية** بشأن مكافحة الجرائم الإلكترونية. يجب تشجيع البلدان على توقيع **اتفاقيات قانونية دولية** لمكافحة الجرائم الإلكترونية، وتبادل المعلومات بين الدول لملاحقة المجرمين عبر الحدود.

الفرع الثاني: إنشاء وحدات متخصصة للتعامل مع الجرائم الإلكترونية

من أجل تعزيز جهود مكافحة الجرائم الإلكترونية، يجب على الدول إنشاء وحدات متخصصة قادرة على التعامل مع هذه الجرائم بشكل فعال، وتقديم الدعم الفني والقانوني المناسب. تشمل هذه الوحدات ما يلي:

1. **إنشاء وحدة شرطة مختصة بالجرائم الإلكترونية:**

[1] أحمد محمود، **تحديث التشريعات لمكافحة الجرائم الإلكترونية**، دار المعرفة القانونية، الطبعة الثانية، السعودية، 2021، ص. 154.

يجب على الدول إنشاء وحدات شرطية متخصصة في التعامل مع الجرائم الإلكترونية. وتعمل هذه الوحدات على التحقيق في الجرائم الإلكترونية، جمع الأدلة الرقمية، وملاحقة المجرمين الذين يرتكبون **الاختراقات** أو **الاحتيال الإلكتروني** .يجب أن تكون هذه الوحدات مجهزة بأحدث التقنيات لتحليل الأدلة الإلكترونية.

2. **إطلاق مركز وطني للاستجابة للحوادث الإلكترونية:**

يجب إنشاء **مراكز وطنية** لاستجابة الحوادث الإلكترونية في كل دولة، حيث يتم تنسيق الاستجابة السريعة للتهديدات الإلكترونية، مثل الهجمات الإلكترونية على البنية التحتية الحساسة أو الهجمات **من نوع الفدية** .يمكن أن يكون لهذا المركز دور رئيسي في توفير الدعم الفني لجميع مؤسسات القطاع العام والخاص.

3. **تدريب كوادر متخصصة في الأمن السيبراني**[1]:

من الضروري تدريب مختصين في **الأمن السيبراني** لتطوير مهاراتهم في مواجهة **التحديات التقنية** . يمكن للمؤسسات الحكومية والتعليمية تنظيم برامج تدريبية لأفراد الأمن السيبراني، مع توفير شهادات دولية معترف بها في هذا المجال، مثل **شهادات** (Certified Information Systems Security Professional) **CISSP** و .(Certified Ethical Hacker) **CEH**

4. **إنشاء منصات لتبادل المعلومات بين المؤسسات الحكومية والشركات:**

يجب إنشاء منصات تقنية آمنة لتمكين **الشركات والمؤسسات الحكومية** من تبادل المعلومات حول **المخاطر الإلكترونية** والتهديدات الجديدة. من خلال هذه المنصات، يمكن أن يتعاون القطاعين العام والخاص في مكافحة الجرائم الإلكترونية والتقليل من تأثير الهجمات الإلكترونية.

5. **إقامة مراكز للبحث والتطوير في مجال مكافحة الجرائم الإلكترونية:**

[1] يوسف عبد الله، **الجرائم الإلكترونية: أبعاد وتحديات**، دار الطليعة للنشر، الطبعة الأولى، لبنان، 2020، ص. 89.

من الضروري إقامة **مراكز بحثية** متخصصة في **مكافحة الجرائم الإلكترونية** والبحث في الحلول التقنية المتقدمة مثل **تقنيات الذكاء الاصطناعي** و **البلوك تشين** .هذه المراكز يمكن أن تساهم في تطوير أدوات وتقنيات جديدة لتحليل الجرائم الإلكترونية والحد من وقوعها.

الفرع الثالث: تعزيز الثقافة القانونية والتقنية لدى الأفراد

إن نشر الوعي القانوني والتقني حول الجرائم الإلكترونية يُعد أمرًا ضروريًا للمساعدة في تقليل أثر هذه الجرائم. يجب تطوير استراتيجيات التوعية على النحو التالي[1]:

1. **حملات توعية رقمية:**

يمكن تنفيذ حملات توعية في وسائل الإعلام ووسائل التواصل الاجتماعي بهدف تعريف المواطنين بمخاطر الجرائم الإلكترونية وكيفية الوقاية منها، مثل أهمية استخدام **كلمات مرور قوية**، وعدم فتح رسائل بريدية مشبوهة.

2. **توفير خدمات دعم قانوني للأفراد:**

يجب توفير خدمات استشارية وقانونية للأفراد الذين وقعوا ضحايا للجرائم الإلكترونية. هذه الخدمات يمكن أن تكون جزءًا من **الهيئات الحكومية** أو عبر **منظمات غير حكومية** متخصصة.

الفرع الرابع: تطوير التعاون بين القطاعات الحكومية والقطاع الخاص

يجب تعزيز التعاون بين **القطاع الحكومي** و **القطاع الخاص** لتطوير الحلول التقنية وحماية الأفراد من الجرائم الإلكترونية، من خلال:

1. **الشراكة بين الشركات الخاصة والحكومات:**

[1] كريم مصطفى، **إستراتيجيات مكافحة الجرائم الإلكترونية**، دار الوعي القانوني، الطبعة الأولى، الإمارات، 2023، ص. 101.

يمكن أن تكون **الشراكات الاستراتيجية** بين الشركات الخاصة والحكومة مفيدة في تطوير أنظمة أمنية وتقنيات جديدة لحماية البيانات الشخصية والشركات من الهجمات الإلكترونية.

خاتمة

الخاتمة:

في ختام هذا البحث، يمكننا أن نؤكد أن التكنولوجيا الحديثة أصبحت جزءًا لا يتجزأ من حياتنا اليومية، حيث أثرت بشكل كبير على جميع جوانب الحياة الاجتماعية والاقتصادية والثقافية. ومع هذا التقدم الهائل، برزت الجرائم الإلكترونية كأحد أخطر التحديات التي تهدد الأفراد والمجتمعات والدول على حد سواء. فقد وفرت هذه التكنولوجيا فرصًا كبيرة لارتكاب الجرائم الإلكترونية عبر الإنترنت، مما جعل من الصعب تعقب مرتكبيها ومعاقبتهم بشكل فعال. تتنوع هذه الجرائم بين الاحتيال الإلكتروني، القرصنة، سرقة الهوية، و الاعتداءات على الخصوصية، وهو ما يتطلب استراتيجيات متعددة لمكافحتها.

أظهرت الدراسة أن التحديات التقنية التي تتسم بها الجرائم الإلكترونية لا تقتصر على القدرات التكنولوجية المتطورة فقط، بل تمتد لتشمل الثغرات القانونية في التشريعات التي لا تواكب التطورات السريعة في مجال الإنترنت. مما يعيق قدرة النظم القانونية على ملاحقة الجناة وحماية الأفراد من هذه الجرائم. ويضاف إلى ذلك أن قلة الوعي المجتمعي حول هذه الجرائم، و الثغرات في الحماية الفردية، تعتبر من أبرز العوامل التي تسهم في انتشار الجرائم الإلكترونية بشكل كبير.

النتائج :

بناءا على ما سبق اكتشفنا ان التكنولوجيا ليست مصدر خطر بالنسبة للجريمة الالكترونية انما طريقة استخدامها هي الخطر القائم فهي سلاح ذو حدين(للتقدم والابتكار وفي نفس الوقت تستخدم لتنفيد الجرائم الالكترونية)

كما ان تطور اساليب الجريمة الالكترونية ساهم في استخدام المجرمين ادوات متقدمة مثل –برمجيات الخبيثة اكثر تطورا

–الانترنت المظلم لاخفاء الهوية كما يتيح استخدام العملات الرقمية مصدر دخل يصعب تتبعه

–افتقار العديد من المؤسسات والافراد الوعي الكافي لحماية انفسهم الكترونيا وهو السبب الرئيسي لهذه الجرائم لان التدريب والتثقيف الرقمي يقللان من معدل الوقوع ضحية الجرائم الالكترونية

اقتراحات :

بناءً على هذه التحديات اقترحنا مجموعة من التوصيات التي لا نقول انها تساهم في القضاء على الجريمة الالكترونية انما تقلل منها

فعلى مستوى الحكومات وصناع القرار من الضروري أن يتم سن وتحديث التشريعات القانونية باستمرار لتواكب التطورات في مجال تكنولوجيا المعلومات.

انشاء وحدات امنية متخصصة في الامن السيبراني كما أن التدريب المستمر للقوات الأمنية والقضائية على التعامل مع هذه الجرائم يعد أمرًا بالغ الأهمية.

التعاون الدولي لمحاربة الجرائم العابرة للحدود

اما على مستوى المؤسسات يجب أن تُعزز القدرات الأمنية التقنية من خلال استخدام أدوات متقدمة مثل الذكاء الاصطناعي، وتحليل البيانات، مع توظيف خبراء امن المعلومات لمراقبة النظام مع تقديم دورات تدريبية للعمال والموظفين

اما الجانب الاهم فيكون على مستوى الافراد، بتعزيز ثقافة الوعي الرقمي بين الأفراد عبر حملات توعية موجهة للحد من الأنماط السلوكية غير الآمنة، مثل استخدام كلمات مرور ضعيفة أو عدم التأكد من مصداقية المصادر عبر الإنترنت مع تجنب مشاركة المعلومات الشخصية الحساسة خصوصا في وسائل التواصل الإجتماعي

قائمة المراجع

قائمة المراجع

- **الكتب**

1. أحمد خالد الزبيدي، مدخل إلى الأمن السيبراني: المبادئ والتطبيقات، دار صفاء للنشر والتوزيع، الطبعة الأولى، الأردن، 2021.
2. أحمد بن عبد العزيز الشدوخي، الجرائم المعلوماتية في المملكة العربية السعودية: دراسة مقارنة، مكتبة الرشد، الرياض، السعودية، الطبعة الأولى، 2018.
3. أحمد بن عبد العزيز الشدوخي، الجرائم المعلوماتية في المملكة العربية السعودية: دراسة مقارنة، مكتبة الرشد، الرياض، السعودية، الطبعة الأولى، 2018.
4. أحمد عماد الدين، الجرائم العابرة للحدود في الفضاء الإلكتروني، دار الفكر، الطبعة الثانية، دمشق، سوريا، 2020.
5. أحمد عبده، الجرائم الإلكترونية بين الواقع والتحديات، دار الفجر للنشر والتوزيع، الطبعة الأولى، القاهرة، مصر، 2019.
6. بانا ضمراوي، تعريف التكنولوجيا، دار النشر غير محددة، الطبعة الأولى، 2017.
7. بلحاج أحمد، قانون الاتصالات الإلكترونية وحماية المستهلك الرقمي، دار المحيط، الجزائر .
8. بوكاف عبد الكريم، حماية المعطيات الشخصية في القانون الجزائري، دار الفضيلة، الجزائر، 2019.
9. توفيق محمود محمد القزاز، الأمن السيبراني لمصادر المعلومات Cyber Security، مؤسسة طيبة للنشر والتوزيع، الطبعة الأولى، مصر، 2022.
10. جفال أحمد، الجرائم الإلكترونية في القانون الجزائري، دار الفجر، ط1، الجزائر، 2018.
11. حسن الطيب، الأمن السيبراني ومخاطر الفضاء الرقمي، دار المسيرة، الطبعة الأولى، عمان، الأردن، 2021.
12. حسين حمدي، وسائل الاتصال والتكنولوجيا في التعليم، دار القلم، الطبعة الأولى، الكويت، 1994.
13. خالد القاضي، الجرائم الإلكترونية – المفهوم وسبل المواجهة، دار الفكر الجامعي، الطبعة الثانية، الإسكندرية، مصر، 2016.

14. خليف عبد الحق، قانون العقوبات: القسم الخاص – الجرائم الحديثة، دار هومه، الجزائر، ط2، 2020.

15. درارجة فاطمة الزهراء، التحقيق في الجريمة الإلكترونية في التشريع الجزائري، دار الجامعي، الجزائر، ط1، 2020.

16. زواوي مروان، الحوكمة الرقمية والأمن السيبراني في الجزائر، دار الكتاب الحديث، الجزائر، 2021.

17. زياد حمود، تقنيات التشفير والأمن السيبراني، دار ابن خلدون، الطبعة الأولى، تونس، 2022.

18. سامي أبو زيد، أمن المعلومات ومواجهة البرمجيات الخبيثة، دار الشروق، عمان، الأردن، الطبعة الثالثة، 2020.

19. سامي خليل، أمن المعلومات والجرائم المعلوماتية، مكتبة الرشد، الرياض، السعودية، الطبعة الأولى، 2019.

20. سامية فوزي إبراهيم، الجريمة الإلكترونية والإرهاب الرقمي، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، الطبعة الأولى، 2020.

21. سفيان دربال، الجرائم السيبرانية: قراءة قانونية ومعلوماتية، دار الهدى، الطبعة الثانية، الجزائر، 2021.

22. سلوى عواد، الجرائم الإلكترونية ومواجهة التشريعات العربية لها، دار النهضة العربية، الطبعة الأولى، بيروت، لبنان، 2018.

23. شتوح سمية، السياسة العقابية في مواجهة الجريمة الإلكترونية، دار الكتاب الجامعي، الجزائر .

24. صفاء نجم، الجريمة المنظمة في ظل العولمة، دار صفاء للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2018.

25. صديقي عبد المجيد، مكافحة الجريمة الإلكترونية من خلال السياسة الجنائية الجزائرية، دار اليقين، الجزائر، ط1، 2021.

26. عادل عبد الله، الجريمة الإلكترونية وأمن المعلومات في التشريعات العربية، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، مصر، 2020.

27. عبد الله العوضي، الجريمة الإلكترونية: تحديات الواقع والمستقبل، دار المطبوعات الجامعية، الطبعة الأولى، بيروت، لبنان، 2020.

28. عبد الله عبد الرحمن، الجرائم الإلكترونية – دراسة قانونية مقارنة، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2017.

29. عبد المجيد محمد، الجرائم الإلكترونية والبيانات الرقمية، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، مصر، 2018.

30. عبد الرحيم بشبر، التكنولوجيا في عملية التعلم والتعليم، دار الشروق للنشر، الطبعة الأولى، عمان، الأردن، 1988.

31. عبد الرحمن حجازي، الهجمات الإلكترونية الحديثة: دراسة تحليلية وتقنية، دار الفكر المعاصر، بيروت، لبنان، الطبعة الأولى، 2021.

32. عبد الغني عماد، القانون الدولي لمكافحة الجريمة الإلكترونية، دار الإشعاع، الطبعة الأولى، بيروت، لبنان، 2019.

33. عبد الجبار سعد الله، الحروب السيبرانية: المفهوم والتأثير السياسي، دار الفكر الجامعي، الجزائر، 2021.

34. عبد الكريم بوكاف، حماية المعطيات الشخصية في القانون الجزائري، دار الفضيلة، الجزائر، 2019.

35. عبد المجيد صديقي، مكافحة الجريمة الإلكترونية من خلال السياسة الجنائية الجزائرية، دار اليقين، الجزائر، ط1، 2021.

36. علي عبد العزيز، تكنولوجيا التعليم في تطوير المواقف التعليمية، مكتبة الفلاح للنشر والتوزيع، الطبعة الأولى، بيروت، لبنان، 1996.

37. عماد الدين مصطفى، الجرائم الإلكترونية في ظل القانون الجنائي المغربي والمقارن، مطبعة النجاح الجديدة، الطبعة الأولى، الدار البيضاء، المغرب، 2022.

38. عبده سمير، العرب والتكنولوجيا، دار الآفاق الجديدة، الطبعة الأولى، بيروت، لبنان، 1981.

39. عماد حسين، القانون الجنائي وتقنيات المعلومات الحديثة، دار الفكر الجامعي، الطبعة الأولى، القاهرة، مصر، 2022.

40. عمار بن الحاج، الجرائم السيبرانية: دراسة قانونية وتقنية، دار الهدى، الجزائر، الطبعة الثانية، 2022.

41. علي عبد العزيز، تكنولوجيا التعليم في تطوير المواقف التعليمية، مكتبة الفلاح للنشر والتوزيع، الطبعة الأولى، بيروت، لبنان، 1996.

42. فاطمة الزهراء السالمي، الجريمة الإلكترونية في التشريع المقارن، دار الأكاديميون، الطبعة الأولى، عمان، الأردن، 2020.

43. فادي البشير، الشرطة الجنائية الدولية ومكافحة الجرائم الإلكترونية، دار الثقافة الجامعية، الطبعة الأولى، القاهرة، مصر، 2019.

44. فؤاد منصور، الجريمة الإلكترونية وتحديات التشريع الجزائي المعاصر، دار الثقافة للنشر، الطبعة الأولى، عمان، الأردن، 2021.

45. قادة بن عيسى، إثبات الجرائم الإلكترونية في التشريع الجزائري، دار المعرفة، الجزائر، ط1، 2019.

46. كارول فاجان، دان لونلي، التخطيط للتقنية: دليل لقادة المدارس، سكولاستيك إنك، الطبعة الأولى، نيويورك، الولايات المتحدة الأمريكية، 1995.

47. كريم مصطفى، إستراتيجيات مكافحة الجرائم الإلكترونية، دار الوعي القانوني، الطبعة الأولى، الإمارات، 2023

48. كمال راجي، التعاون الدولي في مكافحة الجريمة المعلوماتية، دار الكتب القانونية، الطبعة الأولى، بيروت، لبنان، 2020.

49. ليلى محمود، الجريمة الإلكترونية والذكاء الاصطناعي، دار الكتاب الحديث، الطبعة الأولى، القاهرة، مصر، 2023.

50. لعروسي كريمة، الجرائم الإلكترونية في الجزائر ودور الشرطة العلمية في مكافحتها، دار الخلدونية، ط1، الجزائر، 2021.

51. محمود عبد الفضيل، الجرائم السياسية والانقلابات في العالم العربي، دار الشروق، القاهرة، مصر، الطبعة الثانية، 2017.

52. محمود سالم، الجرائم الإلكترونية وأساليب مكافحتها، دار الفكر العربي، القاهرة، مصر، الطبعة الثالثة، 2020.

53. محمد باشا، مفهوم التكنولوجيا والتقنيات، دار النشر غير محددة، الطبعة الأولى، القاهرة، مصر، 2018

54. محمد عبد الحميد النجار، الأمن السيبراني وحماية نظم المعلومات، دار الفكر.

55. محمد الفايد، الجرائم الرقمية في التشريع الجزائري، دار الخلدونية، الطبعة الأولى، الجزائر، 2021.

56. محمد عبد الرحمن حسن، الجريمة الإلكترونية في ضوء أحكام الشريعة والقانون، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

57. مسعودي أمينة، حماية الحياة الخاصة والمعطيات الشخصية في القانون الجزائري، دار الهدى، الجزائر، ط1، 2020.

58. ناصر العزاوي، التحقيق في الجرائم المعلوماتية: أصوله وإجراءاته، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، الأردن، 2021.

59. نوال الشيباني، الفضاء السيبراني والتحولات الإجرامية، دار أسامة للنشر، الطبعة الأولى، الجزائر، 2019.

60. هالة عبد المنعم، الجرائم الإلكترونية: التحديات والحلول، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى، 2021.

- **المجلات**

61. دياب البداحنة، "الجرائم الإلكترونية: المفهوم والأسباب"، مجلة البحوث الأمنية، 2018.

62. زيوش عبد الرؤوف، زغيشي مصطفى، "الجرائم الإلكترونية الاقتصادية: المفهوم والدوافع"، مجلة الدراسات القانونية والاقتصادية، العدد 07، 2024.

63. عبد الله بوجلال، "الهاكتيفيزم والمقاومة الرقمية: رؤية في الأيديولوجيا الإلكترونية"، مجلة العلوم الإنسانية، جامعة بسكرة، العدد 17، 2022.

64. فاطمة الزهراء بن عيسى، "التطور التقني للجريمة الإلكترونية: دراسة مقارنة"، مجلة دراسات قانونية وسياسية، جامعة قسنطينة، العدد 27، 2022.

65. فضيلة عاقلي، "الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"، مجلة جيل الأبحاث القانونية المعمقة، العدد 12، 2014.

66. ليلى محمود، "التحديات في التصدي للجرائم الإلكترونية: دراسة مقارنة"، مجلة الدراسات القانونية، العدد 5، 2021.

67. محمد عبد الله، "تحليل سلسلة الهجوم السيبراني وفق نموذج"Cyber Kill Chain ، مجلة الأمن السيبراني العربي، العدد 5، 2022.

68. نمديلي رحيمة، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة"، مجلة جيل الأبحاث القانونية المعمقة، العدد 12، 2014.

69. ناصر العزاوي، "تجارب دولية في مكافحة الجرائم الإلكترونية: دراسات مقارنة"، مجلة القانون الدولي، 2022.

70. وفاء محمد علي محمد، "الأبعاد الاجتماعية للجرائم الإلكترونية: دراسة تحليلية لمضمون عينة من القضايا في محكمة سوهاج"، مجلة جامعة سوهاج، 2021.

71. وسيم فريد، "برامج الفدية والتهديد الجديد لأمن المعلومات"، مجلة الفكر المعلوماتي، العدد 18، 2023.

العنوان	الصفحة
الإهداء	
شكر و تقدير	
الملخص باللغة العربية	
الملخص باللغة الإنجليزية	
قائمة المحتويات	ا
المقدمة	أ
الفصل الأول: الإطار النظري للجرائم الإلكترونية	
المبحث الأوّل: : مفاهيم الجرائم الالكترونية	11
المطلب الأوّل: تعريف التكنولوجيا الحديثة وأنماطها	13
الفرع الأول: مفهوم التكنولوجيا الحديثة	16
الفرع الثاني: أنماط التكنولوجيا الحديثة	19
المطلب الثاني: تعريف الجريمة الإلكترونية وخصائصها	19
الفرع الأول: تعريف الجريمة الالكترونية	21
الفرع الثاني: خصائص الجريمة الالكترونية	23
المطلب الثالث: التطور التاريخي للجرائم الإلكترونية	23
الفرع الأول: المرحلة الاولى	24
الفرع الثاني: المرحلة الثانية	25
الفرع الثالث: المرحلة الثالثة	25
الفرع الرابع: المرحلة الرابعة	26
المطلب الرابع: تصنيف الجرائم الإلكترونية حسب الأساليب والأهداف	27
الفرع الأول: التصنيف حسب الاساليب التقنية	28
الفرع الثاني: التصنيف حسب الاهداف	29
الفرع الثالث: تصنيف من وجهة نظر القانون	30
الفرع الرابع:تصنيفات اخرى معاصرة	31

المبحث الثاني: الأطر التشريعية الوطنية والدولية لمكافحة الجرائم الالكترونية	32
المطلب الأوّل: المعاهدات والاتفاقيات الدولية في مكافحة الجرائم الإلكترونية	33
الفرع الأول: اتفاقية بودابست لمكافحة الجريمة الالكترونية 2001	34
الفرع الثاني: البروتوكول الثاني المكمل لاتفاقية بودابست 2022	35
الفرع الثالث: اتفاقية الامم المتحدة لمكافحة الجريمة الالكترونية 2024	36
المطلب الثاني: القوانين والتشريعات الوطنية: النموذج الجزائري	37
الفرع الأول: قانون 09-04	38
الفرع الثاني: تعديل قانون العقوبات الجزائري(المادة 394مكرر الى المادة 394مكرر 7)	39
الفرع الثالث: التحديات والافاق المستقبلية	40
المطلب الثالث: مؤسسات الدولة والهيئات المتخصصة في مكافحة الجرائم الإلكترونية	40
الفرع الأول: الهيئات الامنية المختصة	41
الفرع الثاني: الهيئات الادارية والمؤسسات الرسمية	42
المطلب الرابع: العقوبات المقترنة بالجرائم الإلكترونية ومدى فاعليتها	43
الفرع الأول: العقوبات الجزائية في قانون العقوبات الجزائري	44
الفرع الثاني: العقوبات في القوانين الخاصة	45
الفرع الثالث: مدى فاعلية هذه العقوبات في الحد من الجريمة الالكترونية	46
المبحث الثالث: دوافع وأساليب ارتكاب الجرائم الإلكترونية	48
المطلب الأوّل: الدوافع الاقتصادية والاجتماعية للجناة	48
الفرع الأول: الدوافع الاقتصادية	49
الفرع الثاني: الدوافع الاجتماعية	50
الفرع الثالث: التداخل بين الدوافع الاقتصادية والاجتماعية	51
المطلب الثاني: دوافع الجريمة السياسية والإيديولوجية	52
الفرع الأول: الدوافع السياسية	53
الفرع الثاني: الدوافع الايدلوجية والفكرية	54
الفرع الثالث: الجريمة السياسية الايدلوجية كأداة للتمرد او العصيان الرقمي	55

الفرع الرابع: السياق الدولي والاقليمي كبيئة محفزة لهذه الجرائم	55
الفرع الخامس: ضعف المواجهة التشريعية والاعلامية	56
المطلب الثالث: الأساليب التقنية: الفيروسات، الاختراق، التصيّد الاحتيالي	56
الفرع الأول: الفيروسات والبرمجيات الخبيثة	57
الفرع الثاني: الاختراق الالكتروني	57
الفرع الثالث: التصيد الاحتيالي	58
الفرع الرابع: العلاقة التفاعلية بين هذه الاساليب	59
الفرع الخامس: تطور الاساليب التقنية مع الذكاء الاصطناعي	59
المطلب الرابع: استخدام الأدوات والبرمجيات الخبيثة وتحليل سلسلة الهجوم	60
الفرع الأول: مفهوم البرمجيات الخبيثة	60
الفرع الثاني: الأدوات التقنية المستخدم في الهجوم	61
الفرع الثالث: تحليل سلسلة الهجوم السيبراني	61
الفرع الرابع: أمثلة تطبيقية من الواقع	62
الفرع الخامس: مكافحة البرمجيات الخبيثة	63
الفصل الثاني: سبل مكافحة الجرائم الالكترونية	
المبحث الأول: التدابير الوقائية والتقنية	53
المطلب الأوّل: التوعية والتثقيف السيبراني لدى الأفراد والمؤسسات	53
الفرع الأول: أهمية التوعية السيبرانية	53
الفرع الثاني: دور العامل البشري في التصدي للجرائم الالكترونية	57
المطلب الثاني: بروتوكولات أمن المعلومات وأدوات الحماية التقنية	57
الفرع الأول: بروتوكولات امن المعلومات	57
الفرع الثاني: أدوات الحماية التقنية	59
المطلب الثالث: دور القطاع الخاص (مزوّدي الأنظمة وشركات الأمن السيبراني)	61
الفرع الأول:دور الشركات في تعزيز القدرات الحكومية في التصدي للتهديدات السيبرانية	61
الفرع الثاني: تحديات الشركات في مجال الأمن السيبراني	62

المطلب الرابع: آليات التعاون الدولي في تبادل المعلومات والإنذار المبكر	63
الفرع الأول: الإنذار المبكر السيبراني	63
الفرع الثاني:آليات التعاون الدولي	64
المبحث الثاني: الإجراءات الجنائية والتحقيقية	66
المطلب الأوّل: استراتيجيات جمع الأدلة الرقمية وتحليلها	66
الفرع الأول: تقنيات جمع و ثوتيق الجريمة الالكترونية	67
الفرع الثاني: ضوابط احترام خصوصية الأشخاص والبيانات	67
المطلب الثاني: إجراءات الضبط والحجز الإلكتروني	68
الفرع الأول: شرعية الضبط الالكتروني للجريمة الالكترونية	69
الفرع الثاني: صعوبات وتحديات الضبط الالكتروني	69
المطلب الثالث: التعاون بين قوات الأمن والقضاء قنوات الاتصال وأطر البيانات المشتركة	70
الفرع الأول: تشكيل فرق عمل مختلطة	71
الفرع الثاني: وضع اتفاقيات وطنية ودولية	71
المطلب الرابع: متطلبات الإثبات والمحاكمة في المنازعات الإلكترونية	72
الفرع الأول: الاعتراف القانوني بالأدلة الرقمية	72
الفرع الثاني:احترام إجراءات جمع الأدلة الرقمية	72
المبحث الثالث: التحديات المعاصرة والمقترحات التطويرية	73
المطلب الأوّل: دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية	73
الفرع الأول: صور إجرامية للجريمة الالكترونية	74
الفرع الثاني: الأبعاد الرئيسية في الجرائم الالكترونية	74
المطلب الثاني: التحديات القانونية: ثغرات التشريع وتأخر التحديث	75
الفرع الأول: التحديات التقنية	75
الفرع الثاني:التحديات القانونية	76
الفرع الثالث:التأثيرات المترتبة على هذه التحديات	77
المطلب الثالث: التحديات الاجتماعية والثقافية	77

الفرع الأول:قلة الوعي بالأخطار الرقمية	78
الفرع الثاني:ثغرات الحماية الفردية	78
الفرع الثالث: ثاتيرات قلة الوعي وثغرات الحماية	79
المطلب الرابع: مقترحات لتطوير الإطار القانوني والتقني تحديث التشريعات، إنشاء وحدات خاصة، تعزيز التعاون	80
الفرع الأول: تحديث التشريعات لمواكبة التطور التكنولوجي	80
الفرع الثاني: إنشاء وحدات متخصصة للتعامل مع الجرائم الالكترونية	81
الفرع الثالث: تعزيز الثقافة القانونية والتقنية لدى الأفراد	83
الفرع الرابع: تطوير التعاون بين القطاعات الحكومية والقطاع الخاص	83
خاتمة	83
قائمة المراجع	86