جامعة 8 ماي 1945 قالمة

كلية الحقوق والعلوم السياسية

قسم الحقوق تخصص قانون أعمال

مذكرة مكملة لمتطلبات نيل شهادة الماستر في القانون

عنوان المذكرة

الأمن السيبراني في الجزائر.

إعداد الطلبة: تحت إشراف

1/ صمودي كريمة الدكتورة: بوشارب إيمان

2/ برقعي سمر

تشكيل لجنة المناقشة

الرقم	الأستاذ	الجامعة	الرتبة العلمية	الصفة
1	بوحليط يزيد	8ماي 1945 قالمة	أستاذ التعليم العالي	رئيسا
2	بوشارب إيمان	8ماي 1945 قالمة	محاضر أ	مشرفا ومقررا
3	بوزيتونة لينة	8ماي 1945 قالمة	محاضر ب	عضوا مناقشا

السنة الجامعية: 2025/2024


بسم الله الرحمن الرحيم

« رب أوزعني أن أشكر نعمتك التي أنعمت علي وعلى والديّ وأن أعمل صالحا ترضاه وأدخلني برحمتك في عبادك الصالحين».

سورة النمل:" الآية 19

شكر وعرفان

الحمد لله الذي يسر البدايات وأكمل النهايات وبلغنا الغايات

الحمد لله الذي ما تم جهدا غلا بعونه وما ختم سعي إلا بفضله الحمد لله على البلوغ ثم الحمد لله على التمام بتوفيق من الله

تم هذا العمل اللهم انفعنا بما علمتنا وزدنا علما

نتوجه بالشكر الخالص الى كل من ساعدنا في إنجاز هذا العمل المتواضع وأخص بالشكر الخالص **الدكتورة بوشارب إيمان** المشرفة على هذه المذكرة التي لم تتوانى لحظة في توجيهنا وارشادنا جزاها الله خيرا.

كما نتوجه بخالص امتناني لأعضاء لجنة المناقشة على تشريفهم لمناقشة هذا العمل الأستاذ: **بوحليط يزيد** والدكتورة **بوزيتونة لينة** فلهم أخص عبارات التقديروالاحترام.

كما لا يفوتني أن أتقدم بالشكر الخالص لكل **أساتذة جامعة 08 ماي 1945 قالمة قسم الحقوق** فلهم في النفس منزلة وان لم يسعف المقام بذكرهم فهم أصل الفضل

والخير والشكر.

كما أتوجه بخالص امتناني لكل من أمدنا بكلمة طيبة أو نصيحة أو فكرة أو نقد بناء لهم كل الامتنان والاحترام

الإهداء:

..أولا وقبل كل شيء الحمد لله الذي بنعمته تتم الصالحات.. وبفضله تتحقق الأمنيات

يسر لنا البدايات وأكمل لنا النهايات

وبلغنا الغايات

وبكل حب وفخر اهدي ثمرة نجاحي أولا إلى نفسي لقد وفيت بوعدي لكي الذي قطعته عليك منذ سنوات

إلى من أرضعتني الحب والحنان وبلسم الشفاء إلى التي جعل الله الجنة تحت أقدامها التي كانت كالشمعة لكي تنير لي دربي إلى الدرع الواقي والكنز الباقي أمي الغالية أطال الله في عمرها

كما اهدي عملي المتواضع إلى من حصد الاشواك عن دربي ليمهد طريق العلم إلى والدي العزيز أطال الله في عمره وأهداه بالتقوى والعافية وجعله خيمة فوق رؤوسنا

إلى أساتذتي الأفاضل جميع أساتذة كلية الحقوق والعلوم السياسية الذين لم يبخلوا علينا من التوجيه والعلم خاصة مشرفتي دكتورة بوشارب إيمان ولجنة المناقشة شكرا لكم على حسن الإستماع بوركتم على مجهوداتكم الجبارة

إلى من دعموني وكانوا لي كالظل الثابت إلى الذين إذا مالت بي الدنيا وجدتهم في كتفي سندا لا يميل إخوتي أحبائي

(هبة ، ندى ، مريم ، محمد)

إلى من شاركتني الصداقة قبل الدراسة رفيقة دربي وقاسمتني عناء إنجاز هذه المذكرة رفيقة دربي (برقعي سمر)

الى اي شخص جمعتني به الحياة سواء كانت صداقة أو قرابة وتركوا في حياتي أثرا جميلا دمتم على خير ورزقكم الله أضعاف من فرحتي بهذا اليوم وأستودعكم الله الذي لا تضيع ودائعه

الطالبة : صمودي كريمة

بسمِ اللهِ الرَّحْمٰنِ الرَّحِيم

"وَقُلْ رَبِّ زِدْنِي عِلْمًا"

﴿سورة طه – الآية 114﴾

إهداء

...إلى من كان لهم الفضل، بعد الله، فيما تحقق من هذا الإنجاز إلى من كانوا بعد الله سببًا فيما أنا عليه اليوم

إلى والديَّ العزيزين خلفاوي عمار وبرقيعي بادية اللذَين واحتضناني بحبٍّ صادق ورعاية لا تُقدَّر بثمن، فكانا لي نعم العون والسند، ووهبا لي عائلةً ...ومعنى حقيقيًّا للأمان

..إلى والدتي التي أنجبتني جبار كميلية، رحمها الله رحمةً واسعة، وغفر لها وجعل مثواها الجنة، فلولاها بعد الله ما كانت البداية

...إلى والدي البيولوجي عيسى وزوجته الكريمة ورتسي ياسمين، أطال الله في عمرهما، والدي الذي لا أنسى وجوده ودعمه في هذه الرحلة من الحياة

.إلى إخوتي أماني، محمد رواد، تامر حمادة، دينا الذين كانوا لي السند والرفقة الصادقة في كل مراحل حياتي

وإلى ذلك الدعم الخفيّ، الصادق في حضوره، الهادئ في أثره، الذي كان رفيقًا غير مُعلن لمسيرة هذا العمل، فله من الامتنان بقدر ما ترك من أثر

... كما أتوجه بالشكر وبخالص امتناني لابنة عمتي خديجة بوقرن لدعمها وافكارها ومساعداتها التي لا تعد ولا تحصى في تحصيل هذا العمل

إلى رفيقة دربي وصديقة عمري إلى من سكنت لها روحي إلى من شاركتني عناء إنجاز المذكرة صمودي كريمة

إلى جميع أساتذة كلية الحقوق والعلوم السياسية، وأجدر بالذكرة الدكتورة إيمان بوشارب التي كانت بمثابة الأخت

...إلى كل من آمن بي ودعمني، وكان جزءًا من هذا المشوار، إلى كل من حمل لي في قلبه دعوة صادقة، أو كلمة طيبة، أو ابتسامة مشجّعة

أهدي هذا العمل المتواضع، عرفانًا وامتنانًا، وتقديرًا لكل لحظة حبٍّ واهتمام صادقة منكم جميعًا، راجيًا من الله أن يجعلها خطوة مباركة على درب العلم والعمل

الطالبة: برقعي سمر

مقدمـــة

مقدمة:

شهد العالم خلال العقود الأخيرة تحولات جذرية في مجال التكنولوجيا الرقمية، حيث أصبحت التقنيات الحديثة جزءاً لا يتجزأ من حياتنا اليومية. ومع انتشار الإنترنت وتوسع استخدام الأجهزة الذكية، ظهرت تحديات جديدة تتعلق بالأمن السيبراني والجريمة المعلوماتية. فقد بات العالم الافتراضي مسرحاً للعديد من الأنشطة الإجرامية التي تستهدف الأفراد والمؤسسات وحتى الدول. القرصنة الإلكترونية، سرقة البيانات الشخصية، الهجمات على البنية التحتية الحيوية، والاحتيال المالي الإلكتروني ليست سوى أمثلة قليلة على الجرائم التي تهدد استقرار المجتمعات وأمنها.

الأمن السيبراني بدوره يمثل درعاً وقائياً ضد هذه التهديدات، حيث يعمل على حماية الأنظمة الرقمية والمعلومات الحساسة من الاختراقات والاعتداءات. ومع ذلك، فإن التحديات التي تواجه الأمن السيبراني تتزايد يوماً بعد يوم، خاصة مع تطور أدوات الهجوم السيبراني واستخدام تقنيات الذكاء الاصطناعي في تنفيذ الجرائم المعلوماتية. هذا الواقع أدى إلى ضرورة البحث عن حلول شاملة ومتكاملة لمواجهة هذه التهديدات.

يُعد الأمن السيبراني ضمانة قانونية لحماية الأصول المعلوماتية الحيوية التي تؤثر بشكل مباشر على الأمن القومي. فالهجمات السيبرانية التي تستهدف البنية التحتية الحيوية، كالطاقة والمياه والصحة، قد تؤدي إلى انتهاك القوانين المتعلقة بالأمن العام وتعطيل المرافق الأساسية التي تحميها التشريعات كحقوق غير قابلة للتصرف. كما أن الجرائم السيبرانية، مثل القرصنة الإلكترونية والتلاعب بالبيانات، تشكل خرقًا واضحًا للمواد القانونية التي تحظر الاعتداء على الملكية الفكرية أو الأنظمة المعلوماتية، مما يستوجب تجريم مرتكبيها بموجب القوانين الجزائية.

إضافة إلى ذلك، يلعب الأمن السيبراني دورًا محوريًا في تعزيز الثقة القانونية في المعاملات الإلكترونية. فمع تبني العديد من الدول للتجارة الإلكترونية والحكومة الرقمية، أصبحت الحاجة إلى بيئة إلكترونية آمنة مطلبًا قانونيًا وأخلاقيًا. تشدد القوانين ذات الصلة، مثل اتفاقيات الأمم المتحدة بشأن الاستخدامات القانونية لتكنولوجيا المعلومات، على أهمية وضع آليات قانونية وتقنية لتأمين العمليات الرقمية ومنع أي شكل من أشكال التزوير أو الاحتيال الإلكتروني.

يعكس الأمن السيبراني التزام الدول بتطبيق مبادئ سيادة القانون في الفضاء الرقمي، حيث يتمثل دوره

في تحقيق التوازن بين الحرية الرقمية والأمن العام. ففي ظل تنامي التهديدات السيبرانية العابرة للحدود، تصبح القوانين الوطنية والدولية المتعلقة بالتعاون القضائي ومكافحة الجرائم السيبرانية أدوات ضرورية لضمان حماية شاملة للمجتمع الرقمي. وبالتالي يبرز الأمن السيبراني ليس فقط كضرورة تقنية، بل كالتزام قانوني وأخلاقي لحفظ حقوق الأفراد والمؤسسات في العصر الرقمي

أهمية الموضوع:

تأتي أهمية هذه الدراسة من كونها تعالج قضية عابرة للحدود تأثيره على كافة المستويات: الفردية، المؤسسية، والدولية. فالجرائم المعلوماتية لم تعد مجرد حوادث فردية أو هجمات صغيرة، بل أصبحت تمثل تهديداً وجودياً للأمن القومي والاقتصاد العالمي. من هنا، فإن فهم ديناميات هذه الجرائم وآليات مواجهتها يعد أمراً ضرورياً لضمان استمرارية التنمية والاستقرار.

بالإضافة إلى ذلك، فإن الدراسة تسلط الضوء على الجانب القانوني الذي يعاني من نقص تشريعي واضح في العديد من الدول، مما يجعلها عرضة لاستغلال الجرائم المعلوماتية. كما أن التحليل المتعمق لدور الأمن السيبراني يمكن أن يساهم في تعزيز الوعي المجتمعي بأهمية حماية البيانات والأنظمة الرقمية. فإن الدراسة تقدم إطاراً عملياً يمكن أن يستفيد منه صناع القرار في وضع سياسات وتشريعات أكثر فاعلية لمكافحة الجرائم السيبرانية.

وأخيراً، فإن أهمية هذه الدراسة تكمن أيضاً في كونها تتناول موضوعاً مستقبلياً يتطلب مزيداً من البحث والتطوير. فالعالم يتجه نحو المزيد من الاعتماد على التكنولوجيا، مما يعني أن التحديات المرتبطة بالأمن السيبراني ستزداد تعقيداً. وبالتالي، فإن هذه الدراسة تمثل خطوة أولى نحو فهم أعمق لهذه القضايا ووضع الحلول المناسبة لها.

أهداف الموضوع:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف التي تساهم في إثراء المعرفة حول الأمن السيبراني ودوره في مكافحة الجريمة المعلوماتية.

– تسعى الدراسة إلى تسليط الضوء على مفهوم الأمن السيبراني وأهميته في حماية الأنظمة الرقمية والبيانات الحساسة من التهديدات السيبرانية.

– تهدف إلى تحليل أبرز الجرائم المعلوماتية وأساليب تنفيذها، مع التركيز على الآثار السلبية التي تتركها على الأفراد والمجتمعات.

– تهدف الدراسة إلى استعراض الجهود الدولية والمحلية الرامية إلى تعزيز الأمن السيبراني ومكافحة الجرائم المعلوماتية، مع التركيز على الثغرات القانونية والفنية التي تعوق هذه الجهود.

– تسعى الدراسة إلى تقديم توصيات عملية يمكن أن تساهم في تحسين الإطار القانوني والتقني الخاص بمكافحة الجرائم المعلوماتية. خامساً، تهدف إلى تعزيز الوعي المجتمعي بأهمية الأمن السيبراني وكيفية التعامل مع التهديدات السيبرانية.

وأخيراً، تسعى الدراسة إلى تقديم رؤية مستقبلية حول دور الأمن السيبراني في مواجهة التحديات القادمة، خاصة مع التطور المستمر في تقنيات الذكاء الاصطناعي وإنترنت الأشياء. وبهذا، فإن الدراسة تهدف إلى أن تكون مرجعاً علمياً وعملياً يمكن الاستفادة منه من قبل الباحثين وصناع القرار والمهتمين بمجال الأمن السيبراني ومكافحة الجرائم المعلوماتية.

أسبـــاب اختيار الموضـوع.

كان اختيارنا هذا الموضوع عدة أسباب منها:

1-أسباب ذاتية :

– ميولنا الشخصي لهذا الموضوع ورغبتنا بالبحث فيه .

– الرغبة في المساهمة ولو لجزء بسيط في إثراء المكتبة القانونية.

2-أسباب موضوعية :

التطلع لتبيان أهمية الأمن السيبراني ودوره في حياتنا اليومية التي أضحت التحول من المعاملات الإلكترونية بمختلف أشكالها والتهديدات التي تحيط بها.

إشكاليـــــة الموضوع

بالرغم من الأهمية القصوى للأمن السيبراني على المستوى العالمي، بسبب خطورة الجريمة المعلوماتية باعتبارها جريمة عابرة للأمكنة والأزمنة، تمس حتى سيادات وأعمال الدولة ومواقعها الرسمية، وتسبب كوارث تأتي غالبا بدون حلول أو إمكانية تدارك، لم ينص المشرع الوطني على قانون خاص بالأمن السيبراني

بعكس ما ذهبت اليه جل المشرعين في العالم [1]. بالمقابل نجده قد أشار اليه في بعض النصوص الهامة في كل مرة يتعلق الأمر بالرقمنة أو المجال السيبراني بصفة عامة، حيث نجد على رأسهم القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها[2] و القانون رقم 20-05 المتعلق بوضع منظومة الأمن الأنظمة المعلوماتية[3] ، وعديد النصوص التطبيقية التي يحاول المشرع الوطني فيها تحقيق الأمن في المجال السيبراني و التي سيتم التطرق اليها في هذا العمل ،كما ان المشرع و في اطار تسليط الضوء و ابراز أهمية الأمن السيبراني أنشأ المدرسة العليا للأمن السيبراني من أجل ضمان التكوين الأمثل في المجال.

وعليه وامام كل هذه النصوص القانونية والتنظيم المؤسساتي وأهمية الأمن السيبراني على ضوء ما تم تقديمه، يطرح التساؤل التالي:

هل يحقق الامن السيبراني في الجزائر حماية فعالة ضد الجريمة المعلوماتية بشكل يضمن معه بيئة سيبرانية امنة؟

بالنسبة للمنهج المتبع:

محاولة الإجابة عن الإشكالية المطروحة أمام حداثة الموضوع تم بصفة رئيسية المنهج الوصفي بهدف التعريف بالأمن السيبراني ورسم حدوده من الناحية القانونية كما لم يخلو البحث من المنهج التحليلي في بعض طيات هذه المذكرة المناسب لتحليل النصوص القانونية والآراء الفقهية.

خطـة الموضوع.

[1]على سبيل المثال: القانون المغربي رقم 20-05 المؤرخ في 25 ماي 2020، الذي يتعلق بالأمن السيبراني، جريدة رسمية عدد 6904.

[2]القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47.

[3] المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي2020، المتعلق بوضع منظومة وطنية الامن الأنظمة المعلوماتية، جريدة الرسمية عدد 04.

بغرض دراسة الموضوع، تم تقسيم المذكرة إلى فصلين، حاولنا من خلال الفصل الأول التعريف بالأمن السيبراني باعتباره ظاهرة جديدة على الأقل من الناحية القانونية، أما الفصل الثاني فجاء موسوم بـ دور الأمن السيبراني في مكافحة الجريمة المعلوماتية، من أجل التطرق للمجهودات الدولية في مجال الأمن السيبراني ومن ثم المجهودات الوطنية، من أجل اجراء مقاربة وتحسس مواطئ القوة والنقص عند المشرع الوطني وهو لب إشكالية الدراسة. وفي نهاية دراستنا وضعنا خاتمة ضممناها مختلف النتائج والاقتراحات المستخلصة.

حيث جاءت الخطة كما يلي:

- **الفصل الأول: مضمون الامن السيبراني وأهميته.**

المبحث الأول: مفهوم الأمن السيبراني ومجالاته

المطلب الأول: تعريف الأمن السيبراني وأبعاده.

المطلب الثاني: تطبيقات الأمن السيبراني

المبحث الثاني: أهمية الأمن السيبراني في العصر الرقمي.

المطلب الأول: دور الأمن السيبراني في حماية البنية التحتية الحيوية.

المطلب الثاني: أهمية الأمن السيبراني في الحفاظ على الأمن العام.

- **الفصل الثاني: دور الأمن السيبراني في مكافحة الجريمة المعلوماتية**

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية موضوع الأمن السيبراني

المطلب الأول: مضمون الجريمة المعلوماتية.

المطلب الثاني: أبرز أشكال الجرائم المعلوماتية

المبحث الثاني: استراتيجيات الأمن السيبراني لمكافحة الجريمة المعلوماتية.

المطلب الأول: الجهود الدولية في مواجهة التهديدات السيبرانية.

المطلب الثاني: جهود الوطنية في مواجهة التهديدات السيبرانية.

الفصل الأول:
ماهية الأمن السيبراني

يُعد الأمن السيبراني من أبرز القضايا التي تحظى باهتمام عالمي واسع في ظل التطور التكنولوجي المتسارع. يشير هذا المفهوم إلى مجموعة من الإجراءات والتقنيات المصممة لتأمين الأنظمة الرقمية، بما في ذلك الشبكات، الأجهزة، البرمجيات، والبيانات، ضد الهجمات الإلكترونية أو أي محاولات للوصول غير المصرح به. يتضمن ذلك الوقاية من الفيروسات، هجمات القرصنة، سرقة المعلومات، وانتهاكات الخصوصية. تبرز أهمية الأمن السيبراني في كون العالم أصبح أكثر اعتمادًا على التكنولوجيا في مختلف القطاعات الحيوية؛ مثل الصحة، البنوك، الطاقة، والتعليم. أي خرق لهذه الأنظمة قد يؤدي إلى خسائر مالية كبيرة، تعطيل الخدمات الأساسية، أو حتى تهديد الأمن القومي للدول. على سبيل المثال، يمكن أن يؤدي اختراق النظام الصحي إلى تعريض حياة المرضى للخطر، بينما قد يتسبب استهداف البنية التحتية للطاقة في إحداث اضطرابات اقتصادية واجتماعية.

إضافة إلى ذلك، يلعب الأمن السيبراني دورًا أساسيًا في حماية البيانات الشخصية للأفراد والشركات، حيث أصبحت المعلومات الرقمية واحدة من أهم الموارد في العصر الحديث. بدون ضمان مستوى عالٍ من الحماية، يمكن استغلال هذه البيانات لأغراض احتيالية أو تسريبها لصالح جهات غير قانونية، مما يعرض أصحابها لمخاطر كبيرة.

في ظل تنامي التهديدات السيبرانية، أصبح من الضروري وضع استراتيجيات شاملة لتعزيز الأمن السيبراني على مستوى الدول، الشركات، وحتى الأفراد. تتضمن هذه الاستراتيجيات استخدام تقنيات متقدمة مثل الذكاء الاصطناعي، التشفير، وأنظمة الكشف عن التهديدات، بالإضافة إلى زيادة الوعي بين المستخدمين بأفضل الممارسات لتجنب الوقوع ضحية للهجمات. في النهاية، يُعتبر الاستثمار في الأمن السيبراني استثمارًا في استقرار المجتمعات وضمان مستقبل رقمي آمن ومستدام.

وعلى هذا النحو، سيتم تقسيم هذا الفصل إلى مبحثين كما يلي:

المبحث الأول: مفهوم الأمن السيبراني ومجالاته.

المبحث الثاني: أهمية الأمن السيبراني في العصر الرقمي.

المبحث الأول: مفهوم الامن السيبراني ومجالاته.

يعد الأمن السيبراني حجر الزاوية في بنية مجتمع المعلومات، كما يشكل ركيزة قانونية أساسية لحماية الأنشطة الحكومية والفردية. يثير موضوع الأمن السيبراني إشكاليات قانونية بالغة الأهمية تمس الحياة العامة والخاصة، حيث يؤثر بشكل مباشر على حقوق الملكية الفكرية، وحماية السرية والخصوصية، فضلاً عن صون البيانات الشخصية وضمان الحق في حرمة الحياة الخاصة. في ظل التطور التكنولوجي المتسارع وما صاحبه من ثورة معلوماتية واتصالية، برزت مفاهيم قانونية مستحدثة، من أبرزها مفهوم الأمن السيبراني. وقد اكتسب هذا المجال أهمية استراتيجية كونه بات أداة حماية أساسية تسعى الدول إلى توظيفها لدرء المخاطر السيبرانية التي قد تستهدف أمنها القومي واستقرارها. وتدرك الحكومات اليوم حجم التهديدات والتحديات الناشئة عن الجرائم السيبرانية، والتي قد تطال الدولة في بنيتها التحتية الحيوية، مؤسساتها الرسمية، وأفرادها بشكل عام، ومن هنا سنتناول تعريف الامن وابعاده كمطلب الأول، والمطلب الثاني تحت عنوان تطبيق الأمن السيبراني من الناحية المؤسساتية.

المطلب الأول: تعريف الامن السيبراني وابعاده.

إن تعزيز الأمن الفضاء السيبراني أصبح مطلبًا قانونيًا وإستراتيجيًا لا غنى عنه. إذ تعمل الدول على وضع تشريعات وطنية واتفاقيات دولية تهدف إلى تنظيم الفضاء الرقمي ومكافحة الجرائم الإلكترونية، بما يكفل حماية الحقوق والحريات العامة والخاصة. ويتمثل الهدف الأساسي من هذه الجهود في رسم خارطة طريق قانونية واضحة لتعزيز الأمن السيبراني بمختلف أبعاده، بما يضمن تحقيق التوازن بين التنمية التكنولوجية وحماية المجتمعات من المخاطر السيبرانية المحتملة، لأجل ذلك كان من الضروري تعريفه وتحديد أبعاده وفقا للفروع أدناه: تعريف الامن السيبراني كفرع اول، كفرع الثاني *الابعاد المختلفة للأمن السيبراني.*

الفرع الأول: تعريف الامن السيبراني.

الأمن السيبراني يُعنى بحماية الأنظمة والمعلومات من التهديدات الإلكترونية، ويشمل مجموعة من المبادئ والتقنيات التي تضمن سلامة البيانات وسرّيتها. يهدف إلى مواجهة الهجمات الرقمية وتأمين البنية التحتية التكنولوجية. تزداد أهميته في ظل التوسع المتزايد في استخدام التكنولوجيا في جميع جوانب الحياة اليومية وكما يكون له الامن السيبراني تعريف مباشر (أولا) ومن ناحية اصطلاحية (ثانيا).

أولا: التعريف المباشر للأمن السيبراني

إن تعريف الأمن السيبراني يتطلب تحديد معناه اللغوي والاصطلاحي حتى نتمكن من ضبط أبعاده القانونية والتعرف على آثاره القانونية على جميع الفاعلين في مجال مكافحة الجريمة المعلوماتية.

يشتق مصطلح السيبرانية (Cybernetics) من الكلمة الإغريقية"kybernetes" ، التي تعني "الطيار" أو "قائد الدفة" أو "الحاكم"، وتُستخدم مجازًا للإشارة إلى المتحكم أو المدير. في السياق الحديث، يعكس هذا المصطلح آليات التعقيب (Feedback Mechanisms) التي تتيح وظائف القيادة والتحكم في الأنظمة المغلقة[1].

تستمد السيبرانية جذورها أيضًا من كلمة "سيبر"، التي تُعبر عن كل ما يتعلق بثقافة الحواسيب، تقنية المعلومات، أو الواقع الافتراضي. ويظهر أثر هذه الجذرية في العديد من المصطلحات المستخدمة في مجال التكنولوجيا والاتصالات، مثل الفضاء السيبراني (Cyberspace) الذي يشير إلى العالم الرقمي الافتراضي، والخيال العلمي السيبراني (Cyberpunk) الذي يجمع بين التكنولوجيا المتقدمة والمجتمعات الإنسانية.

تُعرَّف السيبرانية بأنها علم الضبط والسيطرة عن بعد، حيث يرتبط مفهومها الأساسي بإدارة وضبط الأنظمة عبر آليات متقدمة. وبالتالي، يبرز المصطلح كأداة محورية لفهم وضبط الأنظمة الرقمية الحديثة، سواء في سياقات التكنولوجيا أو القانون أو الحياة اليومية[2].

2-تعريف الامن السيبراني من ناحية اصطلاحية.

يُعرَّف الأمن السيبراني بأنه مجموعة من الإجراءات المتخذة للدفاع ضد الهجمات الإلكترونية التي يشنها قراصنة الكمبيوتر، بالإضافة إلى التعامل مع تبعاتها وتنفيذ التدابير المضادة اللازمة[3]. كما يُعرَّف أيضًا بأنه مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الوقائية والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات والمستخدمين. وتتضمن هذه الأصول أجهزة الحوسبة المتصلة

[1] بيتر بيل سيل، ترجمة ضياء وراد هنداوي سي أي سي، الكون الرقمي: الثورة العالمية في الاتصالات، 2017، ص 21

[2] لبنى خميس مهدي، **أثر السيبرانية في تطور القوة**، مجلة حمورابي، جامعة النهرين، العدد 33-34, 2020، ص148.

[3] صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية مجلة قضايا سياسية, العدد 62, 2020، ص277.

بالشبكة، الموظفين، البنية التحتية، التطبيقات، الخدمات، أنظمة الاتصالات، والمعلومات المنقولة أو المخزنة في البيئة السيبرانية. ويهدف الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستخدمين والحفاظ عليها، بما يشمل السرية، السلامة، التوفر، وعدم الرفض[1].

كما يعرف على أنه مجموعة الإجراءات والتدابير الوقائية التي تهدف إلى حماية الأنظمة المعلوماتية والبيانات الرقمية من التهديدات السيبرانية، بما يضمن سلامة البنية التحتية الرقمية وسرية المعلومات. يشمل هذا المفهوم حماية الشبكات، الأجهزة، البرمجيات، والبيانات من الوصول غير المصرح به أو التعديل أو الإتلاف، وفقًا للتشريعات الوطنية والمعايير الدولية. من أبعاده القانونية، يرتبط الأمن السيبراني بصون الحقوق الأساسية مثل الحق في الخصوصية، حماية البيانات الشخصية، وضمان حرمة الحياة الخاصة، بالإضافة إلى دوره في حماية الأمن القومي ومنع الجرائم الإلكترونية التي تستهدف المؤسسات والأفراد. يفرض القانون على الجهات المعنية اتخاذ التدابير اللازمة لمنع الهجمات السيبرانية ومعالجة آثارها، تحت طائلة المسؤولية القانونية في حالة الإخلال بهذه الالتزامات.

قدمت وزارة الدفاع الأمريكية (البنتاغون) تعريفًا دقيقًا للأمن السيبراني، حيث اعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها، سواء كانت مادية أو إلكترونية، من الجرائم المختلفة مثل الهجمات، التخريب، التجسس، والحوادث. وبالتالي، يُعد الأمن السيبراني مجموعة من الأدوات، السياسات، مفاهيم الأمن، الضمانات، المبادئ التوجيهية، والتكنولوجيات المستخدمة لحماية البيئة الإلكترونية من المخاطر المحدقة بها.

في السياق الوطني، عرَّف المشرع الأمن السيبراني في **الفقرة الثالثة من المادة العاشرة من القانون رقم 18-04[2] حيث نصت على أنه:**

"الأمن السيبراني: مجموع الأدوات، السياسات، مفاهيم الأمن، الآليات الأمنية، المبادئ التوجيهية، طرق إدارة المخاطر، الأعمال، التكوين، الممارسات الجيدة، الضمانات، والتكنولوجيات التي يمكن

[1] الاتحاد الدولي للاتصالات شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن لمحة عامة عن الأمن السيبراني التوصية رقم .ITU-T X1205 سنة 2008، ص 32.

[2] القانون رقم 18-04، المؤرخ 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية العدد 27.

استخدامها لحماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفير وسلامة البيانات المخزنة أو المعالجة أو المرسلة".

سعى المشرع في تعديله لقانون العقوبات بموجب القانون رقم 04-15 إلى إضافة قسم سابع مكرر في الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 66-156، تحت عنوان "**المساس بأنظمة المعالجة الآلية للمعطيات**"، والذي يشمل المواد من **394 مكرر إلى 439 مكرر 7**[1]. وجاء هذا القسم لتنظيم حماية فعالة لأنظمة المعالجة الآلية للمعطيات، حيث نص على مجموعة من الجرائم والعقوبات المقابلة لها بهدف الحد من ارتكابها[2].

ثانيا: تعريف الامن السيبراني من خلال المفاهيم المرتبطة به.

للأمن السيبراني عدة مفاهيم ترتبط بيه كالفضاء السيبراني والجريمة السيبرانية والتهديد السيبراني والهجمات السيبرانية والردع السيبراني وعمليات الأمن السيبراني وخدمات الأمن السيبراني والإرهاب السيبراني والحرب السيبراني ومن هنا يمكن تفصيلهم:

1- الفضاء السيبرانيCyberspace:

هو بيئة رقمية تفاعلية تجمع بين العناصر المادية وغير المادية، وتشمل الأجهزة الرقمية، أنظمة الشبكات، البرمجيات، والمستخدمين سواء كانوا مشغلين أو مستخدمين عاديين. يُطلق على الفضاء السيبراني أيضًا "الذراع الرابعة للجيوش الحديثة" نظرًا لأهميته الاستراتيجية في الأمن القومي[3]

2- الجريمة السيبرانية Cybercrime: تشير إلى أي عمل ضار يحدث داخل الفضاء السيبراني، مثل عمليات الاحتيال الإلكتروني، نشر محتويات غير قانونية، أو الهجمات التي تستهدف أنظمة المؤسسات والأفراد بهدف التجسس، التخريب، الابتزاز، أو التأثير السلبي على الرأي العام.

---

[1] انظر المواد من 394 مكرر إلى 394 مكرر 7 من القانون رقم 18-04، سبق ذكره، والقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المتضمن تعديل قانون العقوبات لسنة 2004.الجريدة الرسمية العدد 71.

[2] بدري فيصل مكافحة الجريمة المعلوماتية في القانون الدو لي والداخلي، أطروحة لنيل شهادة دكتوراه علوم . تخصص قانون عام كلية الحقوق، جامعة الجزائر1 بن يوسف بن خدة ،2018، ص154

[3] إسلام مصطفى جمعة مصطفى، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية (مجلة علمية محكمة)، جامعة القاهرة، المجلد 12، العدد 3 ،2022، ص 7.

3-**التهديد السيبراني:** هو برنامج ضار أو نشاط مصدره الفضاء السيبراني، ويهدف إلى استهداف أمن الأجهزة الرقمية مثل الحواسيب، الهواتف الذكية، الأجهزة اللوحية، والشبكات المتصلة بالإنترنت. قد يكون مرتكب هذا التهديد فردًا، دولة، مجموعة من القراصنة، أو منظمة ذات أهداف جيوسياسية[1] .

4- الهجمات السيبرانية Attacks Cyber: هي أي عمل يستهدف إضعاف قدرات ووظائف شبكة الكمبيوتر لتحقيق غايات شخصية أو سياسية. يتم ذلك عبر استغلال نقاط الضعف في النظام، مما يمكن المهاجم من التلاعب به أو تعطيله [2]

5- الردع السيبراني :Deterrence Cyber يُعرَّف بأنه منع الأعمال الضارة التي تستهدف الأصول الوطنية في الفضاء الرقمي أو الأصول المرتبطة بالعمليات الفضائية، وذلك من خلال اتخاذ إجراءات استباقية ووقائية لحماية البنية التحتية السيبرانية. [3]

6-عمليات الأمن السيبراني: هي مجموعة الإجراءات المتعلقة بإدارة ومراقبة واكتشاف الحوادث والتهديدات السيبرانية التي تحدث داخل الفضاء السيبراني، بالإضافة إلى وضع خطط للتعامل معها وتنفيذها بشكل فعال.

7-خدمات الأمن السيبراني: تشمل الأنشطة الفنية والإدارية والاستشارية في مجال الأمن السيبراني، مثل خدمات التقييم الأمني، المراقبة المستمرة، التدقيق الأمني، والاستشارات التقنية المتعلقة بتعزيز الحماية السيبراني [4].

---

[1]ساعد بوقرص، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، الجزائر، المجلد 03 ، العدد 1 ،2022 ، ص125

[2]نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد ألمن الدول"، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، المجلد 8 ،العدد 2 ،2018 ،ص 191.

[3]إسلام مصطفى جمعة مصطفى، سبق ذكره، ص 725.

[4]منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني الأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، مصر، العدد 11، سنة 2020، ص 11.

8-الإرهاب السيبراني: ظهر هذا المصطلح مؤخرًا، ويشير إلى هجمات إلكترونية تهدف إلى تهديد الحكومات أو العدوان عليها لتحقيق أهداف سياسية أو دينية أو إيديولوجية. يجب أن تكون لهذه الهجمات آثار مدمرة أو تخريبية تعادل الأفعال المادية للإرهاب التقليد ي[1].

9-الحرب السيبرانية: هي هجوم متعمد يهدف إلى تعطيل أو خداع أو إضعاف أو تدمير أنظمة الكمبيوتر وشبكات الاتصال والمعلومات والبرمجيات الموجودة فيها. كما تشمل استخدام الوسائل السيبرانية مثل الاختراق، التجسس، وتسريب المعلومات الحساسة المتعلقة بالأمن القومي[2].

الفرع الثاني: الابعاد المختلفة للأمن السيبراني.

يرتبط الأمن السيبراني بمجالات عديدة ومختلفة حيث نتطرق الي ابعاد عسكرية واقتصادية وسياسية وقانونية واجتماعية:

أولا-الابعاد العسكرية *للأمن السيبراني.*

تتمثل الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية عبر الشبكات الإلكترونية في الفضاء السيبراني، مما يتيح تبادل المعلومات بسهولة وسرعة، بالإضافة إلى إصدار الأوامر العسكرية وتحقيق الأهداف من مسافة بعيدة بدقة فائقة. ومع ذلك، يمكن أن تتحول هذه الميزة إلى نقطة ضعف إذا لم تكن الشبكات المستخدمة مؤمنة بشكل جيد ضد الاختراقات الخارجية. فالهجمات السيبرانية قد تستهدف شبكات القوات المسلحة وأجهزة الاستخبارات، مما يؤدي إلى التجسس على الأمن العسكري للدول، وتعطيل قدرتها على نشر قواتها بسرعة، أو قطع الاتصالات بين الوحدات العسكرية. كما يمكن لهذه الهجمات أن تشل أنظمة الدفاع الجوي أو التوجيه الإلكتروني، وتؤدي إلى تعطيل عمل شبكات الكمبيوتر، بل وقد تؤدي إلى فقدان السيطرة تمامًا على وحدات القيادة والسيطرة[3].

[1]محمد كمال، الإرهاب السيبراني، دار كليم للطباعة والنشر والتوزيع، القاهرة، مصر،2022، ص 2.

[2] علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، العربي للنشر والتوزيع، 2022، ص 103.

[3]منى عبد الله السمحان، سبق ذكره، ص15.

ثانيا–الابعاد الاقتصادية *للأمن السيبراني*.

يُظهر الأمن السيبراني ترابطًا وثيقًا مع الاقتصاد، حيث يتجلى هذا الارتباط في تعزيز اقتصاد المعرفة من خلال التوسع في استخدام تقنيات المعلومات والاتصالات، مما يساهم في دفع عجلة التنمية الاقتصادية للعديد من الدول. هذه التقنيات تتيح للشركات الدولية والشركات الكبرى فرصة إدارة تكاليف الإنتاج بطرق أكثر كفاءة، لكنها تطرح تحديات متعددة تتعلق بحماية مقدمي الخدمات والمستهلكين عبر الإنترنت. بالإضافة إلى ذلك، مع دخول العالم عصر المال الإلكتروني وانتشار خدمات المحافظ الرقمية، زادت الاستثمارات في القطاع المالي والمصرفي لتطوير حلول الدفع الرقمي. ومع ذلك، وفي ظل ارتفاع معدل الجرائم السيبرانية المنظمة والمعقدة، وحجم التجارة الإلكترونية الذي بلغ تريليونات الدولارات، فإن هذه الأموال الضخمة أصبحت عرضة للتهديدات السيبرانية. لذلك، يمثل ضعف الأمن السيبراني خطرًا مباشرًا على نمو الاقتصاد الرقمي، مما يستدعي من الدول تعزيز معايير الحماية لتقليل هذه المخاطر والحفاظ على استقرار هذا القطاع الحيوي[1].

ثالثا–الابعاد السياسية *للأمن السيبراني*.

تستند الأبعاد السياسية للأمن السيبراني إلى حماية النظام السياسي والكيان العام للدولة، حيث يمكن استغلال التكنولوجيا لنشر معلومات وبيانات قد تؤدي إلى زعزعة استقرار الدول والحكومات. وتصل هذه المعلومات بسرعة كبيرة إلى شرائح واسعة من المواطنين دون التأكد من صحتها أو دقتها، مثل تسريب الوثائق الحساسة الذي قد يسبب أزمات معقدة على المستويين المحلي والدولي. بالإضافة إلى ذلك، لا يمكن إنكار التأثير المتزايد لمنصات التواصل الاجتماعي في الحياة السياسية، سواء من خلال إدارة الحملات الانتخابية، تنظيم التظاهرات الافتراضية، أو إطلاق حركات احتجاجية إلكترونية. كما يتم استغلال هذه المنصات من قبل بعض الحكومات كأدوات لنشر أجنداتها أو تحقيق أهدافها السياسية[2].

رابعا– الأبعاد القانونية للأمن السيبراني.

تتعلق الأنشطة التي يقوم بها الأفراد والمؤسسات بالقوانين التنظيمية، ومع بروز المجتمع المعلوماتي،

---

[1] فارس قوة، الأمن السيبراني Security Cyber – ،الموسوعة السياسية، رابط الموقع:
https://political-encyclopedia.org/dictionary/ /السيبراني20% : تاريخ: 21-04-2024 ساعة 22:00

[2] منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، دار النهضة العربية، القاهرة ،2016، ص 29.

ظهرت تشريعات جديدة تُشكّل الإطار القانوني المنظم لحماية هذا المجتمع وضمان حقوق كافة أطرافه بمختلف جوانبها. وفي هذا السياق، يلعب الأمن السيبراني دورًا محوريًا في حماية المجتمع المعلوماتي من التهديدات الإلكترونية، كما يسهم في تطبيق وإنفاذ القوانين والتشريعات المتعلقة بهذا المجال لضمان الامتثال والحفاظ على النظام الرقمي.

إن إصدار تشريعات مناسبة يُشجع المستثمرين والشركاء الاقتصاديين على الاستثمار، حيث يعمل ذلك على تعزيز ثقتهم من خلال إرساء بنية تحتية موثوقة وآمنة خالية من الاختراقات. وبما أن الأمن المعلوماتي يستند إلى مبادئ الثقة والجودة، فإنه يضع الأسس الضرورية لبناء اقتصاد قائم على تقديم خدمات سليمة ومستدامة[1].

خامسا- الابعاد الاجتماعية *للأمن السيبراني:*

تلعب شبكات التواصل الاجتماعي دورًا هامًا في تمكين الأفراد من التعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بطرق متنوعة. كما تسهم مشاركة مختلف شرائح المجتمع ومكوناته في تطوير المجتمع، حيث تتيح الفرصة لتبادل الأفكار والمعلومات، مما يعزز الحاجة إلى الحفاظ على استقرار الفضاء الإلكتروني والمجتمع الذي يعتمد عليه. بالإضافة إلى ذلك، فإن انفتاح مجتمع معين على المجتمعات الأخرى يخلق فرصًا لتبادل الخبرات والأفكار ويفتح آفاقًا للتعاون والتكامل .

يمكن القول إن الأمن السيبراني أصبح بُعدًا جديدًا ضمن أبعاد الأمن القومي، حيث أحدث تحولات جوهرية في مفاهيم العلاقات الدولية مثل الصراع، القوة، والتهديد. فقد أجبر هذا البعد فاعلي المجتمع الدولي على الانتقال من عالم مادي إلى فضاء افتراضي معقد ومتداخل بشكل كبير. وبالتالي، أصبح الأمن السيبراني ضرورة لا غنى عنها في العصر الحديث، خاصة مع ارتباط كافة التفاعلات الدولية بالتكنولوجيا والجانب الرقمي. وهذا يستدعي من الدول تبني آليات ووسائل فعالة لمجابهة التهديدات السيبرانية التي تتميز بالسرعة، الدقة، والغموض، بهدف تحقيق الأمن السيبراني والحفاظ على مكتسبات الدولة وأمنها القومي[2].

المطلب الثاني: تطبيقات الامن السيبراني

مع التطور المتسارع في التكنولوجيا الرقمية، أصبح الأمن السيبراني جزءًا أساسيًا من حياتنا اليومية. يهدف هذا المجال إلى حماية الأنظمة الإلكترونية والبيانات الحساسة من الهجمات والاختراقات التي قد

[1] أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، 2016، ص 9.

[2] محمد محمود العمري، مدخل إلى الأمن السيبراني، دار زهران للنشر و التوزيع، 2020 ،ص 36.

تؤدي إلى خسائر مادية أو معنوية. تتسع مجالات تطبيق الأمن السيبراني لتشمل مختلف القطاعات الحيوية، بدءًا من المؤسسات الحكومية وصولاً إلى الحياة الشخصية للأفراد. سواء كان ذلك في حماية البنية التحتية الوطنية، أو تأمين المعاملات المالية، أو صيانة الخصوصية الصحية، فإن الحاجة إلى استراتيجيات أمن سيبراني فعالة أصبحت أكثر إلحاحًا. في ظل تنامي التهديدات الإلكترونية، يتعين على كل قطاع تحديد احتياجاته الخاصة لضمان سلامة بياناته وعملياته. ومن هنا تبرز أهمية فهم مجالات تطبيق الأمن السيبراني ودورها الحيوي في تحقيق الاستقرار والحماية. وبذلك سنتطرق الى الناحية المؤسساتية في تطبيق الامن السيبراني من خلال المؤسسات الحكومية والخاصة كفرع اول وتطبيق امن السيبراني في مواجهة التهديدات السيبرانية كفرع ثاني.

الفرع الأول: الامن السيبراني في المؤسسات الحكومية والخاصة.

سواء في المؤسسات الحكومية أو الخاصة، فإن التحديات الرئيسية تشمل التصدي للبرمجيات الخبيثة (Malware)، وهجمات الحرمان من الخدمة(DDoS) ، والهجمات المستهدفة مثل التصيد الاحتيالي (Phishing)لذلك، يتم الاستثمار في حلول متكاملة تجمع بين الجدران النارية(Firewalls) ، وأنظمة الكشف عن التهديدات، وبرامج التوعية للموظفين. كما أصبحت الاستجابة للحوادث جزءًا أساسيًا من خطط الأمن السيبراني، حيث يتم تطوير فرق متخصصة للتعامل مع الاختراقات وإصلاح الأضرار بأسرع وقت ممكن.

أولا: الامن السيبراني في المؤسسات الحكومية:

تُعتبر المؤسسات الحكومية من أبرز الأهداف للهجمات الإلكترونية نظرًا لحساسيتها وتأثيرها على الأمن القومي. يركز الأمن السيبراني هنا على حماية البنية التحتية الحيوية، مثل شبكات الكهرباء والمياه والمواصلات، التي تعد العمود الفقري لأي دولة. يتم تأمين أنظمة إدارة البيانات الحكومية لمنع تسريب المعلومات السرية أو تعرضها للتلاعب. كما تُستخدم تقنيات متقدمة لرصد أي محاولات اختراق إلكتروني قد تستهدف الأنظمة الدفاعية أو العسكرية. بالإضافة إلى ذلك، تعمل الحكومات على وضع استراتيجيات وطنية للأمن السيبراني تشمل تدريب الموظفين وتحديث الأنظمة بشكل مستمر[1].

[1] فاطمة علي السعيد، التحديات السيبرانية في المؤسسات الحديثة، جامعة القاهرة، كلية الحاسبات و المعلومات، المركز القومي للبحوث العلمية , دار النهضة العربية, مصر , 2019, ص89

ثانيا: الامن السيبراني في المؤسسات الخاصة

في القطاع الخاص، يلعب الأمن السيبراني دورًا محوريًا في حماية الأصول الرقمية والحفاظ على سمعة الشركات. تتنوع تطبيقاته بين تأمين بيانات العملاء، مثل المعلومات الشخصية والمالية، ومنع الهجمات التي تستهدف تعطيل العمليات التجارية. على سبيل المثال، تسعى الشركات المالية إلى تأمين المعاملات البنكية عبر الإنترنت باستخدام تقنيات التشفير وتحليل السلوك للكشف عن النشاطات المشبوهة. كما تولي الشركات الكبرى اهتمامًا كبيرًا بحماية الملكية الفكرية من التجسس الصناعي الذي قد يؤدي إلى خسائر تنافسية.

الفرع الثاني: تطبيق الامن السيبراني في مواجهة التهديدات السيبرانية.

تواجه الأمن السيبراني العديد من التحديات (Challenges) والتهديدات(Threats) ، التي تُعتبر من أخطر المشكلات التي يتعامل معها العالم الرقمي، حيث غالبًا ما تؤدي إلى خسائر جسيمة يصعب إدارتها أو احتواؤها. ولا يقتصر دور الأمن السيبراني على الدفاع ضد هذه الهجمات فقط، بل يتعدى ذلك إلى منع وقوعها بشكل استباقي. ووفقًا لنتائج البحوث والدراسات السابقة، بالإضافة إلى الأدبيات ذات الصلة، يمكن تحديد أبرز هذه التحديات والتهديدات وأكثرها شيوعًا على النحو التالي:

سنتناول تطبيق امن السيبراني في التهديدات السيبرانية التقليدية(أولا)، وتطبيق امن السيبراني في التهديدات الحديثة(ثانيا).

اولا: تطبيق الامن السيبراني في التهديدات السيبرانية التقليدية.

سوف نتطرق في نقاط عديدة الى اهم تطبيقات الامن السيبراني في التهديدات السيبرانية التقليدية يتعلق الأمر في البرمجيات الخبيثة في التهديدات السيبرانية، فيروس الفدية الخبيث في التهديدات السيبرانية، تصيد البيانات والمعلومات في التهديدات السيبرانية

1-البرمجيات الخبيثة في التهديدات السيبرانية

البرمجيات الخبيثة، أو ما تُعرف بالبرامج الضارة، هي نوع من البرامج التي يتم تصميمها للوصول غير المصرح به إلى أجهزة الكمبيوتر أو إلحاق الضرر بها. بمعنى آخر، تشمل هذه البرامج أدوات تهدف إلى منح جهات خارجية القدرة على الوصول إلى المعلومات الحساسة دون إذن، أو تعطيل العمليات الطبيعية

للبنية التحتية الحرجة. ومن بين الأمثلة الشائعة على البرمجيات الخبيثة يمكن ذكر أحصنة طروادة، وبرامج التجسس، والفيروسات. وبعبارات أخرى، تُعتبر البرمجيات الخبيثة فيروسات متقدمة تم تطويرها لتجاوز

أنظمة الحماية المثبتة على الأنظمة الرقمية، حيث تعمل على إحداث أضرار أو تشويش في عملها، مما يتيح التلاعب بالبيانات الحساسة أو السيطرة عليها. ويعتمد نجاح هذه البرمجيات بشكل أساسي على استغلال الثغرات الموجودة في الأنظمة[1].

2- فيروس الفدية الخبيث في التهديدات السيبرانية

برامج الفدية الخبيثة تشير إلى نموذج عمل واسع النطاق يعتمد على تقنيات متنوعة تستخدمها الجهات الضارة لابتزاز الأموال من الأفراد والمؤسسات. ويُعتبر فيروس الفدية الخبيث أحد أخطر الهجمات الإلكترونية في العصر الرقمي الحالي. ووفقًا للإحصائيات العالمية الأخيرة، يتم تسجيل هجوم بفيروس الفدية كل 10 ثوانٍ تقريبًا. يتمثل هذا النوع من الهجمات في حجب بيانات الضحية بالكامل وترميزها، مما يمنعه من الوصول إليها إلا بعد دفع فدية مالية كبيرة. وكلما كانت البيانات المُستهدَفة أكثر سرية وأهمية، زادت استغلال الجناة لهذا الأمر لفرض شروط تعجيزية على الضحية. وفي معظم الحالات، لا يجد المتضرر من هذا الهجوم خيارًا سوى الاستسلام لمطالب المبتزين[2].

3- تصيد البيانات والمعلومات في التهديدات السيبرانية

يعتبر تصيد البيانات والمعلومات عملية احتيالية تعتمد على إرسال رسائل بريد إلكتروني مزيفة تبدو كأنها من مصادر موثوقة، بهدف سرقة بيانات حساسة مثل أرقام بطاقات الائتمان أو بيانات تسجيل الدخول. بمعنى آخر، يتم استغلال ضعف الثقافة الإلكترونية لدى الضحية أو عدم انتباهها للمعلومات المعروضة أمامها، مما يؤدي إلى دفعها لمشاركة معلومات حساسة بإرادتها، مثل بيانات بطاقتها الائتمانية أو كلمات المرور الخاصة بالدخول إلى المنصات الرقمية أو المواقع المختلفة. وتجدر الإشارة إلى أن عمليات تصيد المعلومات تُعد من أكثر الهجمات الإلكترونية شيوعًا، حيث تمثل حوالي 80% من إجمالي

[1] الحسين حسن محمد، اسياسيات الامن السيبراني، القاهرة، مصر , 2022,ص234.

[2] علاء عبد الرزاق محمد السالمي، المدخل الى الامن السيبراني , الذاكرة للنشر و التوزيع , بغداد, العراق, 2022,ص119.

الهجمات التي تستهدف الأفراد والمؤسسات. ووفقًا لتقديرات جوجل، يوجد أكثر من 2.1 مليون موقع مخصص لهذه العمليات الاحتيالية[1].

ثانيا: تطبيق الامن السيبراني في التهديدات الحديثة.

سنتناول في نقاط عديدة الى اهم تطبيقات الامن السيبراني في التهديدات الحديثة يتعلق الأمر في استخدام الذكاء الاصطناعي، التهديد بالهجمات الداخلية، التهديد بالهجمات إنترنت الأشياء.

1- **استخدام الذكاء الاصطناعي:**

يعرف الذكاء الاصطناعي(Artificial Intelligence) بأنه تطوير برامج حاسوبية قادرة على محاكاة السلوك الإنساني الذكي، كما يُعنى بدراسة القدرات العقلية باستخدام نماذج حوسبة)(Computational Models), وقد أصبحت هجمات الذكاء الاصطناعي (AI Attacks) وسيلة يستخدمها المخترقون للوصول إلى بيانات الشركات ذات القيمة العالية لتحقيق مكاسب مادية على حساب هذه المؤسسات [2].

2- **التهديد بالهجمات الداخلية:**

تُعتبر الهجمات الداخلية (Insider Attacks) من أبرز التحديات التي تواجه الأمن السيبراني، حيث تنبع هذه الهجمات من داخل الشركة أو المؤسسة نفسها، وتكون مدفوعة من قبل أفراد يعملون فيها. يتمثل هدف هذه العمليات في تسريب بيانات حساسة لشركات منافسة، مما يؤدي إلى خسائر مالية كبيرة للشركة المستهدفة.

3- **التهديد بالهجمات إنترنت الأشياء:**

يشير مفهوم إنترنت الأشياء إلى مجموعة من الأجهزة والتقنيات التي تتيح الاتصال بين الأجهزة المختلفة والشبكات الإلكترونية، وكذلك بين الأجهزة نفسها. وبفضل التقدم في إنتاج رقائق الكمبيوتر منخفضة التكلفة وتوفر اتصالات النطاق العريض، أصبح لدينا مليارات الأجهزة المتصلة بالإنترنت. وهذا يعني أن الأجهزة اليومية مثل مصابيح الإنارة، أجهزة التكييف، المكانس الكهربائية، الأبواب، السيارات، وغيرها، يمكنها جمع البيانات عبر أدوات الاستشعار والاستجابة بذكاء للمستخدمين. بمعنى آخر، إنترنت

[1] بثينة حبيباتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة الجزائر، المجلد 30, العدد 1, جوان2019, الجزائر، ص6

[2] أبو النصر مدحت محمد، الذكاء الاصطناعي، المجموعة العربية للتدريب والنشر، القاهرة، مصر,2022، ص567.

الأشياء يدمج الأشياء اليومية مع الإنترنت ليسمح بإصدار الأوامر لها واستجابتها تلقائيًا. تشمل هذه الأجهزة أنظمة حوسبة رقمية وميكانيكية قادرة على نقل البيانات بشكل مستقل عبر الشبكات الإلكترونية، ومن الأمثلة عليها: أجهزة الكمبيوتر المكتبية والمحمولة، الهواتف الذكية، وأجهزة الأمان الذكية. ومع زيادة استخدام إنترنت الأشياء من قبل الأفراد والشركات، زادت التحديات المرتبطة بالأمان السيبراني، حيث يتيح اختراق هذه الأجهزة مجالاً واسعاً لهجمات ضارة تُعرف باسم هجمات إنترنت الأشياء[1].

المبحث الثاني: أهمية الأمن السيبراني في العصر الرقمي.

في ظل التحول الرقمي المتسارع، يمثل الأمن السيبراني ركيزة أساسية لحماية الحقوق والحريات العامة والخاصة وضمان استقرار النظام الاجتماعي والاقتصادي. من منظور قانوني، تبرز أهمية الأمن السيبراني في حماية البيانات الشخصية التي تعد جزءًا لا يتجزأ من الحق في الخصوصية المنصوص عليه في المواثيق الدولية والتشريعات الوطنية. إذ تفرض القوانين الحديثة، مثل اللائحة العامة لحماية البيانات (GDPR)في الاتحاد الأوروبي أو القانون الجزائري رقم 18-04[2]، التزامات صارمة على المؤسسات لضمان سرية وسلامة المعلومات، تحت طائلة فرض عقوبات مدنية أو جنائية في حال الإخلال بها[3]. وللتفصيل لهذه المسالة سنتطرق الى دور الامن السيبراني في حماية البنية التحتية الحيوية كمطلب اول، وأهمية الامن السيبراني في الحفاظ على الامن العام كمطلب ثاني.

المطلب الاول: دور الامن السيبراني في حماية البنية التحتية الحيوية.

تلعب الأمن السيبراني دورًا محوريًا في حماية البنية التحتية الحيوية، من خلال صون الأنظمة والمعلومات الحساسة ضد الهجمات الإلكترونية. كما يُعد ضمان استمرارية الخدمات الأساسية وحمايتها شرطًا أساسيًا لأمن الدولة واستقرارها. ولذلك، تُعَدّ استراتيجيات الأمن السيبراني أداةً استراتيجية للدفاع عن المرافق الحيوية والحفاظ على المصالح الوطنية.

---

[1] عبد الجبار حسين الظفري، انترنيت الأشياء دار النجاء، صنعاء، اليمن,2022، ص6.

[2] القانون 18-04، سبق ذكره.

[3] سعيد بن عيسى، الامن السيبراني في الجزائر التحديات والتشريعات، جامعة الجزائر 1 (بن يوسف بن خدة) كلية الحقوق والعلوم السياسية، دار الحكمة للنشر والتوزيع، 2020ص45.

الفرع الأول: مفهوم البنية التحتية الحيوية.

تشمل هذه البنية قطاعات مثل الطاقة، المياه، الصحة، النقل، والاتصالات، التي تعد أساسية لاستمرارية الحياة اليومية والأمن (Critical Infrastructure) في ظل التحول الرقمي الذي تشهده الجزائر.

المرسوم الرئاسي 20-05 المتعلق بوضع منظومة وطنية الامن الأنظمة المعلوماتية تضمن أهمية خاصة لحماية هذه القطاعات.

وفقًا **للمادة 3 من المرسوم 20-05 المتعلق بوضع منظومة وطنية الامن الأنظمة المعلوماتية** [1]**، يتم تعريف البنية التحتية الحيوية على أنها "الأنظمة أو الأصول الفيزيائية أو المعلوماتية التي تعتبر ضرورية لسلامة وأمن الدولة ولضمان استمرارية الخدمات الأساسية". كما يلزم القانون الجهات المشغلة لهذه البنية بتطبيق معايير الأمان السيبراني لحمايتها من أي اختراق قد يؤدي إلى تعطيلها أو استغلالها.**

من جهة أخرى، **المادة 7 من نفس المرسوم**[2] **تشدد على ضرورة وضع استراتيجيات وطنية لتحديد المخاطر السيبرانية وتقييمها، مع التركيز على البنية التحتية الحيوية. يُطلب من المؤسسات المعنية إعداد خطط طوارئ للاستجابة للحوادث السيبرانية، بما يضمن استعادة العمليات بسرعة بعد أي هجوم محتمل.**

فإن الهيئة الوطنية للأمن السيبراني، تلعب دورًا محوريًا في تنسيق الجهود بين القطاعين العام والخاص لتعزيز حماية هذه البنية. تعمل الهيئة على رصد التهديدات السيبرانية، تقديم الدعم الفني، وتحديث الإجراءات الوقائية بشكل مستمر.

وفي إطار العقوبات، نص القانون على معاقبة كل من يحاول تعطيل البنية التحتية الحيوية عبر الهجمات السيبرانية بعقوبات صارمة تصل إلى السجن لمدة تصل إلى 20 عامًا وغرامات مالية كبيرة (المادة 16)[3]. هذا التشديد يعكس أهمية هذه البنية في حياة المواطنين واستقرار الدولة.

[1] المرسوم الرئاسي20-05 المؤرخ في 20 جانفي 2020 المتعلق بوضع منظومة وطنية الامن الأنظمة المعلوماتية، الجريدة الرسمية العدد 04.

[2] المادة 7 المرسوم 20-05 سبق ذكره.

[3] المادة 16 من قانون العقوبات.

بالتالي، يظهر أن التشريع الجزائري يولي اهتمامًا كبيرًا لحماية البنية التحتية الحيوية من خلال فرض التزامات قانونية على الجهات المشغلة، تعزيز التعاون بين القطاعات، وفرض عقوبات رادعة ضد المخالفين.

هذه الجهود تهدف إلى بناء نظام سيبراني آمن يحمي المصالح الوطنية ويضمن استمرارية الخدمات الأساسية[1].

الفرع الثاني: علاقة الامن السيبراني بالبنية التحتية الحيوية.

تكمن علاقة الامن السيبراني بالبنية التحتية الحيوية وفق **المواد 4 و18 من المرسوم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ومن خلال استراتيجية الوطنية في مجال الأنظمة المعلوماتية المعدي لطرف المجلس الوطني لأمن الأنظمة المعلوماتية.**

يقوم المجلس الوطني لأمن الأنظمة المعلوماتية بدراسة العناصر الأساسية للإستراتيجية الوطنية المقترحة من قبل الوكالة الوطنية لأمن الأنظمة المعلوماتية، واعتمادها بعد التحقق من شموليتها وملاءمتها للاحتياجات الوطنية .

كما يُعنى بمراجعة ومصادقة مخطط عمل الوكالة وتقرير نشاطاتها السنوي، إلى جانب دراسة التقارير المتعلقة بتتبع وتنفيذ الاستراتيجية الوطنية وإعطاء الموافقة اللازمة عليها .

ومن بين اختصاصات المجلس أيضًا إبرام اتفاقيات التعاون الدولي والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، فضلاً عن المصادقة على سياسة التصديق الإلكتروني التي تتولاها السلطة الوطنية للتصديق الإلكتروني .

كما يتولى المجلس إقرار تصنيف الأنظمة المعلوماتية حسب مستويات الحساسية والأهمية الاستراتيجية، ويقترح عند الاقتضاء تعديلات على الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية بما يخدم تحسين الحكومة السيبرانية .

وأخيرًا، يُبدي المجلس رأيه الملزم في أي مشروع نص تشريعي أو تنظيمي يتعلق بقطاع أمن الأنظمة المعلوماتية، وذلك ضمن إطار تعزيز البنية القانونية والتنظيمية الوطنية[2].

---

[1] فاطمة الزهراء بلقاسم، حماية البنية التحتية الحيوية في ظل التحديات السيبرانية، دراسة قانونية، جامعة قسنطينة 2 كلية الحقوق والعلوم السياسية، ,2021، ص78.

[2] المادة 4 و 18 من المرسوم 20-05 , سبق ذكره.

تُعنى الوكالة خصوصًا بالمهام التالية:

إعداد عناصر الاستراتيجية الوطنية لأمن نظم المعلومات وعرضها على المجلس الوطني المعني لأجل المصادقة عليها .

تنسيق تنفيذ الاستراتيجية الوطنية لأمن نظم المعلومات بعد اعتمادها من قبل المجلس .

-اقتراح آليات اعتماد مزوّدي خدمات التدقيق في مجال أمن نظم المعلومات .

-إجراء تحقيقات رقمية في حالة وقوع هجمات أو حوادث سيبرانية تستهدف المؤسسات الوطنية .

-جمع وتحليل وتقييم البيانات والمعلومات المتعلقة بأمن نظم المعلومات، وذلك لرصد التهديدات والمخاطر .

-وضع الإجراءات الملائمة لتوفير الأمان للمنشآت التابعة للنظم المعلوماتية .

-متابعة عمليات تدقيق أمن نظم المعلومات لضمان فعاليتها واستمراريتها .

-تقديم الاستشارات والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة لمساعدتها في وضع استراتيجيات أمن النظم المعلوماتية .

-ممارسة اليقظة التقنية والتكنولوجية في مجال أمن نظم المعلومات .

-مرافقة الإدارات والمؤسسات والهيئات العامة والخاصة، بالتشاور مع الهياكل المتخصصة، في التعامل مع الحوادث المتعلقة بأمن نظم المعلومات .

-جرد النظم المعلوماتية وتصنيفها وعرضها على المجلس الوطني للموافقة على تصنيفها .

-إعداد وتحيين الخارطة الوطنية للنظم المعلوماتية المصنفة.

-اقتراح مشاريع القوانين والنصوص التنظيمية في مجال أمن نظم المعلومات بعد الحصول على موافقة المجلس .

-إعداد وتحديث المرجعيات والإجراءات والأدلة العملية الخاصة بأمن نظم المعلومات .

-تقديم التوصيات في مجال أمن نظم المعلومات لتعزيز مستوى الحماية واليقظة .

-اعتماد منتجات أمن نظم المعلومات والتصديق عليها وفق المعايير المحددة .

-اعتماد أنظمة إنشاء وفحص التوقيع الإلكتروني.[1]

-تحديد المعايير والإجراءات الخاصة بمنح علامات الجودة والتصديق والاعتماد للمنتجات ومزوّدي

[1] المادة 18 من المرسوم الرئاسي رقم 20-05، سبق ذكره.

الخدمات في مجال أمن نظم المعلومات، طبقًا للتشريعات والقوانين الجاري بها العمل .

-تنظيم وتنفيذ أنشطة التكوين والتوعية المتعلقة بأمن نظم المعلومات[1].

المطلب الثاني: أهمية الامن السيبراني في الحفاظ على الامن العام

للأمن السيبراني أهمية كبيرة لكل مجتمع ولكل دولة، فالأمن السيبراني مهم على مستوى الفرد في حماية البيانات الشخصية والصور والملفات والفيديوهات والحسابات الشخصية وكلمات المرور والحسابات البنكية. وعلى مستوى المجتمع، من حيث حماية المجتمع من الهندسة الاجتماعية واستهداف السلوك الاجتماعي والبيانات المجمعة والخصوصيات للمجتمع. وعلى مستوى الشركات والمؤسسات، في حماية الأصول الإلكترونية والبيانات والمعلومات وبيانات الموظفين والسيرفرات والمواقع الإلكترونية. وعلى مستوى الدولة، في حماية أمنها الإلكتروني وحماية الأنظمة المالية والاقتصادية والعسكرية والتلفزيون والراديو من الاعتداءات الإلكترونية والقرصنة والتعطيل. ومن هنا سوف نتناول تأثير الهجمات السيبرانية على الامن العام كفرع اول وكفرع ثاني دور الامن السيبراني في تعزيز الاستقرار الوطني.

الفرع الأول: تأثير الهجمات السيبرانية على الامن العام.

في ظل التحول الرقمي الذي تشهده الجزائر، أصبحت الهجمات السيبرانية تهديدًا مباشرًا للأمن القومي. يُعرّف القانون الجزائري بالهجوم السيبراني بأنه أي عمل يهدف إلى تعطيل أو عرقلة الأنظمة المعلوماتية أو سرقة البيانات الحساسة. هذه الهجمات قد تستهدف البنية التحتية الحيوية مثل أنظمة الطاقة، والاتصالات، والصحة، والنقل، مما يؤدي إلى تعطيل الخدمات الأساسية التي يعتمد عليها المواطنون

إذا تم اختراق نظام الكهرباء أو المياه، فإن ذلك يؤدي إلى شلل اقتصادي واجتماعي، حيث تتوقف المصانع عن العمل وتتعطل المرافق الصحية والتعليمية. كما أن استهداف المؤسسات الحكومية والأجهزة الأمنية قد يؤدي إلى تسريب معلومات حساسة أو تعطيل نظم الاتصالات العسكرية، مما يهدد سيادة الدولة وقدرتها على اتخاذ القرارات الاستراتيجية [2].

[1] المادة 18 من المرسوم الرئاسي رقم 20-05 , سبق ذكره.

[2] ناصر بن عبد الله القحطاني, الهجمات السيبرانية واثرها على الامن القومي, مجلة الدراسات الأمنية و الاستراتيجية, جامعة القاهرة المجلد35,العدد2 , 2020,ص150.

علاوة على ذلك، تؤثر الهجمات السيبرانية على الاقتصاد الوطني من خلال استهداف الشركات الكبرى والمؤسسات المالية، مما يؤدي إلى خسائر مالية كبيرة وفقدان الثقة الدولية في الاقتصاد المحلي. كما يمكن استخدام هذه الهجمات كأدوات للتأثير السياسي والاجتماعي عبر شبكات التواصل الاجتماعي، حيث يتم بث الشائعات وزعزعة الاستقرار الداخلي، مما يُمكن أن يؤثر على الانتخابات الوطنية أو يثير الفوضى الاجتماعية .

وفي إطار القانون الجزائري، تُعتبر هذه الهجمات جرائم خطيرة تخضع للملاحقة القضائية بموجب قانون العقوبات الجزائري، الذي ينص على عقوبات صارمة ضد مرتكبي الجرائم السيبرانية، بما في ذلك السجن والغرامات الكبيرة. ومع ذلك، فإن تنفيذ هذه القوانين يتطلب تعزيز الإطار القانوني والمؤسسي لضمان مواجهة هذه التهديدات بشكل فعال[1].

الفرع الثاني: دور الامن السيبراني في تعزيز الاستقرار الوطني

يُعتبر الأمن السيبراني ركيزة أساسية لتعزيز الاستقرار الوطني وضمان استمرارية عمل المؤسسات والخدمات العامة في الجزائر. في **ظل القانون الجزائري رقم 18-05 المتعلق بالتجارة الالكترونية،**[2] وفق لأحكام **المواد 2 و3 و5 منه: يُلزم الأمن السيبراني بحماية البنية التحتية الرقمية من الاختراقات والهجمات السيبرانية، مما يضمن استمرارية تقديم الخدمات الأساسية مثل الصحة، التعليم، والطاقة. وبذلك، يساهم في تحقيق الاستقرار الاجتماعي ومنع أي اضطرابات قد تنجم عن تعطيل هذه الخدمات** [3].

على المستوى الاقتصادي، يلعب الأمن السيبراني دورًا محوريًا في حماية الشركات والمؤسسات المالية من الهجمات الإلكترونية التي تستهدف سرقة البيانات أو تعطيل العمليات. كما يعزز الثقة الدولية في الاقتصاد المحلي من خلال ضمان بيئة رقمية آمنة وجاذبة للاستثمارات الأجنبية. وبفضل الأمن السيبراني،

[1] محمد الأمين بوغرارة، الهجمات السيبرانية و اثرها على الامن القومي، دراسة حالة الجزائر، جامعة الجزائر 3 مجلة الدراسات الاستراتيجية و الأمنية , 2021،ص13

[2] القانون رقم 18-05 المتعلق بالتجارة الالكترونية، المؤرخ في 10ماي 2018، الجريدة الرسمية العدد 28.

[3] نادية بلقاسم، السياسات السيبرانية في الجزائر: نحو الاستقرار وطني مستدام، المؤتمر الوطني حول الامن السيبراني المركز الوطني للدراسات الاستراتيجية 2022.

يمكن للجزائر تحقيق تنمية اقتصادية مستدامة قائمة على الابتكار والتكنولوجيا دون القلق بشأن التهديدات السيبرانية .

أما على المستوى السياسي، فإن الأمن السيبراني يحمي الأنظمة الحكومية والمؤسسات الأمنية من التدخلات الخارجية أو التجسس الإلكتروني. ويضمن سرية المعلومات الحساسة المتعلقة بالسياسات الداخلية والخارجية، مما يعزز قدرة الدولة على اتخاذ قرارات استراتيجية مستقلة. كما يسهم في مكافحة الحملات الإعلامية المغرضة التي تسعى إلى زعزعة الاستقرار السياسي والاجتماعي .

وعلى الصعيد العسكري، يُعد الأمن السيبراني جزءًا لا يتجزأ من الأمن القومي الحديث في الجزائر. فهو يحمي الأنظمة الدفاعية والأسلحة الذكية من الاختراقات التي قد تؤدي إلى فقدان السيطرة عليها أو استخدامها ضد الدولة نفسها. كما يساهم في تعزيز قدرات القوات المسلحة على مواجهة التهديدات السيبرانية وتطوير استراتيجيات دفاعية وهجومية في الفضاء السيبراني[1] .

يعزز الأمن السيبراني الاستقرار الوطني من خلال رفع مستوى الوعي المجتمعي بأهمية الحماية السيبرانية. فعبر تعليم الأفراد كيفية التعامل مع التهديدات الإلكترونية مثل التصيد الاحتيالي والبرمجيات الخبيثة، يمكن تقليل المخاطر الناجمة عن الأخطاء البشرية. وبالتالي، يصبح المجتمع أكثر قدرة على مواجهة التهديدات السيبرانية والمساهمة في بناء بيئة رقمية آمنة ومستقرة .

يُظهر الأمن السيبراني دورًا حاسمًا في تعزيز الاستقرار الوطني عبر حماية البنية التحتية، تأمين الاقتصاد، دعم الاستقرار السياسي، تعزيز القدرات العسكرية[2]، ورفع مستوى الوعي المجتمعي. وهو ما يجعله ضرورة استراتيجية لتحقيق الأمن القومي في الجزائر وفقًا للقانون الجزائري رقم 18-05 المتعلق بالتجارة الالكترونية[3].

---

[1] احمد بن عيسى ، **دور الامن السيبراني في تعزيز الامن الوطني الجزائري**, مجلة العلوم الإنسانية و الاجتماعية, جامعة باتنة ,2019. العدد44,ص45.

[2] سليمان بوزيد، **الامن السيبراني كأداة لتعزيز الاستقرار السياسي والاقتصادي في الجزائر مجلة** القانون والمجتمع جامعة قسنطينة 2020 العدد65ص55.

[3] قانون رقم 18-05 المتعلق بالتجارة الالكترونية سبق ذكره.

خلاصة الفصل:

في ظل التطور التكنولوجي المتسارع الذي يشهده العالم، أصبح الأمن السيبراني أحد الركائز الأساسية لحماية الدول من التهديدات الرقمية المتنامية. يمثل الأمن السيبراني درعًا وقائيًا للأنظمة المعلوماتية والبنية التحتية الحيوية، حيث يعمل على تأمين البيانات الحساسة ومنع الهجمات الإلكترونية التي قد تؤدي إلى خسائر فادحة على المستويين الاقتصادي والاجتماعي. من خلال هذا الفصل، تم تسليط الضوء على مفهوم الأمن السيبراني وأهميته في تعزيز الاستقرار الوطني والدولي، حيث أظهرت الدراسات أن الدول التي تعتمد استراتيجيات سيبرانية قوية تكون أكثر قدرة على مواجهة التحديات الأمنية المعاصرة.

أهمية الأمن السيبراني لا تقتصر فقط على حماية الأفراد والمؤسسات، بل تتعدى ذلك إلى ضمان سيرورة عمل القطاعات الحيوية مثل الطاقة، الصحة، والاتصالات، والتي تعتبر عصب الحياة الحديثة. كما أن التهديدات السيبرانية لم تعد مجرد هجمات تقليدية، بل أصبحت أدوات تستهدف زعزعة الاستقرار السياسي والاقتصادي للدول، مما يجعل من الضروري تبني سياسات وطنية شاملة تعزز الوعي السيبراني وتطور الكفاءات التقنية.

وفي ظل تنامي الجرائم الإلكترونية وتعقيد أساليبها، بات من الواجب على الحكومات والمؤسسات التعاون مع الخبراء المحليين والدوليين لتطوير تشريعات قانونية وتقنية قادرة على التصدي لهذه التهديدات. وبهذا، يمكن القول إن الأمن السيبراني ليس مجرد خيار أو رفاهية، بل هو ضرورة استراتيجية لتحقيق التنمية المستدامة وضمان الاستقرار الوطني في عصر يعتمد بشكل كبير على التكنولوجيا. إن الاستثمار في تعزيز الأمن السيبراني يعد استثمارًا في مستقبل أكثر أمانًا واستقرارًا للأجيال القادم

الفصل الثاني:

دور الأمن السيبراني في مكافحة الجريمة المعلوماتية

في ظل التحول الرقمي المتسارع الذي يشهده العالم، أصبح الاعتماد على التكنولوجيا جزءاً أساسياً من حياة الأفراد والمجتمعات والمؤسسات. ومع هذا التطور الهائل، برزت تحديات جديدة تتعلق بالأمن الرقمي، حيث أصبح العالم الافتراضي مسرحاً لممارسات ضارة تُعرف بالجريمة المعلوماتية. هذه الجرائم، التي تتراوح بين اختراق البيانات وسرقة المعلومات إلى الإضرار بالبنية التحتية الرقمية، باتت تشكل تهديداً حقيقياً للأمن الشخصي والمجتمعي والوطني .

يبرز دور الأمن السيبراني كأحد أهم الوسائل الدفاعية لمواجهة هذه التهديدات والحد من تأثيرها. الأمن السيبراني ليس مجرد أداة تقنية، بل هو استراتيجية شاملة تهدف إلى حماية الأنظمة الرقمية والبيانات الحساسة من الاستغلال غير المشروع. ومن هنا، يأتي التركيز على العلاقة التكاملية بين الأمن السيبراني والجريمة المعلوماتية، حيث يسعى الأول إلى تعزيز المناعة الرقمية ضد الهجمات والتهديدات التي تستهدف النظم والمعلومات .

استعراض الدور المحوري الذي يلعبه الأمن السيبراني في مكافحة الجريمة المعلوماتية، من خلال تقديم رؤية واضحة حول كيفية مواجهة هذه التحديات بأساليب فعالة ومبتكرة. وسيتناول الفصل استراتيجيات الأمن السيبراني الحديثة التي تهدف إلى تعزيز الحماية الرقمية، بالإضافة إلى تسليط الضوء على مفهوم الجريمة المعلوماتية وأبرز أشكالها وأنواعها. ومن خلال ذلك، نسعى إلى تقديم إطار شامل يساعد على فهم كيفية تحقيق التوازن بين الابتكار التكنولوجي والأمان السيبراني، بما يضمن بناء بيئة رقمية آمنة ومستدامة للجميع، ومن هنا سنتطرق الى الإطار المفاهيمي للجريمة المعلوماتية باعتبارها محور الحماية في إطار الامن السيبراني كمبحث اول وكمبحث ثاني المبحث الثاني: استراتيجيات الأمن السيبراني لمكافحة الجريمة المعلوماتية.

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية موضوع الأمن السيبراني

المبحث الثاني: استراتيجيات الأمن السيبراني لمكافحة الجريمة المعلوماتية.

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية موضوع الأمن السيبراني

تعد الجريمة المعلوماتية واحدة من أبرز التحديات التي تواجه المجتمع الرقمي في العصر الحديث، وهي جرائم تتم عبر استغلال تقنيات المعلومات والاتصالات لتحقيق أهداف غير مشروعة. تُعرّف الجريمة المعلوماتية بأنها كل فعل أو امتناع يؤدي إلى تعطيل أو اختراق أو سرقة البيانات أو الأنظمة المعلوماتية باستخدام الوسائل الرقمية. ومن أبرز أشكال هذه الجرائم الاختراق الإلكتروني، القرصنة، الاحتيال الإلكتروني، التصيد الاحتيالي، وسرقة الهوية الرقمية. مع تطور التكنولوجيا وتوسع استخدام الإنترنت، أصبحت هذه الجرائم تمثل تهديدًا خطيرًا للأفراد والمؤسسات وحتى الدول، مما يستدعي ضرورة وضع استراتيجيات فعالة لتعزيز الأمن السيبراني كإطار حماية شامل يهدف إلى مكافحة هذه الجرائم والحد من تأثيراتها السلبية على الاقتصاد والمجتمع، من خلال هذه المسالة سنتطرق الى مضمون الجريمة المعلوماتية كمطلب الأول، وأبرز أشكال الجرائم المعلوماتية كمطلب الثاني.

المطلب الأول: مضمون الجريمة المعلوماتية

تشهد العقود الأخيرة تطورًا تقنيًا غير مسبوق، مما أدى إلى ظهور أنماط جديدة من الجرائم مرتبطة باستخدام التكنولوجيا الحديثة. في هذا السياق، برز مفهوم الجريمة المعلوماتية كإحدى الظواهر التي فرضتها الثورة الرقمية وأصبحت تمثل تحديًا حقيقيًا للأمن العالمي. تشير هذه الجرائم إلى الأفعال غير المشروعة التي تستهدف الأنظمة المعلوماتية أو البيانات الرقمية بهدف تحقيق منافع غير قانونية أو الإضرار بالآخرين. ومع تنوع أساليبها وأشكالها، بات من الضروري فهم مفهومها بشكل دقيق لمواجهتها وتطوير آليات قانونية وتقنية لمكافحتها. يسعى هذا المطلب إلى استعراض التعريفات المختلفة للجريمة المعلوماتية وتحديد أبرز أشكال الجرائم المعلوماتية

الفرع الأول: تعريف الجريمة المعلوماتية

تتكون عبارة "الجريمة المعلوماتية" من كلمتين: "الجريمة" و"المعلوماتية". تشير كلمة الجريمة إلى السلوكيات والأفعال التي تخرج عن إطار القانون، بينما يشير مصطلح المعلوماتية إلى العلم الذي يعنى

بدراسة وتجميع وتنظيم وتخزين واسترجاع المعلومات باستخدام التقنيات الحديثة[1]. كما يهتم هذا العلم بأنظمة البرمجة والنظم المعلوماتية، مما يجعله مرتبطًا بعدة مجالات علمية أخرى. وبالتالي، يمكن القول إن المعلوماتية تعتمد على العلاقة بين المعلومات والتقنيات المستخدمة لمعالجتها.

على الرغم من أهمية الموضوع، لا يوجد اتفاق قانوني موحد حول مفهوم الجريمة المعلوماتية، نظرًا للتطور المستمر لأنماط الإجرام المرتبطة بتكنولوجيا المعلومات والاتصالات. فقد أُطلقت العديد من المصطلحات للإشارة إلى هذه الظاهرة، مثل جرائم الكمبيوتر، جرائم الهاكرز، الاختراقات، جرائم الإنترنت[2]، الغش المعلوماتي، الاحتيال المعلوماتي، الاختلاس المعلوماتي، وأخيراً الجريمة الإلكترونية، وهي الأكثر شيوعًا .

تعرف الجريمة الإلكترونية بأنها الجرائم التي تُرتكب باستخدام الحاسوب أو الشبكات أو المعدات الرقمية مثل الهواتف الذكية وغيرها[3]. وتشمل جميع الأفعال غير المشروعة التي تتم عبر الوسائل الإلكترونية وأدوات الاتصال الحديثة كالهواتف والفاكسات والحاسوب. وقد تعددت التعريفات الفقهية لهذه الجرائم بسبب اختلاف وجهات النظر حول تحديد نطاقها، سواء كانت تتعلق فقط بالجرائم التي تستهدف الحواسيب أو تلك التي تشمل جميع الأفعال غير القانونية المرتكبة باستخدام التكنولوجيا الحديثة.

أولا :الاتجاه الضيق لمفهوم الجريمة المعلوماتية

أنصار هذا الاتجاه ركزوا على تعريف الجريمة المعلوماتية بناءً على معيار وسيلة ارتكابها، أي الحاسوب. فاعتبروها كل فعل غير مشروع يتطلب استخدام تقنية الكمبيوتر بشكل كبير لتنفيذه أو لمعاقبته[4]. كما عرفوها بأنها الجرائم التي تقع على الحاسوب أو داخل نظامه فقط. ومن بين هذه التعريفات ما جاء به الفقيه الألماني تيدمان، حيث قال إنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب."[5]

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الإسكندرية، 2005، ص97.

[2] محمد إبراهيم غازي الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص 120.

[3] محمد علي العربان الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص 43.

[4] نائلة عادل محمد فريد قورة، سبق ذكره ، ص 28.

[5] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص 84.

وبالمثل، عرفها جون فورستر بأنها "أي فعل إجرامي يستخدم الكمبيوتر كأداة رئيسية لارتكابه.[1]" إذن، تشترك هذه التعريفات في اعتبار الحاسوب العنصر الأساسي في وقوع الجريمة.

بعض أنصار الاتجاه الضيق لتعريف الجريمة المعلوماتية ركزوا على معيار النتيجة كعنصر أساسي في تعريفها. من بين هؤلاء، الأستاذ الفرنسي "ماس"، الذي عرف الجريمة المعلوماتية بأنها "تلك الاعتداءات القانونية التي ترتكب باستخدام تقنيات المعلومات بغرض تحقيق ربح[2]." يبرز هذا التعريف أن الغاية الأساسية لهذه الجرائم هي تحقيق مكاسب مادية، مما يجعله يركز على معيار النتيجة.

أما الفقيه "روزملات"، فقد قدم تعريفًا آخر للجريمة المعلوماتية باعتبارها "نشاطًا غير مشروع يستهدف الوصول إلى المعلومات المخزنة داخل الحاسوب أو نسخها أو تغييرها أو حذفها[3]." يعتمد هذا التعريف على معيارين: الأول يتعلق بموضوع الجريمة (محاولات الوصول غير المشروع للمعلومات)، والثاني يتعلق بالوسيلة المستخدمة (الحاسوب). وبالمثل، تم تعريف الجريمة المعلوماتية بأنها "أي جريمة يتطلب ارتكابها توفر معرفة بتقنية الحاسوب لدى مرتكبها[4]"، أو "أي فعل غير مشروع يكون فيه الإلمام بالتكنولوجيا شرطًا لتنفيذه".

يتضح من هذه التعريفات أن الجريمة المعلوماتية ترتبط بشكل كبير بالمعرفة التقنية واستخدام الحاسوب. ومع ذلك، يمكن ملاحظة بعض الانتقادات الموجهة لهذه التعريفات:

1-حصر الجريمة في نطاق المعرفة التقنية: إذ إن هذه التعريفات تشترط أن يكون لدى مرتكب الجريمة مستوى عالٍ من المعرفة التقنية، وهو ما لا يحدث دائمًا. فعلى سبيل المثال، قد يتم إتلاف البيانات المخزنة دون الحاجة إلى معرفة تقنية كبيرة، ومع ذلك تُعتبر هذه الأفعال ضمن الجرائم المعلوماتية.

2-قصور التعريفات عن الإحاطة بجميع أشكال الإجرام المعلوماتي: حيث ركز البعض على موضوع الجريمة، بينما ركز آخرون على وسيلة ارتكابها أو على النتيجة المتوقعة

ثانيا: الاتجاه الموسع لتعريف الجريمة المعلوماتية

نظرًا للانتقادات الموجهة للاتجاه الضيق، حاول بعض الفقهاء تقديم تعريفات أوسع وأشمل لظاهرة

[1]خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة، الأردن، 2011، ص29.
[2]محمد علي العريان، سبق ذكره ، ص43.
[3]نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الأردن، 2010، ص48.
[4]عادل يوسف عبد النبي البشكري، "الجريمة المعلوماتية و أزمة الشرعية الجزائية"، العدد السابع، الكوفة، ص113.

الجريمة المعلوماتية، بهدف تغطية جميع أبعادها وتجنب قصور التحديدات السابقة. تباينت تعريفاتهم بناءً على المعايير التي اعتمدوا عليها، وكذلك بناءً على مدى امتداد الجريمة المعلوماتية في بيئتها الرقمية.

من بين التعريفات التي قدمها أنصار هذا الاتجاه: "كل سلوك إجرامي يتم بمساعدة الحاسوب"، أو "كل جريمة تحدث في محيط أجهزة الحاسوب[1]." يُفهم من هذه التعريفات أن الجريمة المعلوماتية تشمل أي سلوك غير مشروع يتطلب مشاركة الحاسوب، معتمدة في ذلك على معيار الوسيلة.

وقد عرفها البعض الآخر بأنها "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتكنولوجيا المعلوماتية، ويهدف إلى الاعتداء على الأموال المادية أو المعنوية." هذا التعريف يتوافق مع تعريف منظمة التعاون الاقتصادي والتنمية في أوروبا، التي وصفت الجريمة المعلوماتية بأنها "كل فعل أو امتناع عن فعل يؤدي إلى الاعتداء على الأموال المادية أو المعنوية[2]، سواء بطريقة مباشرة أو غير مباشرة، كنتيجة لاستخدام تقنيات المعلوماتية"[3].

يتمثل الهدف الأساسي للجريمة المعلوماتية في الاعتداء على الأموال المادية أو المعنوية، سواء كان ذلك بطريقة مباشرة أو غير مباشرة. وقد عرف الفقيه "ستين سكيولبيرغ" الجريمة المعلوماتية بأنها "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لارتكابه وتحقيقه، وكذلك لملاحقته قضائيًا." يشترط هذا التعريف أن يكون مرتكب الجريمة ملمًا بشكل كبير بتقنيات المعلومات، مما يجعله يستحق الجزاء القانوني والملاحقة القضائية[4] .

من خلال هذه التعريفات، يتضح أن الاتجاه الموسع قد أضاف بعدًا أوسع لمفهوم الجريمة المعلوماتية؛ إذ يكفي أن يكون للحاسوب دور مباشر أو غير مباشر في النشاط الإجرامي حتى يُعتبر الفعل جريمة معلوماتية. أما على المستوى الدولي، فإن تعريف الجريمة المعلوماتية يعتمد على الغرض من استخدام المصطلح. فهناك مجموعة محدودة من الأفعال التي تمس السرية والنزاهة والبيانات وأنظمة الكمبيوتر، والتي تعتبر جوهر الجرائم الإلكترونية. كما تشمل الأعمال المرتبطة باستخدام الحاسوب لتحقيق مكاسب شخصية أو مالية أو إلحاق ضرر بالآخرين، بما في ذلك الجرائم المتعلقة بمحتويات الكمبيوتر.

---

[1]أمير فرج يوسف الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الكومبيوتر و الانترنت، الطبعة الأولى، مكتبة الوفاء القانونية، مصر، 2011، ص 10. محمود إبراهيم غازي، المرجع السابق، ص 118.

[2]نهلا عبد القادر المومني، سبق ذكره ، ص49.

[3] علي حسن الطوابلة، الجرائم الالكترونية، مؤسسة الفخراوي للدراسات والنشر، البحرين، 2008، ص 94

[4] علي حسن الطوابلة, سبق ذكره. ص50

ثالثا: موقف المشرع الجزائري من تعريف الجريمة المعلوماتية

اعتمد المشرع الجزائري مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1]" للدلالة على الجرائم المعلوماتية حسب نص المادة 2 **وتنص على أنه: " يقصد في مفهوم هذا القانون بما يأتي أ. الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.. حيث اعتبر أن النظام المعلوماتي وما يحتويه من مكونات غير مادية يمثل محور الجرائم المعلوماتية. ويُعد نظام المعالجة الآلية للمعطيات الشرط الأساسي الذي يجب توفره لتحقق أركان الجريمة. وبالرجوع إلى قانون العقوبات الجزائري، نجد أنه لم يقدم تعريفًا محددًا لجرائم الإنترنت، بل اكتفى بتجريم بعض الأفعال تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات"، وذلك في المواد من المادة 394 مكرر إلى المادة 394 مكرر 7** .

وفقًا **للقانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، قدّم المشرع الجزائري تعريفًا موسعًا للجرائم المعلوماتية، حيث شملت –إضافة إلى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أي جريمة أخرى تُرتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية. وبذلك، لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر فقط على الأفعال التي تكون فيها المنظومة المعلوماتية محل الاعتداء، بل تمدد ليشمل الأفعال التي تُستخدم فيها المنظومة المعلوماتية كوسيلة لارتكاب الجريمة .

المشرع الجزائري تطرق أيضًا إلى الجرائم الإلكترونية والعقوبات المقررة لها من خلال **قانون التجارة الإلكترونية رقم 05/ 18**[2]، وتحديدًا في الفصل الثاني من الباب الثالث تحت عنوان "الجرائم والعقوبات"، الذي شملها **في المواد من 37 إلى 48**. ومع ذلك، لم يقدم هذا القانون تعريفًا واضحًا للجريمة المعلوماتية.

اعتمد المشرع الجزائري معيارًا ثالثًا لتحديد نطاق الجرائم الإلكترونية، وهو القانون الواجب التطبيق أو ما يُعرف بالركن الشرعي للجريمة، والذي يتم النص عليه في قانون العقوبات. كما استند إلى معيار رابع يتمثل في اعتبار أن الجريمة الإلكترونية تُرتكب ضمن إطار نظام معلوماتي أو نظام اتصالات إلكتروني[3]،

---

[1] المادة الثانية من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، المعدل والمتمم.

[2] القانون18-05 المتعلق بالتجارة الالكترونية، سبق ذكره.

[3] انظر: المادة 2 من القانون رقم 09/04 السابق ذكرها أعلاه

كما هو منصوص عليه **في المادة 2 من القانون رقم 09-04**.فإن نص المادة 2 من هذا القانون، الذي يشير إلى "**أي جريمة أخرى تُرتكب أو يسهل ارتكابها بواسطة المنظومة المعلوماتية"، لا يكفي بمفرده لتجريم الأفعال التي تقع باستخدام هذه المنظومة. فطالما لم يتم تحديد أركان كل فعل مجرم بشكل واضح وصريح في نصوص قانونية موضوعية، مع تحديد العقوبات المقررة لها، فإن هذا الأمر يتعارض مع مبدأ شرعية التجريم والعقاب. واستخدام عبارة أي جريمة أخرى**" من قبل المشرع الجزائري يثير تساؤلات قانونية حول مدى إمكانية متابعة شخص جزائيًا عن جرائم تقليدية تم ارتكابها عبر منظومة معلوماتية، خاصة في غياب نصوص جزائية صريحة تجرّم هذه الأفعال إذا ارتُكبت باستخدام التكنولوجيا الحديثة.

لذلك، يُستحسن بالمشرع الجزائري أن يعمل على تعديل النصوص القانونية القائمة لتكون أكثر شمولية واستيعابًا للصور المتطورة للجرائم التقليدية التي قد تُرتكب بواسطة المنظومة المعلوماتية. وهذا التعديل سيساهم في تحقيق التوازن بين التصدي لهذه الجرائم المستجدة والحفاظ على مبدأ شرعية التجريم والعقاب.

الفرع الثاني: الدوافع او الأسباب الرئيسية لانتشار الجريمة المعلوماتية

لقد شهد العالم في العقود الأخيرة طفرة تكنولوجية هائلة غيرت من مفهوم التعاملات اليومية، وأصبحت فيها التكنولوجيا عنصرًا أساسيًّا في جميع مجالات الحياة، من التعليم والصحة إلى التجارة والصناعة. ومع هذا التوسع الكبير في استخدام الحواسيب والإنترنت، ظهرت تحديات جديدة تهدد أمن وخصوصية الأفراد والمجتمعات، من بينها الجريمة المعلوماتية التي أصبحت أحد أكثر أنواع الجرائم انتشارًا وخطورة في العصر الحديث.

ولا يخفى على أحد أن هذه الجرائم لا تعترف بالحدود الجغرافية، وتتخذ أشكالًا متعددة ومتطورة مثل القرصنة، والاحتيال الإلكتروني، وسرقة البيانات، ونشر البرمجيات الخبيثة لهذا سوف نتطرق الى الدوافع او الأسباب الذاتية لهذه الجريمة المعلوماتية[1].

أولا: دوافع او الأسباب الذاتية

1-: الرغبة في الانتقام

الرغبة في الانتقام تعد من الدوافع القوية التي تكمن داخل النفس البشرية. فهناك العديد من الأفراد الذين يتعرضون لظلم أو معاملة غير عادلة من قبل جهات مثل الشركات، المنظمات الحكومية، أو حتى

[1]عادل يوسف عبد النبي البشكري، سبق ذكره, ص124

المصارف. نتيجة لذلك، يلجأ هؤلاء الأفراد إلى استغلال معرفتهم وخبراتهم التقنية للقيام بأعمال انتقامية ضد هذه الجهات. غالبًا ما يكون لديهم إلمام كافٍ بخفايا عمل هذه المؤسسات، مما يمكنهم من تنفيذ جرائم إلكترونية تسبب خسائر مالية كبيرة للجهة المستهدفة[1].

2-: الطمع وحب الثراء السريع

المال يعتبر المحرك الأساسي لحياة الإنسان، وهو ما يدفع بعض الأفراد إلى اللجوء للقرصنة أو السرقة أو الاختلاس باستخدام الحاسب الآلي. الهدف هنا هو تحقيق الثراء السريع دون بذل الكثير من الجهد أو التكلفة. قد تكون دوافعهم تلبية الاحتياجات الأساسية أو تحقيق أحلام الثراء والمكاسب المادية السريعة.

3-: الدوافع النفسية

تتجلى هذه الدوافع في رغبة الفرد لإثبات ذاته والتفوق على تقنيات حديثة ومعقدة. غالباً ما يتم تصوير مرتكبي الجرائم الإلكترونية في الذهن العام كأشخاص أذكياء يستحقون الإعجاب بدلاً من اعتبارهم مجرمين يجب معاقبتهم. يسعى هؤلاء الأفراد إلى إظهار براعتهم وقدرتهم على التغلب على التحديات التقنية. عندما تظهر تقنيات جديدة، يشعر هؤلاء الأفراد بشغف كبير لاختبارها واكتشاف طرق لتحطيمها أو التفوق عليها[2].

4-: الدوافع العقائدية

العقيدة تمثل واحدة من أقوى الدوافع التي تحرك الإنسان، حيث يصبح مستعدًا للتضحية بحياته بالكامل من أجلها. وبالتالي، فإن القيام بأعمال أقل أهمية يبدو أمرًا سهلًا بالنسبة لهم. هناك من يقوم باختراق أجهزة أو مواقع إلكترونية بناءً على تفسيرات دينية خاطئة أو أفكار متطرفة. قد يعتقدون أن اختراق مثل هذه الأنظمة هو وسيلة لفضح أسرار معينة أو تشويه صورة جهة معينة بسبب اختلاف المذاهب أو الطوائف الدينية[3] .

5: الدوافع العنصرية

تتمثل هذه الدوافع في التمييز بين قبيلة وأخرى أو بين أعراق مختلفة. بعض الأفراد يحملون مشاعر

[1] عادل يوسف عبد النبي البشكري، سبق ذكره, ص125

[2] نهلا عبد القادر المومني, سبق ذكره,ص65

[3] نهلة عبد القادر المؤمني، الجرائم المعلوماتية ، عمان , دار الثقافة , جامعة البلقاء التطبيقية, 2008 , ص45.

عدائية تجاه قبائل أو أعراق أخرى، مما يدفعهم إلى تنفيذ أعمال تخريبية أو نشر الشائعات والأكاذيب ضدهم. قد يستخدمون الجرائم المعلوماتية كوسيلة لتدمير سمعة أو إحداث مشاكل للقبائل أو الأعراق الأخر

6-: الدوافع السياسية والإيديولوجية

في عصرنا الحالي، برزت العديد من المنظمات التي تتبنى أفكارًا وأيديولوجيات سياسية أو دينية معينة، وتسعى للدفاع عن هذه الآراء من خلال تنفيذ أفعال إجرامية ضد معارضيها. يتم ذلك غالبًا عبر التشهير بهم واستغلال شبكة الإنترنت لنشر أفكارهم وتجنيد الأفراد. يُعتبر هذا العصر الجديد للإرهاب مميزًا بالدور المحوري الذي تلعبه شبكة الإنترنت في نقل الأفكار والخبرات بين الجماعات والأفراد الذين يشكلونها .

بات الإرهاب وثيق الصلة بالتكنولوجيا الحديثة لدرجة أن "الإرهاب الإلكتروني" أصبح أحد سمات الألفية الثالثة. يتميز الإرهاب الإلكتروني باستخدام الوسائل التقنية المتطورة مثل المواد المعلوماتية والشبكات الإلكترونية، مما يجعل البنية التحتية المعلوماتية وأنظمة الحوسبة هدفًا رئيسيًا للجماعات الإرهابية [1].

تتضاعف خطورة الإرهاب الإلكتروني في الدول المتقدمة، حيث تعتمد بنيتها التحتية بشكل كبير على الحواسيب الآلية والشبكات المعلوماتية، مما يجعلها أكثر عرضة للتهديدات الإلكترونية. فبدلاً من استخدام وسائل تقليدية مثل المتفجرات، يمكن للجماعات الإرهابية تحقيق أهدافها من خلال الضغط على لوحة المفاتيح فقط. قد يؤدي ذلك إلى تدمير البنية المعلوماتية، وإغلاق المواقع الحيوية، مثل أنظمة القيادة والاتصالات، أو تعطيل شبكات الدفاع الجوي، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو شل محطات إمداد الطاقة والمياه، أو اختراق النظام المصرفي، مما يسبب أضرارًا جسيمة على الصعيد العالمي.

7-: الدوافع الاجتماعية

يلعب التحضر دورًا كبيرًا في انتشار الجرائم الإلكترونية بشكل عام. مع الهجرة الكبيرة من المناطق الريفية إلى المدن الكبرى والمناطق الحضرية، يواجه الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية صعوبات كبيرة. هذه الحياة غالبًا ما تكون باهظة التكاليف وتحتاج إلى مهارات عالية، مما يدفع هؤلاء الأفراد إلى الاستقرار في الأحياء الهامشية أو مدن الصفيح (أو البيوت القصديرية) .

من بين العوامل التي تدفع البعض إلى الاستثمار في الجرائم الإلكترونية هي الحاجة إلى رأس مال كبير ،

[1] احمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي ، الإسكندرية,2005,ص126.

والتحضر الذي يُعتبر سببًا رئيسيًا لزيادة هذه الجرائم في بعض الدول كما يرى البعض. بالإضافة إلى ذلك، تلعب البطالة دورًا بارزًا كدافع اجتماعي، حيث تتشابه الجريمة الإلكترونية مع الجرائم التقليدية في فالبطالة والظروف الاقتصادية الصعبة تتركز بشكل كبير بين الشباب، مما يجعلهم عرضة لاستغلال معرفتهم التقنية في الأنشطة الإجرامية الإلكترونية .

كما أن الضغوط الاجتماعية مثل الفقر، البطالة، الأمية، والظروف الاقتصادية القاسية تُشكل عوامل ضاغطة على المجتمع بشكل عام وعلى الشباب بشكل خاص. هذه الضغوط تولد مشاعر سلبية لدى شرائح واسعة من الناس ضد الظروف المحيطة والمجتمع نفسه، مما يدفعهم إلى اتباع أساليب تأقلم غير قانونية، مثل الاتجار الإلكتروني بالبشر أو الجنس أو الانخراط في الجرائم الإلكترونية[1].

8-دوافع تتعلق بخصائص الجريمة المعلوماتية:

ا: خاصية الإزالة (Removable)

الجريمة المعلوماتية لا تتطلب إزالة البيانات أو الموارد المستهدفة، بل يمكن نسخها فقط دون التأثير على وجودها الأصلي .

ب: خاصية التوافر (Available)

المعلومات متوفرة في كل مكان، وجاهزة لأن تكون هدفًا للجريمة .

ج: **خاصية القيمة (Valuable)**

بعض المعلومات تحمل قيمة كبيرة، مثل بيانات بطاقات الائتمان، الحسابات البنكية، والتصاميم، مما يجعلها هدفًا مغريًا للمجرمين

د: خاصية المتعة (Enjoyable)

بعض الجرائم الإلكترونية تُعتبر ممتعة بالنسبة للمجرمين، مثل سرقة الموسيقى أو المال بطريقة سهلة وغير مباشرة .

هـ: خاصية الديمومة (Durable)

الأدوات والبرامج المسروقة يمكن استخدامها لفترات طويلة، مما يزيد من جاذبيتها للمجرمين .

و: خاصية سرعة التنفيذ

تنفيذ الجرائم المعلوماتية لا يتطلب وقتًا طويلًا. فبضغطة واحدة على لوحة المفاتيح، يمكن نقل ملايين

[1]احمد خليفة الملط, سبق ذكره,ص127.

الدولارات من مكان إلى آخر. ومع ذلك، هذا لا يعني أنها لا تحتاج إلى إعداد مسبق أو استخدام أدوات وبرامج متخصصة [1].

ي: خاصية التنفيذ عن بعد

في معظم الجرائم المعلوماتية (ما عدا جرائم سرقة معدات الحاسب)، لا يتطلب الأمر وجود الفاعل في موقع الجريمة. يمكن للمجرم تنفيذ الجريمة وهو في دولة بعيدة تمامًا عن مكان وقوع الجريمة سواء تم ذلك من خلال اختراق الشبكات المستهدفة، اعتراض عمليات التحويل المالي، سرقة المعلومات الحساسة، أو تنفيذ أعمال تخريبية، فإن الجرائم الإلكترونية تظل تشكل خطرًا كبيرًا .

الجاذبية: تمثل سوق المعلومات، الحواسيب، والإنترنت ثروة ضخمة تجذب المجرمين وأعمال الجريمة المنظمة. فقد أصبحت هذه المجالات أكثر جذبًا لاستثمار الأموال وغسلها، مع استخدام الكثير منها لتطوير تقنيات وأساليب متطورة تمكنهم من اختراق الشبكات، سرقة المعلومات وبيعها، سرقة أموال البنوك، اعتراض العمليات المالية وتحويل مسارها، أو حتى استغلال أرقام البطاقات البنكية لتحقيق مكاسب غير قانونية[2].

المطلب الثاني: أبرز أشكال الجرائم المعلوماتية.

في ظل التطور التكنولوجي المتسارع والتحول الرقمي الذي يشهده العالم في مختلف المجالات، أصبحت التكنولوجيا جزءًا لا يتجزأ من الحياة اليومية، سواء على المستوى الفردي أو المؤسسي. ومع هذا التوسع الكبير في استخدام الحواسيب والإنترنت وشبكات الاتصال، ظهرت أنماط جديدة من الجرائم تُعرف بـ "الجرائم المعلوماتية أو "الجريمة الإلكترونية"، والتي تُعدّ امتدادًا للسلوك الإجرامي في البيئة الرقمية.

وتُعرَّف الجرائم المعلوماتية عمومًا بأنها أي فعل إجرامي يتم ارتكابه باستعمال الحاسوب أو الشبكة المعلوماتية كوسيلة رئيسية لتحقيق الغرض الجنائي، سواء كان ذلك عن طريق اختراق الأنظمة، أو سرقة البيانات، أو الاحتيال الإلكتروني، أو نشر المحتوى الضار، وغيرها من الأساليب التي تستغل الثغرات التقنية لتحقيق مكاسب غير مشروعة.

[1] نهلة عبد القادر المؤمني, سبق ذكره ص77.

[2] احمد خليفة الملط، سبق ذكره ، ص128.

وقد أدت طبيعة هذه الجرائم إلى تحديات كبيرة على المستويات القانونية والاجتماعية والأمنية، حيث تتسم بالسرعة، وعدم التحديد الجغرافي، وقدرتها على التأثير على أفراد ومؤسسات وحتى دول بأكملها. كما أن تطور أساليب الاعتداء الإلكتروني يجعل من الضروري مواكبة التشريعات الوطنية والدولية لهذا النوع من الجرائم، وتطوير آليات رقابية وتقنية لمواجهتها، لذلك سندرس كفرع اول الجرائم المالية الإلكترونية (الاحتيال الإلكتروني، غسل الأموال)، وكفرع ثاني الجرائم المرتبطة بالبيانات الشخصية (سرقة الهوية، انتهاك الخصوصية).

الفرع الأول: الجرائم المالية الإلكترونية (الاحتيال الإلكتروني، غسل الأموال).

تُعَدّ الجرائم المالية الإلكترونية من أخطر أنواع الجرائم في العصر الحديث، حيث تُستغل فيها التقنيات الرقمية لارتكاب عمليات احتيال، غسيل أموال، أو سرقة بيانات مالية، مما يهدد الأمن المالي للدول والافراد على حد سواء. وتنبع خطورتها من سرعة انتشارها وصعوبة كشف مرتكبيها بسبب طبيعتها العابرة للحدود سنتطرق اليها بالتفصيل:

أولا: مبدأ عمل الفيروسات يختلف بناءً على أسلوب تصميمها

فمنها ما يبدأ بالعمل بمجرد فتح الرسالة التي تحتوي عليها، ومنها ما ينشط بمجرد تشغيل البرنامج الذي يحمله. وتُعد هذه الفيروسات من أخطر وأكثر جرائم الإنترنت انتشاراً وتأثيراً. يعود تاريخ ظهور الفيروسات إلى أربعينيات القرن الماضي، عندما تحدث عنها العالم الرياضي "جون فون نيومان" في سياق الحوسبة دون الاتصال بشبكة الإنترنت. ومن أشهر الأمثلة على الفيروسات: فيروس رسائل الحب وفيروس الدودة الحمراء، حيث تسبب الأخير في إحداث أعطال في أكثر من ربع مليون جهاز كمبيوتر حول العالم خلال أقل من 9 ساعات في عام 2001[1]

ثانيا: جرائم الاختراقات.

تُعرَّف عملية الاختراق بأنها دخول غير مصرح به إلى أجهزة أو شبكات الغير، ويتم ذلك باستخدام برامج متطورة ينفذها الأفراد الذين يمتلكون الخبرة الكافية لتخطي أنظمة الحماية المتخذة لتأمين تلك الأجهزة أو الشبكات .

[1] منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005,ص36.

تختلف دوافع الاختراق باختلاف أهداف المخترقين؛ فبعضهم قد يقوم بالاختراق بدافع الفضول، بينما يسعى البعض الآخر إلى سرقة المعلومات، وهو الهدف الأكثر شيوعاً. يتمثل هذا النوع من الجرائم في الوصول إلى بيانات حساسة قد تكون مطروحة للبيع مقابل مبالغ مالية .

قد يكون الهدف أيضاً تعديل أو تحريف أو تعطيل المعلومات الموجودة في أجهزة الضحايا، وهو من أخطر أنواع الاختراقات. ومن أبرز ضحايا هذه الجرائم مواقع الإنترنت، حيث يقوم المخترقون بتغيير تصاميمها أو البيانات الموجودة عليها، وهي العملية المعروفة باسم [1]تغيير وجه الموقع.

ثالثا: جريمة تعطيل الأجهزة والشبكات:

يمكن أن يؤدي هذا النوع من الجرائم إلى تعطيل أجهزة الحاسوب عن طريق استهداف برامجهما. كما أن تعطيل البرامج قد يتسبب في حدوث أعطال فنية تؤثر على القطع الإلكترونية للأجهزة .

طريق إرسال كميات كبيرة من الرسائل باستخدام أساليب فنية معينة إلى الأجهزة أو الشبكات المستهدفة، وهو ما يؤدي إلى إعاقة عملها وإيقافها عن أداء وظائفها بشكل طبيعي[2]

رابعا: جريمة النصب والاحتيال[3]:

أصبح التعاقد عبر الإنترنت ضرورة حيوية نظرًا للسرعة والسهولة التي يوفرها هذا النوع من التعاملات. ومع ذلك، فقد رافق هذه الميزة العديد من السلبيات، والتي تمثلت في أفعال إجرامية تُعرف بالنصب والاحتيال. ومن بين صور هذه الجرائم:

– خرق التعاملات الإلكترونية: من خلال أساليب احتيالية مبتكرة، مما أدى إلى زيادة حالات النصب التي لا يزال يسقط ضحيتها عدد كبير من مستخدمي الإنترنت .

–أما الصورة الأكثر وضوحًا للاحتيال فهي سرقة بيانات البطاقات الائتمانية واستغلال هذه المعلومات لسرقة الأموال الموجودة في حسابات الضحايا. ومن السمات البارزة لهذه الجرائم أن مرتكبيها يتمكنون بسهولة من الهروب والتستر، مما يجعل من الصعب للغاية تتبعهم أو القبض عليهم.

[1]منير محمد الجنبيهي ممدوح محمد الجنبيهي، سبق ذكره ، ص37.

[2] منير محمد الجنبيهي ممدوح محمد الجنبيهي سبق ذكره ص38.

[3]عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر كلية الحقوق والعلوم السايسية، جامعة د. الطاهر ،مولاي، سعيدة، سنة 2015/2016,ص23.

الفرع الثاني: الجرائم المرتبطة بالبيانات الشخصية (سرقة الهوية، انتهاك الخصوصية).

تُعَدّ الجرائم المرتبطة بالبيانات الشخصية من أبرز التحديات التي تواجه العالم في العصر الرقمي، حيث تتعرض المعلومات الحساسة للاختراق والسرقة والاستغلال غير المشروع، مما يهدد خصوصية الأفراد وحقوقهم. وتتبع خطورتها من الآثار المترتبة عليها، مثل الاحتيال الإلكتروني وانتحال الهوية، والتي تطال الأفراد والمؤسسات على حد سواء. ومن هنا سوف نشرح الجرائم التي ترتكب ضد الأشخاص:

اولا-جريمة انتحال الشخصية:

تُعد هذه الجريمة واحدة من أقدم أنواع الجرائم التي تمثلت في الماضي بالأساليب التقليدية. ومع تطور التكنولوجيا وانتشار الإنترنت، اتخذت هذه الجريمة شكلاً جديداً يتمثل في انتحال هوية الأفراد عبر الشبكة الإلكترونية واستغلالها بشكل سيء للغاية. يحصل المجرم على البيانات الشخصية للضحية، مثل العنوان، تاريخ الميلاد، رقم الضمان الاجتماعي وغيرها، لاستخدامها في الحصول على بطاقات ائتمانية أو غيرها من العمليات الاحتيالية. باستخدام هذه المعلومات، يتمكن المجرم من إخفاء هويته الحقيقية والتحرك بحرية تحت اسم مستعار. غالبًا ما يجمع المجرم هذه المعلومات من خلال الإعلانات المنتشرة بكثافة على شبكة الإنترنت[1].

ثانيا-جريمة المضايقة والملاحقة:

هذا النوع من الجرائم يعتبر حديث العهد، وهو في تزايد مستمر مع كل تحديث أو تطوير يحدث على برامج الدردشة والمحادثات الفورية. تشير هذه الجريمة إلى الاستغلال السلبي للمساحات الإلكترونية التي توفرها الإنترنت، حيث تتيح هذه البرامج للمستخدمين التواصل فيما بينهم عبر محادثات مباشرة. ومع ذلك، يتم استغلال هذه المساحات لممارسة أنشطة مزعجة أو مطاردة الآخرين بشكل غير قانوني.

جرائم الملاحقة تشمل القيام بإرسال رسائل تهديد، تخويف، ومضايقة، وقد قارن القضاة هذه الجرائم التي تحدث عبر الإنترنت بجرائم التهديد العلني التقليدية. ومن الجدير بالذكر أن جرائم الملاحقة الإلكترونية لا تستلزم وجود أي اتصال مادي بين الجاني والضحية، ومع ذلك فإن لهذه الجرائم آثار نفسية سلبية على الضحايا، حيث إنها قد تؤدي إلى استشعار الخوف دون الحاجة إلى وقوع أعمال عنف فعلية[2].

---

[1] منير محمد الحنبيهى ممدوح محمد الحنبيهي سبق ذكره,ص43-42.

[2] محمد امين احمد الشوابكة , جرائم الحاسوب الأولى و الانترنت ,دار القافة للنشر و التوزيع ,ط1, عمان ,2004,ص45.

ثالثا–جرائم التغرير والاستدراج:

تعد من أبرز وأكثر جرائم الإنترنت شيوعاً، خاصة بين فئة صغار السن من مستخدمي الشبكة. تعتمد هذه الجرائم على خداع الضحية وإيهامها برغبة الجاني في بناء علاقة صداقة أو زواج عبر الإنترنت. وقد تتسع دائرة هذه الجرائم المعلوماتية لتصل إلى لقاءات فعلية بين الجاني والضحية. ومن أخطر ما يميز هذه الجرائم هو أنها لا تعرف حدوداً سياسية أو اجتماعية، حيث يمكن لأي شخص عبر الشبكة ارتكابها بسهولة، كما يمكن لأي مستخدم حسن النية الوقوع ضحية لها[1].

رابعا–جرائم التشهير وتشويه السمعة:

مع انتشار الشائعات والأخبار الكاذبة التي تمس رموز الشعوب سواء كانت فكرية أو سياسية أو حتى دينية، ظهرت مواقع إلكترونية متخصصة في نشر مثل هذه الأخبار الزائفة بهدف تشويه سمعة تلك الرموز، أو تسميم أفكار الناس، أو حتى ابتزاز بعض الأشخاص بنشر شائعات عنهم. وتتمثل أبرز وسائل ارتكاب هذه الجرائم في إنشاء مواقع إلكترونية تتضمن المعلومات المضللة التي يسعى الجاني إلى نشرها[2].

خامسا–الجرائم المخلة بالأخلاق والآداب العامة:

تتميز شبكة الإنترنت بكونها وسيلة عالمية لا تقتصر على مستخدم بعينه أو منطقة معينة. ومع ذلك، فإن المواد التي يتم عرضها عبر هذه الشبكة والتي قد تعتبر مخلة بالآداب والقيم الأخلاقية في بلد معين، قد تُشكّل جرائم تتنافى مع القوانين المحلية السائدة في ذلك البلد.

تُعتبر جريمة معاقب عليها قانونياً في بعض الدول، بينما قد لا تُعتبر كذلك في دول أخرى. وتتضمن هذه الجرائم تحريض القاصرين على المشاركة في أنشطة جنسية غير قانونية أو إفسادهم من خلال الوسائل الإلكترونية، بالإضافة إلى محاولات إغوائهم للقيام بمثل هذه الأنشطة. كما تشمل نشر معلومات عنهم عبر الحاسوب ودعوتهم إلى الانخراط في أعمال فاحشة أو تصويرهم أثناء ممارسة أنشطة ذات طابع جنسي.

ومن الجدير بالذكر أن المحتوى الإباحي يُعد من أكثر الأعمال انتشاراً ورواجاً في الوقت الحالي، خاصة في الدول العربية وأوروبا وآسيا. وتغطي الجرائم المتعلقة بانتهاك الأخلاق والآداب العامة على

[1] عبد الكريم شيباني ، مرجع سابق, ص19.

[2] منير محمد الحنبيهي ممدوح محمد الجنبيهي، سبق ذكره ,ص34

الإنترنت مختلف الأشكال، سواء كانت صوراً، مقاطع فيديو، حوارات، أو حتى أرقام هواتف. وقد ساهم هذا التنوع في جعل الشبكة متاحة للجميع دون أي عوائق أو قيود[1].

المبحث الثاني: استراتيجيات الأمن السيبراني لمكافحة الجريمة المعلوماتية.

في ظل التطور التقني المتسارع، أصبحت شبكة الإنترنت جزءاً لا غنى عنه من حياتنا اليومية، لكنها في الوقت ذاته فتحت المجال أمام الجرائم المعلوماتية التي تهدد الأفراد والمؤسسات. تتنوع هذه الجرائم بين الاختراقات الإلكترونية، النصب والاحتيال، الهجمات بالفيروسات، وسرقة البيانات الحساسة، مما يستدعي وضع استراتيجيات أمن سيبراني فعالة. يهدف الأمن السيبراني إلى حماية الأنظمة الرقمية والبيانات من أي تهديدات إلكترونية عبر استخدام تقنيات متطورة مثل التشفير، أنظمة الكشف عن التسلل، وإجراءات التحقق المتعدد. كما يعتمد على تعزيز الوعي المجتمعي بأهمية الحماية الرقمية وتطبيق القوانين الرادعة. إن مكافحة الجريمة المعلوماتية ليست مجرد مسؤولية تقنية، بل تتطلب تعاوناً مشتركاً بين الحكومات، الشركات، والمستخدمين لضمان بيئة إلكترونية آمنة ومستدامة

وفي ظل التطور التكنولوجي المتسارع، أصبح العالم يواجه تحديات متزايدة تتعلق بالجريمة المعلوماتية التي تهدد أمن الأفراد والمؤسسات والدول. تمثل هذه الجرائم خطراً متنامياً نتيجة تعقيد أساليبها وسرعتها في استغلال الثغرات التقنية. ولمواجهة هذه التهديدات السيبرانية، كان لزاماً على الدول اتخاذ إجراءات قانونية وتقنية فعالة ضمن إطارين رئيسيين الجهود الوطنية التي تشمل سن التشريعات المحلية وتعزيز البنية التحتية الأمنية، والجهود الدولية التي تتطلب التعاون بين الدول من خلال الاتفاقيات والمعاهدات المشتركة لمكافحة الجرائم العابرة للحدود، وللتفصيل في هذه المسألة سنتطرق الى الجهود الدولية في مواجهة التهديدات السيبرانية (مطلب الأول), ثم الى الجهود الوطنية في مواجهة التهديدات السيبرانية (مطلب الثاني).

[1] انظر محمد امين احمد الشوابكة سبق ذكره ص 136

المطلب الأول: الجهود الدولية في مواجهة التهديدات السيبرانية.

تُعد التهديدات السيبرانية من أبرز التحديات الأمنية التي تواجه العالم في العصر الرقمي، مما يستدعي تعاوناً دولياً فعالاً لمواجهتها. وتنصب الجهود الدولية في هذا المجال حول تعزيز التعاون القضائي والتقني بين الدول لمحاربة الجريمة الإلكترونية. ويمكن تقسيم هذه الجهود الى التعاون القضائي في مجال مكافحة الجريمة الالكترونية.

الفرع الاول: التعاون القضائي في مجال مكافحة الجريمة الإلكترونية.

إن إجراءات التحقيق والملاحقة القضائية في جرائم الإنترنت تتطلب تتبع النشاط الإجرامي، وهو ما يستدعي تقصي آثار الجريمة من مصدرها وحتى تنفيذها، مع تحديد مواقع الأضرار التي طالتها. وقد تقع هذه الأفعال في مختلف البلدان، مما يجعل ملاحقة مرتكبي هذه الجرائم أمراً يتطلب التعاون القضائي الدولي وتوسيع نطاق صلاحياته لتشمل جميع الدول. وبهذا يمكن تحقيق تعاون دولي فعال يسهم في القضاء على هذه الظاهرة الإجرامية. ويمكن في هذا السياق استعراض شكلين من أشكال التعاون القضائي وهما:

أولا: التعاون الأمني.

بما أن الجريمة الإلكترونية تعد عابرة للحدود، فمن المفترض ألا تكون الحدود الجغرافية عائقاً أمام الإجراءات الجنائية الرامية إلى التصدي لهذه الجرائم وملاحقة مجرمي المعلومات الذين ينتشر نشاطهم عبر مختلف أنحاء العالم. على سبيل المثال، قد يكون الجاني يحمل جنسية دولة معينة، لكنه يقوم بتنفيذ أفعاله باستخدام أجهزة وأدوات تقنية موجودة في دولة أخرى، في حين أن آثار وأضرار جريمته تطال دولة ثالثة. ومن هنا تأتي الحاجة الملحة والضرورية لإيجاد آليات تعاون قانوني وأمني دولي موحد لمواجهة هذه التحديات.

إن مواجهة مجرمي المعلومات تتطلب تضافر جهود جميع الدول من خلال قوانينها وتشريعاتها الجنائية، بهدف الكشف عن هوياتهم وشركائهم والمؤسسات التي تساعدهم على تنفيذ أنشطتهم الإجرامية. فجهود دولة واحدة باستخدام أنظمتها الأمنية لا تكفي للقضاء على الجريمة الإلكترونية، حيث إن نطاق الملاحقة يقتصر غالباً على الحدود الجغرافية لتلك الدولة. وفي حال فرار المجرم إلى دولة أخرى تتوقف ملاحقته مما يتيح له الاستمرار في أفعاله غير المشروعة والتسبب بأضرار مشابهة لما سببه في دولتهالأم[1].

[1] محمود احمد عبابنة و محمد معمر الرازقي, جرائم الحاسوب و ابعادها الدولية , عمان ,دار الثقافة للنشر و التوزيع,2009 ص132.

ولمكافحة هذه الظاهرة، هناك عدة أشكال للتعاون الأمني الدولي لمكافحة الجرائم الإلكترونية:

1-إنشاء مكاتب وهيئات متخصصة لجمع المعلومات حول مرتكبي الجرائم الإلكترونية ونشرها :

تهدف هذه المكاتب إلى تعزيز التعاون بين السلطات القضائية الدولية في مجال مكافحة الجرائم الإلكترونية. يتم ذلك من خلال جمع البيانات والمعلومات المتعلقة بالمجرمين وتعميمها بين الدول الأعضاء، إضافة إلى تبادل الخبرات وتقديم الدعم والعون لكل الأطراف عند الحاجة.

2-التعاون في إطار المنظمة العالمية للشرطة الجنائية (الإنتربول) :

تأسست هذه المنظمة لتعزيز التعاون الدولي الفعال والسليم بين أجهزة الشرطة في مختلف الدول. تسعى الإنتربول إلى مكافحة الجرائم الإلكترونية عبر جمع المعلومات والبيانات عن المجرمين، سواء كانوا أفراداً أو مؤسسات، بالتنسيق مع المكاتب المركزية الوطنية للشرطة الدولية المنتشرة في الدول الأعضاء. يتم تبادل هذه المعلومات بين الدول لتسهيل متابعة الجناة. وقد أسهمت الإنتربول بشكل كبير في حل العديد من القضايا المتعلقة بالجرائم الإلكترونية، مثل تبييض الأموال والتجارة غير المشروعة عبر الإنترنت، كما تمكنت من القبض على مجرمين مطلوبين وتسليمهم إلى الدول المعنية لمحاكمتهم وفرض العقوبات المناسبة عليهم.

3 -القيام بعمليات أمنية مشتركة لمتابعة مجرمي المعلومات :

يتم ذلك من خلال تتبع الأدلة والبيانات الرقمية وضبطها، بالإضافة إلى تنفيذ عمليات تفتيش عابرة للحدود تستهدف مكونات الأجهزة الإلكترونية مثل أجهزة الإعلام الآلي وشبكات الاتصال، بهدف البحث عن الأدلة والبراهين المتعلقة بالجرائم الإلكترونية. ومع ذلك، لا يمكن تحقيق هذا الأمر إلا عبر التعاون الدولي المشترك، من خلال تنظيم عمليات نوعية مكثفة ودورية في مناسبات خاصة. ويؤدي هذا النوع من التعاون إلى صقل المهارات وتبادل الأفكار والخبرات بين المشاركين، مما يعزز الجهود الدولية لمكافحة الجريمة الإلكترونية والتصدي لها[1].

أ-المساعدات الدولية القضائية لمكافحة الجريمة الإلكترونية:

يمكن استخلاص المبادئ العامة التي تحكم التزام الدول بتقديم المساعدة القضائية المتبادلة من الفقرة الأولى من المادة 25 من اتفاقية بودابست بشأن الإجرام الإلكتروني. وتشير هذه المبادئ إلى أن الالتزام

[1] محمد عبد الله قاسم، الحماية الجنائية للمعلومات الالكترونية , مصر , دار الكتب القانونية, 2010, ص128.

بتقديم المساعدة يجب أن يكون متاحاً لأقصى حد ممكن، على أن تكون شاملة وممتدة وخالية من الصعوبات والمعوقات.

وتتخذ المساعدة القضائية الدولية عدة أشكال، نذكر منها

1 –تبادل المعلومات حول الجرائم الإلكترونية:

ويشمل ذلك تبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها السلطات القضائية أثناء النظر في قضايا معينة. كما يتضمن تبادل السوابق القضائية الخاصة بالمتابعين وملفاتهم المتعلقة بالجرائم التي تم محاكمتهم عليها في دولهم الأصلية. لهذه الآلية تطبيقات عديدة، منها ما ورد في الفقرتين 6 و7 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في القضايا الجنائية، وكذلك في الفقرتين 3 و4 من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة.

ب–نقل الإجراءات الجنائية لجرائم المعلومات :

يتمثل هذا الإجراء في قيام دولة معينة، بناءً على اتفاقية مبرمة، باتخاذ مجموعة من الإجراءات الجنائية بشأن جريمة وقعت داخل حدود دولة أخرى ولصالح تلك الدولة. ويستلزم ذلك توفر شروط محددة، من أبرزها مبدأ التجريم المزدوج، الذي يعني أن يكون الفعل مجرماً في كل من الدولة الطالبة والدولة المطلوب منها نقل الإجراءات. كما يجب أن تكون الإجراءات المطلوبة مشروعة، أي متوافقة مع قوانين الدولة المطلوب منها تنفيذها، وأن تكون جدية وتتسم بأهمية تكفي للمساهمة في الوصول إلى الحقيقة وكشف ملابسات الجريمة. وقد تم إقرار هذا النوع من التعاون في العديد من المواثيق والمعاهدات الدولية، مثل معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (المادة 21)[1]، وكذلك المادة 23 من اتفاقية بودابست للإجرام الإلكتروني[2].

ج–الإنابة القضائية الدولية :

تُعرّف الإنابة القضائية بأنها الطلب المقدم من دولة إلى أخرى لاتخاذ إجراء قانوني ضمن إجراءات الدعوى الجنائية، وذلك عندما تعجز الدولة الطالبة عن تنفيذه بنفسها بسبب اختصاصات أو قيود إقليمية. يهدف هذا الإجراء إلى تسهيل التعاون بين الدول في مجال الإجراءات الجنائية، بما يضمن إجراء التحقيقات اللازمة وتقديم المتهمين للمحاكمة. عادة ما يتم تقديم طلبات الإنابة عبر قنوات دبلوماسية لتجنب تعقيدات

[1] المادة 21 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة.

[2] المادة 23 من اتفاقية بودابست للإجرام الإلكتروني.

الإجراءات وتأخيرها، وغالباً ما تُوجه هذه الطلبات إلى وزارة العدل في الدولة المستقبلة.

وعلى الرغم من أن التعاون القضائي الدولي يُعد أحد أهم الآليات والاستراتيجيات لمكافحة الجريمة الإلكترونية، إلا أنه يمكن ملاحظة أن غالبية الاتفاقيات والمعاهدات كانت سطحية في معالجتها لهذه الجرائم. ويرجع ذلك إلى الوضع الدولي العام.

يبدو أن التطور السريع في مجال الجريمة الإلكترونية يترك أثراً عميقاً وسلبياً على الأمن الدولي، مما ينبئ بمخاطر كبيرة تهدد المجموعة الدولية وأمنها السيبراني. في ظل هذا الواقع، أصبح من الضروري والمُلح عقد اجتماعات طارئة وبلورة اتفاقيات دولية قادرة على مواكبة هذا التطور الهائل في المجال الإلكتروني والمعلوماتي. ومن الضروري أن تتسم هذه الاتفاقيات بالصرامة والفعالية وأن تلتزم الدول بتطبيق بنودها بشكل صادق وحقيقي[1] لتحقيق الأهداف المرجوة.

ثانيا: تطبيق سياسة تسليم المجرمين كآلية دولية لمكافحة الجريمة الإلكترونية

تُعتبر عملية تسليم المجرمين إحدى الآليات الدولية الفاعلة لمكافحة الجريمة الإلكترونية على المستوى العالمي. وقد لجأت إليها غالبية الدول للحفاظ على أمنها السيبراني، وهي نتيجة حتمية للتطور السريع الذي تشهده تقنيات الاتصالات والمعلوماتية. ومع تنامي ذكاء المجرم الإلكتروني وسرعته في تنفيذ جرائمه عبر عدة دول وفي وقت قصير، أصبح بإمكانه التخطيط لجريمة إلكترونية في دولة ما وتنفيذها في دولة أخرى بهدف زعزعة استقرارها وإلحاق الضرر بها.

1-: أشكال تسليم المجرمين الإلكترونيين.

وفقًا للممارسات الدولية في مجال مكافحة الجريمة الإلكترونية، تم وضع ثلاثة أنظمة أساسية لتسليم المجرمين الإلكترونيين، وهي:

أ-التسليم القضائي:

يتميز هذا النوع بأن الجهة القضائية هي التي تتولى مسؤولية إصدار قرار تسليم المجرمين إلى الدول الطالبة، مع الحفاظ على حقوق الأفراد في الدفاع عن أنفسهم. ومن سلبيات هذا النظام بطء الإجراءات المتعلقة بالتسليم، وهو ما يؤثر سلبًا على سرعة ملاحقة المجرمين، خاصة وأن الأدلة الرقمية قد تندثر بسرعة.

[1] رامي متولي القاضي، الجريمة الالكترونية في القانون الجنائي الدولي: تحديات و ابعاد، ,مصر , دار النهجة العربية,2012,ص97.

ب-التسليم الإداري :

في هذا النظام، تكون السلطة التنفيذية هي الجهة المختصة باتخاذ قرار التسليم من عدمه، وتتمتع بالصلاحية الكاملة في هذا الشأن. يتميز هذا النوع بالسرعة وتجنب الإجراءات المعقدة التي قد تعيق إنهاء عملية التسليم. ومع ذلك، يواجه هذا النظام انتقادات بسبب تجاهل حقوق الدفاع للفرد، بالإضافة إلى خضوع قرارات التسليم لاعتبارات سياسية، فضلًا عن جهل الجهة المنفذة للتسليم بالخلفيات القانونية للقضية.

ج-التسليم المختلط:

يعتبر هذا النوع الأكثر شيوعًا، حيث يجمع بين مميزات النظامين السابقين. فهو يهدف إلى تسهيل الإجراءات وتسريعها مع ضمان حقوق الدفاع للمتهمين[1]، مما يجعله أكثر توازنًا وفعالية.

الفرع الثاني: دور الاونستيرال النموذجي في مكافحة جريمة المعلوماتية.

جاء هذا القانون نتيجة اقتناع الدول المتضررة من الجرائم الإلكترونية وإيمانها بأن تحقيق الحماية الدولية للأفراد والمؤسسات العالمية يتطلب تضافر الجهود والعمل بطريقة شاملة وديناميكية لمكافحة ظاهرة الإجرام الإلكتروني. وقد تم صياغة هذا القانون بالاستناد إلى قوانين تتعلق بالتجارة الإلكترونية وأخرى بشأن التوقيعات الإلكترونية، بهدف تعزيز الإطار القانوني الدولي للتعامل مع هذه الجرائم.

أولا: القانون المتعلق بالتجارة الإلكترونية:

تنطبق أحكام هذا القانون18-05 المتعلق بالتجارة الالكترونية [2], على ان جميع أنواع المعلومات التي تتخذ شكل رسائل بيانات تُستخدم في سياق الأنشطة التجارية، والتي يتم تسليمها وتخزينها باستخدام الوسائل الإلكترونية. كما يشمل القانون عمليات تبادل ونقل هذه البيانات إلكترونيًا بين الحواسيب من خلال معيار متفق عليه ومعتمد دوليًا.

ثانيا: القانون المتعلق بالتوقيعات الإلكترونية:

جاء هذا القانون 12-07 المتعلق بالتوقيعات الالكترونية [3]لاستبدال التوقيعات التقليدية بالتوقيعات الإلكترونية بهدف تجاوز قيود المسافات والأقاليم الدولية، حيث يتميز هذا النوع من التوقيعات بالسرعة

[1] محمد الشناوي, استراتيجية مكافحة النصب المستحدثة : الانترنت بطاقات الائتمان الدعاية التجارية الكاذبة, ,دار البيان للطبع و لنشر , القاهرة,2006,ص92.

[2]القانون18-05 المتعلق بالتجارة الالكترونية.

[3] القانون 12-07المتعلق بالتوقيعات الالكترونية، المؤرخ في 19 افريل 2012 من الجريدة الرسمية. العدد 24

والسرية. يُعرّف التوقيع الإلكتروني بأنه رمز أو شفرة سرية يتم الحصول عليها بعد اتباع مجموعة من الإجراءات الأمنية[1].

المطلب الثاني: الجهود الوطنية في مواجهة التهديدات السيبرانية.

في ظل التطور التكنولوجي المتسارع وتزايد الاعتماد على الأنظمة الرقمية في جميع مناحي الحياة، أصبحت الأمن السيبراني واحدة من أبرز التحديات التي تواجه الدول في القرن الحادي والعشرين. وتشكل التهديدات السيبرانية خطراً حقيقياً يهدد الأمن القومي، والاقتصاد الوطني، وسرية المعلومات الحساسة، واستمرارية الخدمات الحيوية مثل الطاقة، والصحة، والبنوك، والتواصل .

برزت الحاجة إلى بناء قدرات وطنية شاملة للتصدي لهذه التهديدات عبر مجموعة من الإجراءات الاستباقية والردود الفعلية التي تشمل: وضع التشريعات اللازمة، وإنشاء الهيئات المتخصصة، وبناء الكوادر المؤهلة، وتعزيز التعاون الدولي، ونشر الوعي المجتمعي ومن هنا سندرج بعض من القوانين والمراسيم المتعلقة بالجهود الوطنية في مواجهة التهديدات السيبرانية.

الفرع الأول: الهيئات المكلفة بالأمن السيبراني.

تُعتبر الهيئات المكلفة بالأمن السيبراني الركيزة الأساسية لحماية الفضاء الرقمي الوطني، من خلال وضع الآليات والإجراءات الوقائية والردية لمواجهة التهديدات الإلكترونية المتزايدة. وتتنوع مهام هذه الهيئات بين وضع الاستراتيجيات الوطنية، ومراقبة تنفيذها، واعتماد المعايير التقنية، والتدخل في حالات الطوارئ السيبرانية. وتعمل هذه المؤسسات بتنسيق عضوي مع مختلف القطاعات الحيوية لضمان أمن الأنظمة المعلوماتية وسلامة البيانات ودعم استمرارية الخدمات الأساسية للدولة ومن بين هذه الهيئات هي الوكالة الوطنية لتطوير الرقمنة (أولا) والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال (ثانيا) والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي(ثالثا)والمجلس الوطني لأمن الأنظمة المعلوماتية (رابعا).

أولا: الوكالة الوطنية لتطوير الرقمنة

عالج المشرع الجزائري احكام الوكالة الوطنية لتطوير الرقمنة بموجب القانون19-317 المتضمن انشاء الوكالة الوطنية لتطوير الرقمنة.

[1] سامي عياد حامد، الجريمة الإلكترونية، الإسكندرية، دار الفكر الجامعي,2007، ص51.

تُعد الوكالة الوطنية لتطوير الرقمنة الذراع التنفيذي المسؤول عن دعم ومواكبة عملية التحول الرقمي في مختلف قطاعات الدولة. وتهدف إلى تعزيز استخدام التقنيات الحديثة وتطوير البنية التحتية الرقمية لبناء اقتصاد رقمي مبتكر ومستدام. كما تلعب الوكالة دورًا محوريًا في إعداد السياسات والبرامج الخاصة بالرقمنة، وتقديم الدعم الفني واللوجستي للإدارات العمومية والهيئات المحلية لرفع كفاءة الخدمات الرقمية وجودتها[1].

ثانيا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

عالج المشرع الجزائري احكام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

رغم تركيزه على قطاع الاتصالات، إلا أنه يشترط على مزودي الخدمات ضمان الأمان والحماية من التهديدات السيبرانية.

-يُلزم الشركات باتخاذ الإجراءات اللازمة لحماية المستخدمين والمعلومات[2].

ثالثا: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

عالج المشرع الجزائري احكام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون 18 -07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

-هو أول تشريع شامل ينظم مجال الجرائم الإلكترونية في الجزائر.

-يحدد الجرائم المرتكبة ضد أنظمة المعالجة الآلية للمعطيات.

-يتضمن عقوبات على جرائم الاختراق، الاحتيال الإلكتروني، والتدخل غير المشروع في البيانات.

-ساهم في تأسيس إطار قانوني لمكافحة الجرائم السيبرانية[3].

رابعا: المجلس الوطني لأمن الأنظمة المعلوماتية.

عالج المشرع الجزائري احكام المجلس الوطني لأمن الأنظمة المعلوماتية، بموجب القانون 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

---

[1] المرسوم الرئاسي رقم 19-317 مؤرخ في 26 نوفمبر 2019 المتعلق انشاء الوكالة الوطنية لتطوير الرقمنة. الجريدة الرسمية في 1 ديسمبر 2019، العدد 74.

[2] لقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها , سبق ذكره.

[3] قانون رقم 18-07 مؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي, الصادر في الجريدة الرسمية في 10 جوان 2018 , العدد 34.

يُعد المجلس الوطني لأمن أنظمة المعلومات الجهة العليا المكلفة بوضع السياسات والاستراتيجيات الوطنية في مجال الأمن السيبراني، وتحديد التوجهات العامة لحماية الأنظمة والمعلومات الحساسة. وهو يترأس جهود التنسيق بين المؤسسات العمومية والخاصة لتعزيز القدرات الوطنية في مواجهة التهديدات الرقمية. ويهدف المجلس من خلال مقاربة استباقية وشاملة إلى ضمان أمن cyberspace ودعم الثقة في الخدمات الإلكترونية واستمرارية الأعمال الحيوية للدولة[1].

الفرع الثاني: القوانين الأساسية في مجال الامن السيبراني.

تُشكل القوانين الأساسية في مجال الأمن السيبراني الإطار التشريعي الضروري لضمان حماية الفضاء الرقمي الوطني وتنظيم استعماله بأسلوب آمن وموثوق. وتهدف هذه النصوص القانونية إلى تحديد الحقوق والواجبات المتعلقة بحماية البيانات والمعلومات الحساسة، ومعالجة المخالفات الإلكترونية، وضبط معايير الأمان المطلوبة للأنظمة المعلوماتية الحيوية. كما تمثل هذه القوانين حاضنة للتعاون بين الجهات العمومية والخاصة، وتساهم في تعزيز السيادة الرقمية ومواجهة التحديات المرتبطة على الجرائم السيبرانية والهجمات الإلكتروني ويتعلق الامر ب مرسوم تنفيذي رقم 16-135 يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكليها وتنظيمها وسيرها(أولا) ومرسوم تنفيذي رقم 16-134 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها(ثانيا)ومرسوم تنفيذي رقم 22-110يضبط مبادئ تحديد تعريفة خدمات للتصديق الالكتروني(ثالثا).

أولا: مرسوم تنفيذي رقم 16-135 يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكليها وتنظيمها وسيرها

تُعد السلطة الحكومية للتصديق الإلكتروني هيئة عمومية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، تُعنى بتنظيم وضمان أمن وموثوقية العمليات الرقمية، خاصةً في مجال التوقيع الإلكتروني والشهادات الرقمية. وتتألف هذه السلطة من هيكل تنظيمي يضم أجهزة إدارية وفنية متخصصة، تتوزع بينها المهام المتعلقة بإصدار الشهادات، والمراقبة، والاعتماد، والرقابة التقنية. ويتم تنظيم سير عملها وفق مبادئ

[1] المرسوم الرئاسي20-05 المتعلق بوضع منظومة وطنية الامن الأنظمة المعلوماتية، سبق ذكره.

الشفافية والكفاءة، وبما يتماشى مع المعايير الدولية لضمان الثقة في التعاملات الإلكترونية ودعم الاقتصاد الرقمي الوطني[1].

ثانيا: مرسوم تنفيذي رقم 16-134 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها

تُعد السلطة الوطنية للتصديق الإلكتروني الذراع التنظيمية والتنفيذية المكلفة بضمان أمن وموثوقية العمليات الرقمية، خاصةً في مجال التوقيع الإلكتروني والخدمات المرتبطة به. وتتمثل مهمتها الأساسية في وضع الأطر التقنية والإدارية اللازمة لتنظيم عمليات إصدار الشهادات الإلكترونية، والرقابة على مزوّد الخدمات المعتمدين. ويأتي تنظيم مصالح هذه السلطة وتحديد مهامها وسير عملها بهدف ضمان كفاءة الأداء، وحماية البيانات، وتعزيز الثقة في التعاملات الإلكترونية على المستوى الوطني والدولي[2].

ثالثا: مرسوم تنفيذي رقم 22-110يضبط مبادئ تحديد تعريفة خدمات للتصديق الالكتروني.

تُعد تحديد تعريفة الخدمات المتعلقة بالتصديق الإلكتروني أحد الجوانب الأساسية لتنظيم هذا المجال، ويهدف إلى ضمان شفافية الأسعار وعقلنتها بما يخدم المصلحة العامة ويحقق توازنًا بين جودة الخدمة والتكلفة. وتستند هذه التعريفة إلى معايير موضوعية تراعي طبيعة الخدمات المقدمة، وتكاليف الإنتاج، ومتطلبات الأمن السيبراني، بالإضافة إلى قدرة المستخدمين على تحملها. ويساهم تنظيم هذا الجانب في تعزيز الثقة في منظومة التصديق الإلكتروني، ودفع عجلة استخدام الوثائق الرقمية في مختلف المجالات الاقتصادية والإدارية[3].

الفرع الثالث: استراتيجية الجزائر في المجال القضائي.

تُعد الاستراتيجية الوطنية في المجال القضائي ركيزة أساسية لتعزيز سيادة القانون، وتكافؤ الفرص، والعدل الاجتماعي، من خلال بناء نظام قضائي عادل، مستقل، وفعال يضمن حقوق الأفراد وحرياتهم

---

[1] مرسوم تنفيذي رقم 16-135 يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكليها وتنظيمها وسيرها, المؤرخ 25 افريل 2016 الجريدة الرسمية , العدد26.

[2] مرسوم تنفيذي رقم 16-134 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني و سيرها و مهامها المؤرخ 25 افريل 2016,الجريدة الرسمية , العدد26.

[3] مرسوم تنفيذي رقم 22-110يضبط مبادئ تحديد تعريفة خدمات للتصديق الالكتروني، المؤرخ 14 مارس 2022 الجريدة الرسمية ,العدد19.

العامة. وتسعى هذه الاستراتيجية إلى تحديث منظومة العدالة، وتحسين آليات التقاضي، واعتماد الوسائل الرقمية لتسريع الإجراءات ورفع كفاءة المرفق القضائي. كما تهدف إلى تعزيز الثقة في القضاء، وتجسيد مبادئ الشفافية والمساءلة، وتطوير الكوادر البشرية وتأهيلها بما يتلاءم مع التحديات المعاصرة ومتطلبات الدولة الحديثة. ويتعلق الامر في الاختصاص القضائي (أولا)، و**المساعدة** القضائية الدولية المتبادلة(ثانيا)

أولا: الاختصاص القضائي.

تتطرق المشرع الجزائري في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وخص احكام المادة 15 من هذا القانون بجانب القواعد المتعلقة بالاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تكون المحاكم الجزائرية مختصة بالنظر في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال التي تُرتكب خارج الحدود الوطنية، إذا كان مرتكبها أجنبيًا وكانت الجريمة تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[1].

ثانيا: المساعدة القضائية الدولية المتبادلة.

اطر المشرع الجزائري في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، نصت المادة 16 من على ان: في إطار التحريات أو التحقيقات القضائية الجارية للكشف عن الجرائم المنصوص عليها في هذا القانون وتحديد مرتكبيها، يُمكن للسلطات المختصة اللجوء إلى تبادل المساعدة القضائية الدولية لجمع الأدلة المتعلقة بالجريمة بصيغتها الإلكترونية.

كما يُمكن قبول الطلبات المتعلقة بهذه المساعدة القضائية، في حالة الاستعجال، عبر وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني، شريطة احترام الاتفاقيات الدولية ومبدأ المعاملة بالمثل، وبشرط أن توفر هذه الوسائل ضمانات كافية تؤكد صحتها وموثوقيتها.[2]

[1] المادة 15 من المرسوم الرئاسي 09-04، سبق ذكره.

[2] المادة 16 من المرسوم الرئاسي 09-04، سبق ذكره.

خلاصة الفصل الثاني.

يُعَدُّ الأمن السيبراني أحد الأسس الرئيسية في مواجهة التحديات المتنامية للجريمة المعلوماتية في ظل التطور التكنولوجي المتسارع الذي أتاح فرصًا كبيرة للمجرمين الإلكترونيين للاستفادة من الثغرات الأمنية. ولقد أصبح من الضروري اعتماد استراتيجيات متينة وأطر قانونية وتقنية تضمن حماية الأنظمة المعلوماتية وتأمين الفضاء الرقمي على المستوى الفردي والمؤسسي وحتى الوطني .

وقد أظهرت الدراسات أن للأمن السيبراني دورًا محوريًا في الكشف عن الجرائم الإلكترونية، ومنع حدوثها عبر نظم المراقبة الذكية والتوعية الأمنية. كما لا يقتصر دوره على الجانب الوقائي فقط، بل يمتد إلى تعزيز التعاون الدولي، وتطوير بنية تحتية رقمية آمنة تدعمها تشريعات صارمة ومؤسسات متخصصة .

وبالإضافة إلى ذلك، فإن دمج تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي في نظم الأمن السيبراني يساهم بشكل كبير في تحسين استباقية التصدي للهجمات الإلكترونية قبل وقوعها. ومع ذلك، تبقى هناك تحديات كبيرة تواجه هذا المجال، منها ضعف البنية التحتية في بعض الدول، وقلة الخبرات المتخصصة، بالإضافة إلى عدم كفاية التشريعات المحلية لمجاراة طبيعة الجرائم الحديثة .

لذلك، يتطلب الأمر تضافر الجهود بين المؤسسات الحكومية، وشركات التقنية، والمجتمع المدني لنشر ثقافة الأمان الرقمي، وبناء خط دفاعي قوي ضد الجريمة المعلوماتية، بما يحقق الحماية الشاملة لحقوق الأفراد ومصالح الدول في الفضاء السيبراني.

الخاتمـــــة

لا يزال الأمن السيبراني في الجزائر في طور التطور، ورغم الجهود المبذولة لتعزيز الحماية ضد الجريمة المعلوماتية، إلا أن التحديات التقنية والتشريعية تحد من فعاليته مقارنة بالممارسات العالمية. تم اتخاذ خطوات مهمة مثل إنشاء هيئة الأمن السيبراني واعتماد قوانين جديدة، لكن البنية التحتية تحتاج إلى تحديث مستمر وقدرة استجابة أسرع للهجمات الإلكترونية. كما أن الوعي المجتمعي والمؤسسي بمخاطر الأمن الرقمي لا يزال محدودًا. لذلك، يمكن القول إن مستوى الحماية لم يرتقِ بعد إلى المعايير العالمية المطلوبة. ومع ذلك، فإن الإرادة السياسية والتطور التكنولوجي المستمر يفتحان آفاقاً واعدة لتحسين الوضع مستقبلاً.

يُعد الأمن السيبراني أحد أهم الركائز الأساسية في بناء مجتمع رقمي آمن ومزدهر، خاصة في ظل التطور التكنولوجي المتسارع والاعتماد المتزايد على الأنظمة الرقمية في جميع مجالات الحياة. ومع انتشار أنواع متعددة من الجرائم المعلوماتية مثل الاختراقات الإلكترونية، والاحتيال عبر الإنترنت، وسرقة البيانات الحساسة، أصبح من الضروري تعزيز البنية التحتية الأمنية الرقمية وتطوير استراتيجيات فعالة للتصدي لهذه التهديدات.

وقد أظهرت الدراسة أن للأمن السيبراني دورًا محوريًا في حماية الأفراد والمؤسسات والدول من مخاطر الجريمة المعلوماتية، من خلال تطبيق تقنيات وأساليب متطورة مثل التشفير، ونظام الكشف عن الاختراقات، وتحليل التهديدات في الوقت الفعلي، بالإضافة إلى نشر الوعي الأمني بين المستخدمين.

ولذلك، فإن الاستثمار في الأمن السيبراني ليس خيارًا بل ضرورة استراتيجية لضمان استمرارية العمل وحماية الخصوصية والأمن الوطني في العصر الرقمي.

وعليه تم تطرق الى عديد من نتائج أهمها:

1-هناك علاقة وثيقة بين تقوية إجراءات الأمن السيبراني وتقليل معدلات الجريمة المعلوماتية.

2-معظم الجرائم الإلكترونية تحدث نتيجة ضعف الوعي الأمني لدى المستخدمين وعدم وجود خطط شاملة للحماية.

3- المؤسسات التي تستثمر في بنية تحتية أمنية قوية تقل لديها فرص التعرض لهجمات إلكترونية ناجحة.

4-الحاجة ملحة إلى تشريعات قانونية رادعة لجرائم الإنترنت وتعزيز التعاون الدولي في مجال مكافحة الجريمة السيبرانية.

5-التدريب والتوعية هما من أهم الوسائل لرفع مستوى الأمان الرقمي على المستوى الفردي والمؤسسي.

بناءا عن نتائج أعلاه نقترح جملة من التوصيات نجزها في ما يلي:

1- تعزيز البنية التحتية للأمن السيبراني على مستوى الدولة من خلال إنشاء مراكز متخصصة لمراقبة التهديدات والاستجابة لها.

2- وضع تشريعات قانونية واضحة لتجريم الأفعال المرتبطة بالجريمة المعلوماتية ومعاقبة مرتكبيها.

3-نشر الثقافة الأمنية الرقمية بين المواطنين والمقيمين من خلال الحملات التوعوية والتدريب في المدارس والجامعات والقطاعات الحكومية والخاصة.

4-تشجيع البحث العلمي في مجال الأمن السيبراني ودعم المشاريع التقنية التي تهدف إلى تطوير حلول أمنية محلية.

5-تفعيل التعاون الدولي مع المنظمات والدول المتقدمة في هذا المجال لتبادل الخبرات والمعلومات حول أحدث أنواع الهجمات والتقنيات الدفاعية.

6- تطبيق سياسات الأمان داخل المؤسسات مثل استخدام كلمات مرور قوية، والتحقق الثنائي، وتحديث البرامج باستمرار، وتدريب الموظفين على التعامل مع المخاطر الإلكترونية.

قائمة المصادروالمراجع

قائمة المصادر والمراجع

- **القوانين:**

1- القانون 04-15 المؤرخ في 10 نوفمبر 2004 الصادر في الج. ر. رقم 71، المتضمن تعديل قانون العقوبات لسنة 2004.

2- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد ،47، الصادرة في سنة 2009 المعدل والمتمم.

3- القانون 12-07آلمتعلق بالتوقيعات الالكترونية، المؤرخ في 19 أفريل 2012 والصادر في العدد 24 من الجريدة الرسمية بتاريخ 25 أفريل 2012.

4-القانون رقم 18-04، المؤرخ 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية العدد 27.

5- القانون رقم 18-05 المتعلق بالتجارة الالكترونية. المؤرخ في 10ماي 2018، الصادر في جريدة الرسمية في 16 ماي 2018، العدد 28.

6- القانون رقم 18-07 مؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر في الجريدة الرسمية في 10 جوان 2018 , العدد 34.

المراسيم:

1- مرسوم تنفيذي رقم 16-135 يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكليها وتنظيمها وسيرها، المؤرخ 25 أفريل 2016 الصادر في الجريدة الرسمية في 28 أفريل 2016، العدد26.

2- مرسوم تنفيذي رقم 16-134 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها المؤرخ 25 أفريل 2016 الصادر في الجريدة الرسمية في 28 أفريل 2016، العدد26.

3- المرسوم الرئاسي رقم 19-317 مؤرخ في 26 نوفمبر 2019 المتعلق انشاء الوكالة الوطنية لتطوير الرقمنة الصادر في الجريدة الرسمية في 1 ديسمبر 2019, العدد 74.

4- المرسوم الرئاسي20-05 المؤرخ في 20 جانفي سنة 2020 المتعلق بوضع منظومة وطنية الامن الأنظمة المعلوماتية، الصادر في الجريدة الرسمية 26جانفي 2020 العدد 04.

5- مرسوم تنفيذي رقم 22-110يضبط مبادئ تحديد تعريفة خدمات للتصديق الالكتروني، المؤرخ 14 مارس 2022 الصادر في الجريدة الرسمية في 19 مارس 2022، العدد19.

الكتب:

1- أبو النصر مدحت محمد، الذكاء الإصطناعي, المجموعة العربية للتدريب والنشر، القاهرة، مصر،2022.

2- أمير فرج يوسف الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والانترنت، الطبعة الأولى، مكتبة الوفاء القانونية، مصر، 2011.

3- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

4- الحسين حسن محمد، اسياسيات الامن السيبراني، دار النهضة العربية، القاهرة، مصر , 2022

5- احمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية,2005.

6- بيتر بيل سيل، ترجمة ضياء وراد هنداوي سي أي سي، الكون الرقمي: الثورة العالمية في الاتصالات، 2017.

7- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2011.

8- رامي متولي القاضي، الجريمة الالكترونية في القانون الجنائي الدولي: تحديات وابعاد، ط2,مصر، دار النهجة العربية,2012.

9-سعيد بن عيسى، الامن السيبراني في الجزائر التحديات والتشريعات، جامعة الجزائر 1 (بن يوسف بن خدة) كلية الحقوق والعلوم السياسية، دار الحكمة للنشر والتوزيع.

10- سامي عل عياد حامد، الجريمة الالكترونية، ط1 الإسكندرية، دار الفكر الجامعي,2007,.

11- علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، العربي للنشر والتوزيع، 2022.

12- علاء عبد الرزاق محمد السالمي، المدخل الى الامن السيبراني، الذاكرة للنشر والتوزيع، بغداد، العراق, 2022,.

13- عبد الجبار حسين الظفري، انترنيت الأشياء دار النجاء، صنعاء، اليمن,2022.

14- علي حسن الطوابلة، الجرائم الالكترونية، مؤسسة الفخراوي للدراسات والنشر، البحرين، 2008.

15- فاطمة علي السعيد، التحديات السيبرانية في المؤسسات الحديثة، جامعة القاهرة، كلية الحاسبات والمعلومات، المركز القومي للبحوث العلمية، دار النهضة العربية، مصر، 2019.

16- محمد كمال، الإرهاب السيبراني، دار كليم للطباعة والنشر والتوزيع، القاهرة، مصر،2022،

17- منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، دار النهضة العربية، القاهرة ،2016.

18- محمد محمود العمري، مدخل إلى الأمن السيبراني، دار زهران للنشر والتوزيع، 2020.

19- محمد إبراهيم غازي الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، 2014.

20- محمد علي العربان الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.

21- منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

22- محمد امين احمد الشوابكة جرائم الحاسوب الأولى والانترنت، دار القافة للنشر والتوزيع، ط1، عمان ،2004.

23- محمود احمد عبابنة ومحمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، عمان، دار الثقافة للنشر والتوزيع,2009.

24- محمد عبد الله قاسم، الحماية الجنائية للمعلومات الإلكترونية، ط1، مصر، دار الكتب القانونية، 2010.

25- محمد الشناوي، استراتيجية مكافحة النصب المستحدثة: الانترنت بطاقات الائتمان الدعاية التجارية الكاذبة، ط1، دار القاهرة، دار البيان للطبع والنشر،2006.

26- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الإسكندرية، 2005.

27- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الأردن، 2010.

28- نهلة عبد القادر المؤمني، الجرائم المعلوماتية، عمان، دار الثقافة، جامعة البلقاء التطبيقية، 2008.

- **الرسائل والمذكرات الجامعية:**

1- بدري فيصل مكافحة الجريمة المعلوماتية في القانون الدو لي والداخلي، أطروحة لنيل شهادة دكتوراه علوم . تخصص قانون عام كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة ،2018،

2-عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر كلية الحقوق والعلوم السياسية، جامعة الطاهر، مولاي، سعيدة، سنة 2015/2016.

- **مقالات:**

1- احمد بن عيسى، دور الامن السيبراني في تعزيز الامن الوطني الجزائري، مجلة العلوم الإنسانية والاجتماعية، جامعة باتنة ,2019. العدد44.,

2- الاتحاد الدولي للاتصالات شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن لمحة عامة عن الأمن السيبراني التوصية رقم .ITU-T X1205 سنة 2008.

3- إسلام مصطفى جمعة مصطفى، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية (مجلة علمية محكمة)، جامعة القاهرة، المجلد 12، العدد 3 ،2022.

4- أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، 2016.

5- بثينة حبيباتي، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة الجزائر، المجلد 30, العدد 1, جوان2019, الجزائر.

6- ساعد بوقرص، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، الجزائر، المجلد 03، العدد 1 ،2022.

7- سليمان بوزيد الامن السيبراني كأداة لتعزيز الاستقرار السياسي والاقتصادي في الجزائر مجلة القانون والمجتمع جامعة قسنطينة 2020.

8- صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية مجلة قضايا سياسية، العدد 62, 2020.

9- نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد ألمن الدول"، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، المجلد 8 ،العدد 2 ،2018 .

10- فاطمة الزهراء بلقاسم، حماية البنية التحتية الحيوية في ظل التحديات السيبرانية، دراسة قانونية، جامعة قسنطينة 2 كلية الحقوق والعلوم السياسية، ,2021.

11- لبنى خميس مهدي، **أثر السيبرانية في تطور القوة**، مجلة حمورابي، جامعة النهرين، العدد 33-34, 2020.

12- منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني الأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، مصر، العدد 11، سنة 2020.

13- محمد الأمين بوغرارة، الهجمات السيبرانية وأثرها على الامن القومي، دراسة حالة الجزائر، جامعة الجزائر 3 مجلة الدراسات الاستراتيجية والأمنية , 2021.

14- ناصر بن عبد الله القحطاني، الهجمات السيبرانية وأثرها على الامن القومي، مجلة الدراسات الأمنية والاستراتيجية، جامعة القاهرة المجلد35,العدد2 , 2020,

15- عادل يوسف عبد النبي البشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة مركز دراسات الكوفة العدد السابع.

- **مؤتمرات**

1- نادية بلقاسم، السياسات السيبرانية في الجزائر: نحو الاستقرار وطني مستدام، المؤتمر الوطني حول الامن السيبراني المركز الوطني للدراسات الاستراتيجية 2022.

-مواقع إلكترونية:

1- فارس قوة، الأمن السيبرانيSecurity Cyber - ، الموسوعة السياسية، رابط الموقع: https://political-encyclopedia.org/dictionary/السيبراني%20 تاريخ: 21-04-2024 ساعة 22.00

فهرس المحتويات

العنـــــوان	الصفحة
إهداء	
شكر وتقدير	
مقدمة	2-6
الفصل الأول: ماهية الامن السيبراني.	8
المبحث الأول: مفهوم الأمن السيبراني ومجالاته.	9
المطلب الأول: تعريف الأمن السيبراني وأبعاده.	9
الفرع الأول: تعريف الأمن السيبراني.	9
أولا: التعريف المباشر للأمن السيبراني	10
ثانيا: تعريف الامن السيبراني من خلال المفاهيم المرتبطة به.	12
الفرع الثاني الأبعاد المختلفة للأمن السيبراني.	14
أولا-الابعاد العسكرية للأمن السيبراني.	14
ثانيا-الابعاد الاقتصادية للأمن السيبراني.	15
ثالثا-الابعاد السياسية للأمن السيبراني.	15
رابعا- الأبعاد القانونية للأمن السيبراني.	15
خامسا- الابعاد الاجتماعية للأمن السيبراني	16
المطلب الثاني: تطبيقات الامن السيبراني	16
الفرع الأول: الأمن السيبراني في المؤسسات الحكومية والخاصة.	17
أولا: الامن في السيبراني المؤسسات الحكومية	17
ثانيا: الامن السيبراني في المؤسسات الخاصة	18
الفرع الثاني: تطبيق امن السيبراني في مواجهة التهديدات السيبرانية.	18
أولا: تطبيق امن السيبراني في التهديدات السيبرانية التقليدية	18
ثانيا: تطبيق امن السيبراني في التهديدات السيبرانية الحديثة	20
المبحث الثاني: أهمية الأمن السيبراني في العصر الرقمي.	21
المطلب الأول: دور الأمن السيبراني في حماية البنية التحتية الحيوية .	21
الفرع الأول: مفهوم البنية التحتية الحيوية.	22
الفرع الثاني: علاقة الامن السيبراني بالبنية التحتية الحيوية.	23

المطلب الثاني: أهمية الأمن السيبراني في الحفاظ على الأمن العام.	**25**
الفرع الأول: تأثير الهجمات السيبرانية على الأمن العام.	**25**
الفرع الثاني: دور الأمن السيبراني في تعزيز الاستقرار الوطني.	**26**
خلاصة الفصل	**28**
الفصل الثاني: دور الأمن السيبراني في مكافحة الجريمة المعلوماتية	**30**
المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية موضوع الأمن السيبراني	**31**
المطلب الأول: مضمون الجريمة المعلوماتية.	**31**
الفرع الأول: تعريف الجريمة المعلوماتية.	**31**
أولا: الاتجاه الضيق لمفهوم الجريمة المعلوماتية.	**32**
ثانيا: الاتجاه الموسع لتعريف الجريمة المعلوماتية.	**33**
ثالثا: موقف المشرع الجزائري من تعريف الجريمة المعلوماتية.	**35**
الفرع الثاني: الأسباب الرئيسية لانتشار الجريمة المعلوماتية.	**36**
أولا: دوافع او الأسباب الذاتية.	**36**
المطلب الثاني: أبرز أشكال الجرائم المعلوماتية	**40**
الفرع الأول: الجرائم المالية الإلكترونية (الاحتيال الإلكتروني، غسل الأموال).	**41**
أولا: مبدأ عمل الفيروسات يختلف بناءً على أسلوب تصميمها	**41**
ثانيا: جرائم الاختراقات.	**41**
ثالثا: جريمة تعطيل الأجهزة والشبكات	**42**
رابعا: جريمة النصب والاحتيال	**42**
الفرع الثاني: الجرائم المرتبطة بالبيانات الشخصية (سرقة الهوية، انتهاك الخصوصية).	**43**
اولا–جريمة انتحال الشخصية:	**43**
ثانيا–جريمة المضايقة والملاحقة	**43**
ثالثا–جرائم التغرير والاستدراج:	**44**
رابعا–جرائم التشهير وتشويه السمعة	**44**
خامسا–الجرائم المخلة بالأخلاق والآداب العامة:	**44**
المبحث الثاني: استراتيجيات الأمن السيبراني لمكافحة الجريمة المعلوماتية	**45**
المطلب الأول: الجهود الدولية في مواجهة التهديدات السيبرانية.	**45**

الفرع الاول: التعاون القضائي في مجال مكافحة الجريمة الإلكترونية	**46**
أولا: التعاون الأمني.	**46**
ثانيا: تطبيق سياسة تسليم المجرمين كآلية دولية لمكافحة الجريمة الإلكترونية	**49**
الفرع الثاني: دور الأونستيرال النموذجي في مكافحة جريمة المعلوماتية.	**50**
أولا: –القانون المتعلق بالتجارة الإلكترونية	**50**
ثانيا: –القانون المتعلق بالتوقيعات الإلكترونية	**50**
المطلب الثاني: الجهود الوطنية في مواجهة التهديدات السيبرانية	**51**
الفرع الأول: الهيئات المكلفة بالأمن السيبراني.	**51**
أولا: الوكالة الوطنية لتطوير الرقمنة	**51**
ثانيا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال	**52**
ثالثا: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي	**52**
رابعا: المجلس الوطني لأمن الأنظمة المعلوماتية.	**52**
الفرع الثاني: القوانين الأساسية في مجال الامن السيبراني.	**53**
أولا: مرسوم تنفيذي رقم 16–135 يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكليها وتنظيمها وسيرها	**53**
ثانيا: مرسوم تنفيذي رقم 16–134 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها	**54**
ثالثا: مرسوم تنفيذي رقم 22–110يضبط مبادئ تحديد تعريفة خدمات للتصديق الالكتروني.	**54**
الفرع الثالث: استراتيجية الجزائر في المجال القضائي.	**54**
أولا: الاختصاص القضائي.	**55**
ثانيا: المساعدة القضائية الدولية المتبادلة.	**55**
خلاصة الفصل	**56**
الخاتمة العامة	**59–58**
قائمة المصادر والمراجع	**65–61**

الملخص:

يُعد الأمن السيبراني عنصرًا أساسيًا في بناء مجتمع رقمي آمن في ظل التقدم التكنولوجي والاعتماد على الأنظمة الرقمية. وتزايد الجرائم المعلوماتية مثل الاختراق وسرقة البيانات يستدعي تعزيز البنية التحتية الرقمية وتطوير استراتيجيات الحماية. وقد أظهرت الدراسات أن الأمن السيبراني يحمي الأفراد والمؤسسات من خلال تقنيات مثل التشفير وكشف الاختراقات والتحليل الفوري للتهديدات، إلى جانب التوعية الأمنية. لذا، فإن الاستثمار في الأمن السيبراني هو ضرورة لضمان الخصوصية والأمن الوطني واستمرارية العمل في العصر الرقمي.

الكلمات المفتاحية:

- **الأمن السيبراني– الجريمة المعلوماتية –التهديدات الرقمية –البنية التحتية الأمنية**

Summary:

Cybersecurity is a fundamental component in building a secure digital society, especially with the rapid advancement of technology and increasing reliance on digital systems. The rise in cybercrimes such as hacking and data theft highlights the need to strengthen digital infrastructure and develop effective protection strategies. Studies show that cybersecurity safeguards individuals and organizations through encryption, intrusion detection, real-time threat analysis, and awareness programs. Therefore, investing in cybersecurity is essential to ensure privacy, national security, and business continuity in the digital age.

Keywords

- **Cybersecurity - Cybercrime - Digital threats - Security infrastructure**