وزارة التعليـم العالــي والبحـث العلمي

المركز الجامعي عبد الحفيظ بوالصوف –ميلة

معهد الحقوق

الشعبة : الحقوق

القسم: قانون عام

التخصص: قانون جنائي

الرقم التسلسلي:.....

الرمـــــــــز: .....

تأثير الجريمة الإلكترونية على الأمن السيبراني في الجزائر

مذكرة ضمن متطلبات نيل شهادة الماستر

من إعداد الطالبتين:

- **مساط شيماء**
- **بوطيبة عائشة**

إشراف الأستاذة:

د. مزياني صبرينة

السنة الجامعية: 2025/2024

وزارة التعليـم العالــي والبحـث العلمي
المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهد الحقوق

الشعبة: الحقوق
القسم: قانون عام
التخصص: قانون جنائي

الرقم التسلسلي:.....
الرمـــــــــز: .....

تأثير الجريمة الإلكترونية على الأمن السيبراني في الجزائر

مذكرة ضمن متطلبات نيل شهادة الماستر

من إعداد الطالبتين:
- **مساط شيماء**
- **بوطيبة عائشة**

إشراف الأستاذة:
د. مزياني صبرينة

أعضاء لجنة المناقشة:

د.مفيدة مقورة	**(المركز الجامعي ميلة)**	**(أستاذ محاضر ب)**	**رئيسا**
د.صبرينة مزياني	**(المركز الجامعي ميلة)**	**(أستاذ محاضر ب)**	**مشرفا ومقررا**
د.شوقي حفياني	**(المركز الجامعي ميلة)**	**(أستاذ محاضر ب)**	**عضوا ممتحنا**

السنة الجامعية: 2025/2024

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

الملخص:

أولا: اللغة العربية:

تناولت هذه الدراسة موضوع " **تأثير الجريمة الإلكترونية على الأمن السيبراني في الجزائر**" باعتبارها من أبرز التهديدات المستحدثة في العصر الرقمي، لما تنطوي عليه من مخاطر متزايدة تؤثر على الأفراد والمؤسسات والدول. وتهدف الدراسة إلى تحليل مفهوم الجريمة الإلكترونية، والكشف عن أسباب انتشارها وخصائصها وأنواعها، مع تسليط الضوء على واقعها في الجزائر والتحديات المرتبطة بمواجهتها، من ضعف البنية التحتية التقنية، والقصور التشريعي، ونقص الكفاءات والوعي السيبراني. واعتمدت الدراسة المنهج الوصفي التحليلي لفهم أبعاد الظاهرة وتقييم انعكاساتها على الأمن السيبراني الوطني، كما استخدمت الوثائق والتقارير الرسمية والإحصائيات الصادرة عن الهيئات الوطنية والدولية كأدوات رئيسية لجمع البيانات. وأظهرت نتائج الدراسة أن الجريمة الإلكترونية في الجزائر تشهد تطورًا مستمرًا من حيث الكم والنوع، مما يستدعي تعزيز البنية السيبرانية، وتحديث التشريعات، وتكثيف التعاون الدولي لضمان أمن الفضاء السيبراني وحمايته من التهديدات المتصاعدة.

الكلمات المفتاحية: الجريمة، الجريمة الإلكترونية، الأمن، الأمن السيبراني، الفضاء السيبراني.

ثانيا: اللغة الإنجليزية.

This study addresses the topic of **"The Impact of Cybercrime on Cybersecurity in Algeria,"** considering it one of the most prominent emerging threats in the digital era due to the increasing risks it poses to individuals, institutions, and states. The study aims to analyze the concept of cybercrime, identify its causes, characteristics, and types, while shedding light on its current situation in Algeria and the challenges faced in combating it, including weak technological infrastructure, legislative shortcomings, and lack of expertise and cyber awareness. The study employed a descriptive analytical approach to understand the dimensions of the phenomenon and assess its implications for national cybersecurity .In addition official documents, reports, and statistics issued by national and international bodies were used as primary tools for data collection. The results indicate that cybercrime in Algeria is continuously evolving in both quantity and complexity, necessitating the enhancement of cyber infrastructure, updating legislation, and intensifying international cooperation to ensure the security and protection of cyberspace from escalating threats.

Keywords: Crime, Cybercrime, Security, Cybersecurity, Cyberspace.

الشكر والتقدير

بسم الله الرحمن الرحيم

الحمد لله الذي علّم الإنسان ما لم يعلم، والحمد له على ما أنعم به من توفيق وسداد، فلولا فضله ما بلغنا هذه المرحلة، ولا تحقق لنا هذا الإنجاز العلمي.

في هذه المناسبة، يطيب لنا أن نرفع أسمى آيات الشكر والعرفان لأستاذتنا الفاضلة **مزياني صبرينة**، على إشرافها الكريم ومرافقتها النيرة لنا خلال مختلف مراحل إعداد هذه المذكرة. لقد كانت مثالًا في الجدية والحرص والعطاء، فجزاها الله عنا خير الجزاء، وبارك في علمها وعملها، وجعل ما تبذله من جهد في ميزان حسناتها.

كما نخصّ بالشكر والتقدير السادة أعضاء لجنة المناقشة الأفاضل، على قبولهم مناقشة هذا العمل، وتفضّلهم بتقديم ملاحظاتهم القيّمة التي نعتز بها، لما تحمله من فائدة علمية سيكون لها بالغ الأثر في تقويم هذا الجهد وتطويره.

ولا يسعنا كذلك إلا أن نتوجّه بخالص الامتنان لجميع أساتذتنا الكرام، الذين ساهموا في بنائنا العلمي والمعرفي، وأسهموا في تشكيل شخصيتنا الأكاديمية، فلكم منا كل الشكر والتقدير على ما قدّمتم من علم وإرشاد، وما تركتم من أثر لا يُمحى.

كما نعبر عن امتناننا لكل من كان عونًا وسندًا لنا، بكلمة مشجعة، أو دعوة صادقة، أو موقف محفّز... لكم منّا أصدق المشاعر وأخلص الدعاء، ونحمل لكم في قلوبنا تقديرًا لا يزول.

الإهداء

بسم الله الرحمن الرحيم لحمد لله أولًا وآخرًا، ظاهرًا وباطنًا، الحمد لله الذي علّمني الصبر، وغرس في قلبي العزيمة الحمد لله الذي يسر البدايات وبلغني النهايات، وبارك لي فيما تعلمت، وزدني علمًا وفهمًا ونورًا.

هذا النجاح العظيم أهديه بكل فخر واعتزاز

إلى أبي حبيب قلبي خالد مساط أنت عمود حياتي، وقوتي التي لا تنكسر، بك أفتخر، ومنك تعلمت أن أكون لا تُقهَر، كنت الحصن المنيع والدعم اللامتناهي، هذا النجاح هو انتصارك معي، حفظك الله، وأبقاك لي رمزًا للقوة والعزة. وأمي روح قلبي حبيبة بولطيف أنتِ الملكة التي تحكم قلبي، وقلعة الحنان التي لا تهدم، بحبك دعمتيني وبصبرك ربتيني على الكبرياء والثبات، أنتِ النور الذي لا يخبو والصدر الحنون الذي لا ينكسر هذا النجاح لكِ وكل شيء أملكه في حياتي أنتم سر قوتي وأساس ثباتي، وبفضل دعائكم وحبكم سأظل دومًا قوية لا تُقهَر أنا اليوم أقف شامخة، واثقة، لا أقبل إلا القمة. بإرادتي وبقوتي سأواصل المسير، لأحقق المزيد، وأثبت أنني ولدت لأكون الأفضل.

إلى عبد المؤمن بوطمينة شريك روحي ورفيق دربي شكرًا لوقوفك بجانبي، أنت جزء من قوتي، وأحد أعمدة نجاحي، فجزاك الله عني خير الجزاء، ورفع مقامك، وحقق لك كل ما تتمنى.

إلى عائلتي الكريمة:

لكل من يحمل لقب مساط، من عماتي وأعمامي، أنتم الامتداد الذي أفتخر به والجذور التي أستمد منها ثباتي.

إلى عائلة بولطيف أتقدم بالشكر والامتنان إلى خالاتي وأخوالي الأفاضل، وعلى رأسهم خالي العزيز عبد الكريم بولطيف، جزيل الشكر والامتنان على ما غمرتموني به من حب ودعاء.

إلى عائلة بوطمينة، أخص بالشكر عمّتي الطيبة عتيقة، وأرفع الدعاء إلى روح العم عبد الوهاب بوطمينة، سائلة الله أن يجعل هذا الإنجاز صدقة جارية في ميزانه.

إلى صديقتي عائشة بوطيبة لك مني أصدق الأمنيات بدوام التوفيق، وأسأل الله أن يحقق لك كل أحلامك.

وأخيرًا، أحمدك ربي حمدًا يليق بجلال وجهك وعظيم سلطانك، وأسألك مزيدًا من التوفيق والنور فيما هو آت.

مساط شيماء

الإهداء

"بسم الله الرحمن الرحيم الحمد لله الذي ما نجحنا ولا تفوقنا إلا برضاه اللهم لك الحمد والشكر على نجاحي فوفقني يا الله وسخرني لأشكرك وأذكر فضلك فيما بقى من عمري، اللهم إني أسألك دوام النجاح ودوام عطاياك لنا. لم تكن الرحلة قصيرة ولا الطريق محفوفاً بالتسهيلات، لكنني فعلتها فالحمد لله الذي يسر البدايات وبلغنا النهايات.

أهدي هذا النجاح لنفسي الطموحة أولا من طفلة صغيرة كانت ترى هذا الحلم بعيد لكنني فعلتها وإنني الآن أقف على باب تخرجي، لكن هذا يعتبر بالنسبة لي بداية لمسيرة نجاحات أخرى بإذن الله.

وبكل حب أهدي ثمرة نجاحي وتخرجي

إلى من خاضوا الحياة لأجلي إلى من غرسوا في قلبي الحلم وسقوه بدعائهم الخالص إلى من كانوا نور دربي وظلي حين أثقلتني الأيام إلى أمي وأبي يا معنى الحياة وأجمل ما فيها هذا النجاح لكم أنا كنت فقط الوسيلة وأنتم الغاية التي سعيت لها بكل قلبي أنتم الإنجاز الحقيقي أنا كنت النتيجة فحسب شكرا لأنكم كنتم وستظلون دوما أعظم انتصاراتي.

إلى أخواتي رفيقات دربي منذ الطفولة شقيقات الروح كنتن دائما الحافز الذي يدفعني للأمام والسند الذي اتكئ عليه في أوقات ضعفي أسأل الله أن يحفظكن لي ما حييت وأن يديم بيننا المحبة. إلى من كان ولا يزال رمزا للحماية والقوة في حياتي إلى من تشرفت بأن أناديه "أخي الوحيد" إلى عوضي الجميل كنت دائما السند والظهر أهديك هذه المذكرة عرفنًا وامتنانًا على كم دعم قدمته أسأل الله أن يزيدك عزا ورفعة.

إلى من كان النور في أيامي والسند في لحظات ضعفي إلى من آمن بي حين شككت في نفسي وشجعني في كل خطوة أهديك هذا الإنجاز لأنك كنت جزءًا منه في كل لحظة.

إلى صديقتي وأختي التي شاركتني رحلة هذا العمل وتشاركنا هذا الحلم أسأل الله أن يكتب لك النجاح الدائم ويحقق لك آمالك. إلى صديقاتي جنود الخفاء الحقيقيات لكن بصماتهم كانت أوضح في كل مرحلة عشتها بالخصوص صديقتي سيليا التي لم تغييرها الأيام والسنوات حفظك الله ورعاك دمتي لي رفيقة الدرب وشكرا لكم على كل الدعم والحب الذي قدمتموه لي.

في الختام أحمدك اللهم حمد الشاكرين اللهم لك الشكر على ما أنعمتني.

بوطيبة عائشة

الفهرس

الفهرس

الملخص

الشكر والتقدير

الإهداء

الإهداء

الفهرس

قائمة الجداول

مقدمة 2

الفصل الأول: الإطار المفاهيمي للدراسة

تمهيد:.....10

المبحث الأول: ماهية الجريمة الإلكترونية 11

المطلب الأول: مفهوم الجريمة الإلكترونية وأسباب انتشارها.....11

الفرع الأول: تعريف الجريمة الإلكترونية. 11

الفرع الثاني: أسباب الجريمة الإلكترونية. 18

المطلب الثاني: مراحل تطور الجريمة الالكترونية وأنواعها.....22

الفرع الأول: مراحل تطور الجريمة الإلكترونية.....22

الفرع الثاني أنواع الجريمة الإلكترونية: 25

المطلب الثالث: خصائص و أركان الجريمة الإلكترونية.....27

الفرع الأول: خصائص الجريمة الإلكترونية. 27

الفرع الثاني: أركان الجريمة الإلكترونية. 32

المبحث الثاني: ماهية الأمن السيبراني وعلاقته بالجريمة الإلكترونية. 37

المطلب الأول: مفهوم الأمن السيبراني وأبعاده. 37

الفرع الأول: تعريف الأمن السيبراني.....37

الفرع الثاني: أبعاد الأمن السيبراني. 41
المطلب الثاني: مراحل تطور الأمن السيبراني وأهميته. 43
الفرع الأول: مراحل تطور الأمن السيبراني. 43
الفرع الثاني: أهمية الأمن السيبراني. 45
المطلب الثالث: علاقة الأمن السيبراني بالجريمة الإلكترونية. 46
الفرع الأول: تأثير الجريمة الإلكترونية على الأمن السيبراني. 47
الفرع الثاني: الجهود الدولية والإقليمية في مكافحة الجريمة الإلكترونية. 51
خلاصة الفصل الأول: 56

الفصل الثاني: سبل تعزيز الأمن السيبراني في ظل تنامي الجريمة الإلكترونية في الجزائر

تمهيد: 58
المبحث الأول: واقع الجريمة الإلكترونية في الجزائر 59
المطلب الأول: تطور وأنواع الجريمة الالكترونية في الجزائر. 59
الفرع الأول: تطور الجريمة الإلكترونية في الجزائر. 60
الفرع الثاني: الجرائم الإلكترونية في الجزائر. 63
المطلب الثاني: تحديات وانعكاسات الجريمة الإلكترونية على الأمن السيبراني في الجزائر. 65
الفرع الأول: تحديات الجريمة الالكترونية في الجزائر. 66
الفرع الثاني: انعكاسات الجريمة الإلكترونية على الأمن السيبراني في الجزائر 72
المبحث الثاني: الاستراتيجية الجزائرية لمكافحة الجريمة الإلكترونية وتحقيق الأمن السيبراني. 76
المطلب الأول: مكافحة الجريمة الإلكترونية في التشريع الجزائري. 76
الفرع الأول: مكافحة الجريمة الإلكترونية بموجب القوانين العامة.....76
الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة. 78
المطلب الثاني: الآليات الأمنية لمكافحة الجريمة الإلكترونية وضمان الأمن السيبيراني. 83
الفرع الأول: المصلحة المركزية لمكافحة الإجرام السيبيراني للدرك الوطني. 83

الفرع الثاني: المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني 84
الفرع الثالث: المصلحة المركزية لمكافحة الجريمة الإلكترونية التابعة للأمن الوطني (SCLC) ..86
الفرع الرابع: المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني. ..87
المطلب الثالث: الآليات الإدارية المختصة لمكافحة الجريمة الإلكترونية وضمان الأمن السيبراني. ..90
الفرع الأول: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. 90
الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. 92
الفرع الثالث: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 95
الفرع الرابع: تنظيم دورات تكوينية ومؤتمرات حول الجريمة الإلكترونية لتحقيق الأمن السيبيراني ..99
خلاصة الفصل الثاني: 101
الخاتمة 103
قائمة المصادر والمراجع 107

قائمة الجداول

قائمة الجداول

رقم الجدول	عنوان الجدول	رقم الصفحة
الجدول رقم (01)	مقارنة بين الجريمة الالكترونية والجريمة التقليدية	**35**
الجدول رقم (02)	توزيع الجرائم الإلكترونية المسجلة في الجزائر لسنة 2024.	**62**
الجدول رقم (03)	مؤشرات الأمن السيبراني في الجزائر مقارنة بالدول المتقدمة (2024).	**66**
الجدول رقم (04)	التدابير القانونية للأمن السيبراني (2024).	**67**
الجدول رقم (05)	التدابير التنظيمية والتقنية للأمن السيبراني (2024).	**68**
الجدول رقم (06)	تطوير الكفاءات التقنية لمكافحة الجريمة الإلكترونية (2024).	**69**
الجدول رقم (07)	التدابير التعاونية الدولية في مجال الأمن السيبراني (2024).	**71**

قائمة المختصرات

قائمة المختصرات:

د.ن: دون طبعة

ج.ر: الجريدة الرسمية

مقدمة

مقدمة

شهد العالم في العقود الأخيرة تحوّلات جذرية في مختلف نواحي الحياة، نتيجةً للثورة التكنولوجية المتسارعة التي أدّت إلى نقلة نوعية شاملة، مست الجوانب السياسية، والاقتصادية، والأمنية، والاجتماعية وذلك بفضل التسهيلات التي تقدمها التكنولوجيا الحديثة. فقد أصبحت الفضاءات الإلكترونية والإنترنت جزءًا لا يتجزأ من الحياة اليومية للأفراد، والمؤسسات، والدول، مما فتح آفاقًا واسعة في العديد من المجالات.

غير أن هذا التقدّم لم يكن خاليًا من التحدّيات، إذ رافقته ظواهر إجرامية مستحدثة فرضت نفسها على المشهد الأمني والقانوني، وعلى رأسها "الجريمة الإلكترونية"، التي ظهرت مع بداية استخدام الحواسيب وانتشار الإنترنت في النصف الثاني من القرن العشرين. وقد أصبحت تُشكّل تهديدًا متناميًا للأفراد والمؤسسات، والدول على حد سواء، بعدما خرجت عن الإطار التقليدي للجرائم، نظرًا لخصائصها المتفردة. فبعد أن كانت مجرد اختراقات بسيطة للأنظمة والشبكات، تطورت لتُستخدم في أنشطة أكثر خطورة، كالتجسس السياسي، والتأثير على الرأي العام، وزعزعة أمن واستقرار الدول، فضلًا عن استخدامها كوسيلة لتحقيق مكاسب مالية غير مشروعة.

تُعد الجزائر كغيرها من الدول عرضة لمخاطر هذه الجرائم التي تتخذ أشكالًا متعددة، حيث عرفت في السنوات الأخيرة تزايدًا ملحوظًا في عدد الجرائم الإلكترونية، سواء تلك التي تستهدف الأفراد وخصوصياتهم، أو تلك الموجّهة ضد المؤسسات والهيئات الحكومية. ومهما تنوّعت صور هذه الجرائم فإنها تؤثر بشكل مباشر على الأمن السيبراني داخل الفضاء الإلكتروني، مما يؤدي إلى اختلال في جهود مكافحتها. وهو ما فرض على المشرّع الجزائري ضرورة تبنّي استراتيجية شاملة ومواكبة لتطورات الجريمة الإلكترونية، سواء من خلال سنّ قوانين متخصصة، أو استحداث هيئات معنية، أو تعزيز القدرات الوطنية في مجال حماية الفضاء السيبراني.

أولا: إشكالية الدراسة:

انطلاقا مما سبق يمكن طرح الإشكالية التالية:

كيف يؤثر انتشار الجريمة الإلكترونية على الأمن السيبراني في الجزائر؟

وبعد طرح الإشكالية نطرح الاسئلة الفرعية التالية:

- ما هي العوامل التي ساهمت في تنامي الجريمة الإلكترونية؟
- ما مدى فعالية وجاهزية الهيئات الوطنية المختصة في مجال الأمن السيبراني لمواجهة التهديدات الإلكترونية في الجزائر؟

ثانيا: فرضية الدراسة:

كلما ارتفعت معدلات الجريمة الإلكترونية، كلما تراجع مؤشر الأمن السيبراني، مما يؤدي إلى زيادة الهشاشة الرقمية للمؤسسات والأفراد والدولة .

ثالثا: أهمية الدراسة:

تكتسي هذه الدراسة أهمية خاصة من الناحية النظرية والعملية، بالنظر إلى ما يشكله موضوعها من ارتباط وثيق بالتحولات التكنولوجية التي يشهدها العالم بصفة عامة، والجزائر بصفة خاصة، في ظل تزايد التهديدات الإلكترونية وتعاظم المخاطر المرتبطة بها على الأمن السيبراني.

وتتجلى أهمية هذه الدراسة في ما يلي:

- **الأهمية النظرية:** تتمثل في المساهمة في تطوير الإطار المفاهيمي للجريمة الإلكترونية والأمن السيبراني، من خلال تحليل العلاقة التفاعلية بين الجانبين، وتوضيح الخصائص القانونية للجريمة الإلكترونية، وكذا انعكاساتها على أمن المعلومات والبنية الرقمية.

- **الأهمية العملية:** تكمن في دراسة الواقع الجزائري ورصد الإشكالات التي تعيق فعالية التصدي للجريمة الإلكترونية، سواء من حيث التشريعات أو القدرات التقنية، مما يسمح بتقديم مقترحات من شأنها تحسين مستوى الحماية السيبرانية.

- **الأهمية التطبيقية:** تظهر من خلال السعي إلى توجيه الانتباه نحو ضرورة بناء استراتيجية وطنية متكاملة لمواجهة الجريمة الإلكترونية، تشمل الجوانب القانونية، التقنية، المؤسسية والتوعوية، وهو ما يجعل الدراسة ذات فائدة للباحثين، والمشرعين، وصناع القرار.

رابعا: أهداف الدراسة:

تهدف هذه الدراسة إلى:

- ضبط مفهوم الجريمة الإلكترونية وتحديد كل ما يرتبط بها، ومن ثم ربطها بمفهوم الأمن السيبراني، ومن ثم تحليل طبيعة العلاقة بين الجريمة الإلكترونية والأمن السيبراني.
- تهدف هذه الدراسة كذلك إلى توفير منظور يمكن من خلاله تفسير ظاهرة الجريمة الإلكترونية ورفع الوعي المجتمعي بخطورتها.
- تسليط الضوء على واقع الأمن السيبراني في الجزائر، من حيث البنية التحتية الرقمية، والإطار التشريعي والتنظيمي، والقدرات المؤسساتية المعنية بالحماية والاستجابة.
- تسليط الضوء على التحديات التي تواجه الأجهزة الأمنية والقضائية بسب انتشار هذا النمط من الجرائم.
- تهدف هذه الدراسة كذلك لتقييم مدى نجاعة السياسات المعتمدة في الجزائر في سبيل حماية الفضاء السيبراني واقتراح حلول وآليات من شأنها تعزيز الأمن السيبراني.

خامسا: أسباب اختيار الموضوع:

هناك جملة من الأسباب التي كانت وراء اختيارنا لهذا الموضوع، والتي تنوعت بين الأسباب الذاتية والموضوعية:

- **الأسباب الموضوعية:**

- التطور السريع للتكنولوجيا مما رافقه من ازدياد ملحوظ في عدد الجريمة الإلكترونية مما يستدعي دراسة معمقة لفهم هذه الظاهرة وأبعادها.
- التهديد المباشر الذي تشكله الجرائم الإلكترونية على الأمن السيبراني سواء على مستوى الأفراد أو المؤسسات أو الدول، مما يجعل من الضروري دراسة وتحليل العلاقة بين الجريمة الإلكترونية ومدى استطاعة المؤسسات في حماية الأمن السيبراني وتحقيقه.
- النقص النسبي في الدراسات القانونية المتخصصة التي تتناول أثر الجرائم الإلكترونية على الأمن السيبراني في الجزائر.
- كثرة هذه الجرائم في الجزائر يستلزم وجود عدة أبحاث التي من شأنها يمكن أن تجد استراتيجية شاملة لمكافحتها وتوفير الحماية داخل الفضاء الإلكتروني.

- **الأسباب الذاتية:**

- يقع هذا الموضوع ضمن أهم المحاور في الحقل المعرفي لاهتمامات الطالبتين الشخصية والذي يتضمن تخصص القانون الجنائي.

- الرغبة الشخصية في التطرق لدراسة أنوع مستحدثة من الجرائم خاصة الجريمة الإلكترونية وباعتباره الموضوع يمس عدة جوانب من الحياة (الجانب الاقتصادي، الجانب السياسي، الجانب الاجتماعي الجانب الأمني..).

- يعد البحث في هذا الموضوع فرصة لاكتساب معارف ومهارات جديدة، في مجال تقنية البحث العلمي والأساليب المنهجية الصحيحة.

- رغبتنا في تقديم اسهام علمي يضاف للمكتبات ويكون نقطة ارتكاز للانطلاق في بحوث أخرى خاصة وأن الدراسات حوله لاتزال مستمرة.

- **الأسباب الموضوعية:**

- التطور السريع للتكنولوجيا مما رافقه من ازدياد ملحوظ في عدد الجريمة الإلكترونية مما يستدعي دراسة معمقة لفهم هذه الظاهرة وأبعادها.

- التهديد المباشر الذي تشكله الجرائم الإلكترونية على الأمن السيبراني سواء على مستوى الأفراد أو المؤسسات أو الدول، مما يجعل من الضروري دراسة وتحليل العلاقة بين الجريمة الإلكترونية ومدى استطاعة المؤسسات في حماية الأمن السيبراني وتحقيقه.

- النقص النسبي في الدراسات القانونية المتخصصة التي تتناول أثر الجرائم الإلكترونية على الأمن السيبراني في الجزائر.

- كثرة هذه الجرائم في الجزائر يستلزم وجود عدة أبحاث التي من شأنها يمكن أن تجد استراتيجية شاملة لمكافحتها وتوفير الحماية داخل الفضاء الإلكتروني.

سادسا: المنهج المتبع.

اعتمدنا في دراستنا لموضوع الجريمة الإلكترونية وتأثيرها على الأمن السيبراني وبهدف توضيح ومعالجة الإشكالية المطروحة على مجموعة من المناهج من أجل تغطية مختلف جوانب الدراسة، وتتمثل هذه المناهج في ما يلي:

- **المنهج الوصفي:** استخدمنا المنهج الوصفي لعرض المفاهيم الأساسية للجريمة الإلكترونية والأمن السيبراني، مع توضيح خصائصها وأركانها، بالإضافة إلى وصف البيئة الرقمية والتحديات التقنية والقانونية المرتبطة بها.
- **المنهج التاريخي:** اعتمدنا المنهج التاريخي لتتبع تطور الجريمة الإلكترونية عالمياً ومحلياً، مما أتاح فهم السياق التاريخي للظاهرة وتحليل مراحل تطورها، بالإضافة إلى دراسة تعامل الجزائر مع هذا التهديد وتطور استراتيجيات مواجهته.
- **المنهج التحليلي:** وظفنا المنهج التحليلي لدراسة النصوص القانونية الجزائرية المتعلقة بالجريمة الإلكترونية، وتحليل فعالية الإجراءات المتخذة، إلى جانب تحليل مؤشرات الأمن السيبراني لاستخلاص نتائج علمية دقيقة.

سابعا: الدراسات السابقة.

- **يوسف صغير** في مذكرته لنيل شهادة الماجستير بعنوان "الجريمة المرتكبة عبر الإنترنت"، جامعة مولود معمري – تيزي وزو،2013 ، تناول الباحث الإطار القانوني للجرائم الإلكترونية، مسلطًا الضوء على التحديات التي تواجه التشريعات التقليدية في التعامل مع هذا النوع من الجرائم.
- **نعمان عبد الكريم** في مذكرته للماجستير بعنوان "الجرائم الإلكترونية وموقف المشرع الجزائري منها "جامعة الجزائر 1 – بن يوسف بن خدة، 2017، قام الباحث بتحليل موقف المشرع الجزائري من الجرائم الإلكترونية، متناولًا الجوانب التشريعية والإجرائية المتعلقة بها.
- **بوحزمة نصيرة** في أطروحة الدكتوراه بعنوان "التحقيق الجنائي في الجرائم الإلكترونية: دراسة مقارنة" جامعة جيلالي ليابس – سيدي بلعباس، 2022، قامت الباحثة بدراسة مقارنة لآليات التحقيق في الجرائم الإلكترونية، مع التركيز على التحديات التي تواجه الأجهزة القضائية والأمنية في جمع الأدلة الرقمية.

- **الطاهر ياكر** في كتابه "الجرائم الإلكترونية: الأحكام الموضوعية والإجرائية"، الصادر عن دار بلقيس، الجزائر، 2024، تناول المؤلف الجوانب الموضوعية والإجرائية للجرائم الإلكترونية، مع التركيز على الطبيعة القانونية لهذه الجرائم والتنظيم التشريعي لمسؤولية مقدمي خدمات الإنترنت.
- **أم الخير معتوق** في مقالها بعنوان "كسب رهان الأمن السيبيراني ضمان لتعزيز الأمن والدفاع الوطنيين في الجزائر"، المنشور في مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون – تيارت، ناقشت الكاتبة العلاقة بين الأمن السيبراني والسيادة الوطنية، وأبرزت التحديات الأمنية المرتبطة بالتهديدات الرقمية.

على الرغم من الأهمية البالغة للدراسات السابقة، إلا أن هذه الدراسة تتميز عن غيرها من خلال:

- التركيز على العلاقة التفاعلية بين الجريمة الإلكترونية والأمن السيبراني، من حيث التأثيرات المتبادلة.
- تحليل واقع الجريمة الإلكترونية في الجزائر بالأرقام والإحصائيات، ورصد التحولات من الجرائم الفردية إلى الشبكات المنظمة.
- تقديم مقاربة تحليلية متكاملة تشمل الأبعاد القانونية، التقنية، الأمنية، والسياسية في آنٍ واحد.

ثامنا: صعوبات الدراسة:

بالرغم من الأهمية التي يحظى بها الموضوع إلا أننا وجدنا صعوبات:

- صعوبة الاحاطة الشاملة بالجريمة الالكترونية وأشكالها ووسائل ارتكابها نظرا لكونها جريمة مستحدثة ومتطورة باستمرار.
- قلة المراجع المتخصصة بالغة العربية خصوصا في الجانب المتعلق بالأمن السيبراني.
- صعوبة الحصول على بيانات وإحصائيات موثوقة، فالكثير من الهيئات تتردد في الإفصاح عن البيانات بشكل دقيق لأسباب أمنية وسيادية.
- ضعف الوعي العام حول أهمية الأمن السيبراني، سواء في الأوساط الأكاديمية أو المؤسساتية، مما ينعكس على صعوبة الوصول إلى مختصين أو مشاركين يمتلكون خبرة ميدانية معمقة في هذا المجال.

- عدم وجود اطار تشريعي متكامل خاص بمعالجة الجريمة الإلكترونية، وهذا ما شكل تحديًا إضافيًا أمام الطالبتين لفهم الإطار القانوني الحالي، خاصة مع عدم توفر نصوص قانونية متكاملة تغطي جميع جوانب الجريمة السيبرانية.

تاسعا: تقسيم الدراسة.

بهدف الإجابة على الإشكالية البحثية المطروحة، تم تقسيم الدراسة إلى فصلين رئيسيين. جاء الفصل الأول بعنوان "**الإطار المفاهيمي للدراسة**"، وقُسم إلى مبحثين؛ حيث تناول المبحث الأول ماهية الجريمة الإلكترونية، بينما ركز المبحث الثاني على مفهوم الأمن السيبراني وعلاقته بالجريمة الإلكترونية. أما الفصل الثاني، فجاء بعنوان "**الجريمة الإلكترونية في الجزائر وسبل تعزيز الأمن السيبراني الوطني**" وقُسم كذلك إلى مبحثين؛ تناول الأول واقع الجريمة الإلكترونية في الجزائر، فيما استعرض المبحث الثاني السياسات والاستراتيجيات المعتمدة لتعزيز الأمن السيبراني الوطني.

الفصل الأول:

الإطار المفاهيمي للدراسة

تمهيد:

إن التطور التكنولوجي السريع في العصر الرقمي قد أسفر عن تغييرات جذرية في جميع مجالات الحياة، من خلال تبني المجتمعات للأنظمة الرقمية في كافة مجالاتها الاقتصادية، الاجتماعية والسياسية. ومع هذه التحولات العميقة، برزت العديد من التحديات، أبرزها الجريمة الإلكترونية التي أصبحت تهدد الأفراد، المؤسسات، بل والدول أيضًا. فالجريمة الإلكترونية لا تقتصر على الأفعال غير القانونية التي تُرتكب باستخدام الإنترنت، بل هي ظاهرة معقدة تتداخل فيها عدة عوامل تكنولوجية، اجتماعية، ونفسية مما يجعلها قادرة على إلحاق أضرار جسيمة بالأمن الشخصي والمؤسسي وحتى الأمن القومي.

ومن أجل التصدي لهذه الظاهرة، برز مفهوم "الأمن السيبراني" كحاجة ملحة للحفاظ على الأمن المعلوماتي وحماية الأنظمة والشبكات من الهجمات الإلكترونية. وبالتالي، يشكل فهم العلاقة بين الجريمة الإلكترونية والأمن السيبراني أمرًا ضروريًا في عصر تكنولوجيا المعلومات. إذ يتطلب الأمر تحليلًا معمقًا للتعريفات المختلفة المتعلقة بالجريمة الإلكترونية، دراسة أسباب انتشارها، وأنواعها، وكذلك خصائصها بالإضافة إلى فهم الأبعاد المتعددة للأمن السبيراني وتأثيراته على مختلف المجالات.

يهدف هذا الفصل إلى تقديم إطار مفاهيمي دقيق يعزز الفهم الشامل للجريمة الإلكترونية، من خلال مناقشة مفهوم الجريمة الإلكترونية وأسباب انتشارها، بالإضافة إلى توضيح دور الأمن السبيراني في مواجهة التهديدات الناجمة عنها.

المبحث الأول: ماهية الجريمة الإلكترونية

أدى التوسع في استخدام التكنولوجيا الرقمية إلى ظهور أنماط إجرامية مستحدثة كالجريمة الإلكترونية، التي باتت تشكل تحديًا متناميًا للأنظمة القانونية والأمنية على الصعيدين الوطني والدولي. ويعود ذلك إلى طبيعتها المعقدة، سواء من حيث بيئتها غير المادية أو الأدوات التقنية المستخدمة فيها أو من حيث النتائج المترتبة عنها. ونظرًا لأهمية الإحاطة بهذه الظاهرة، يُخصص هذا المبحث لتوضيح الإطار المفاهيمي والخصائص الجوهرية التي تميز الجريمة الإلكترونية عن غيرها من الجرائم، وعليه قسم هذا المبحث إلى ثلاث مطالب:

المطلب الأول يعالج التعريفات المختلفة للجريمة الإلكترونية مع بيان أبرز العوامل التي ساهمت في انتشارها على نطاق واسع، أما المطلب الثاني، فسيُعنى بتتبع المراحل التي مرت بها هذه الجريمة منذ ظهورها بالإضافة إلى استعراض أبرز تصنيفاتها، أما المطلب الثالث فسيتم من خلاله تسليط الضوء على السمات الأساسية التي تنفرد بها، ثم تحليل الأركان القانونية التي تُبنى عليها المسؤولية الجنائية في هذا السياق.

المطلب الأول: مفهوم الجريمة الإلكترونية وأسباب انتشارها.

يُشكّل تحديد مفهوم الجريمة الإلكترونية إشكالية أساسية في ظل تعدد المقاربات وتباين الخلفيات الفقهية والقانونية، الأمر الذي أفرز تعاريف متباينة باختلاف المرجعيات المعتمدة. كما تساهم عوامل متعددة في تفسير اتساع نطاق هذه الظاهرة وانتشارها السريع عبر المستويين الوطني والدولي. وبناءً عليه، يتناول هذا المطلب في فرعه الأول تحليل مفهوم الجريمة الإلكترونية وفق أبرز التعريفات اللغوية والفقهية والقانونية، بينما يخصص فرعه الثاني لبحث الأسباب الرئيسية لانتشارها من خلال تصنيفها وفق أبعادها الدولية والاقتصادية والاجتماعية والنفسية.

الفرع الأول: تعريف الجريمة الإلكترونية.

يعد تحديد مفهوم الجريمة الإلكترونية خطوة ضرورية لفهم طبيعتها القانونية والواقعية، خاصة في ظل تعدد وجهات النظر حولها، فقد تعددت المصطلحات التي أُطلقت عليها مثل:"جرائم الكمبيوتر والإنترنت وجرائم الحاسب الآلي **" Computer Crimes"** والجرائم الرقمية **" Digital Crimes "** والجرائم

الناعمة " **Crimes Soft** "، الجرائم عالية التقنية "**High-Tech Crimes** " وجريمة الياقات البيضاء " **White Collar Crimes** "، والجرائم النظيفة " **Clean Crimes** ".[1]

وانطلاقًا من ذلك، سنعرض في هذا الفرع التعريف اللغوي لكل من "الجريمة" و"الإلكترونية"، ثم ننتقل إلى التعريف الاصطلاحي بشقيه الفقهي والقانوني، كما ورد في الدراسات والأنظمة التشريعية المختلفة:

أولا: التعريف اللغوي.

يتكون مصطلح الجريمة الإلكترونية والتي تعرف باللغة الإنجليزية بـ **"Cyber Crime"** من جزئين هما: الجريمة **"Crime"**، والإلكترونية **"Cyber"**، ولكل منهما معنى خاص ومستقل ما يتطلب التناول الدقيق والوقوف على دلالتهما اللغوية.

فالجريمة لغةً: الجريمة والجُرم معناها في اللغة الذنب، ومن اشتقاقها جَرم وأَجْرم و اجترام، وتجَّرم عليه بمعنى اتَّهَمَه بذنْبٍ لم يرتكبه ، وكلمة لا جرم تعني القسم، والجرم هو الذنب أو الجناية.[2]

أما التعريف الاصطلاحي للجريمة: هي فعل يفرض له القانون عقاباُ وتعني العمل الخارجي الذي يأتيه الإنسان مخالفا به للنص قانون، [3] والذي يقرر له القانون عقوبة وجزاء لمخالقته للقانون.

أما الإلكترونية (المعلوماتية) لغة: يقصد بها المعالجة الآلية للمعلومات وهي ترجمة للمصطلح الفرنسي **"Informatique"**، وهي اختصار للكلمتين الفرنسيتين " **Information** " معلومات " **Automatique** " ذاتيا، وصاحب هذا المصطلح هو فليب درايفوس **"Philip Dreyfus** " الذي أراد أن يعني به "**العلم الذي يربط علم الحاسوب "Computer Science" والمعلومات " Information " والاتصالات " Télécommunications " [4].**

---

[1] فريد ناشف، "آليات التعاون الدولي في مكافحة الجرائم الإلكترونية "، **مجلة البحوث في الحقوق والعلوم السياسية**، المجلد 08، العدد 01، جوان 2022، ص 432.

[2] ميرفت محمد حبابية، "**مكافحة الجريمة الإلكترونية: دراسة مقارنة في التشريع الجزائري و الفلسطيني**"، المجلد 01، ط الأولى، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2020، ص 29.

[3] زينب ياقوت، "واقع الجريمة عير الفيسبوك وسبل الحد من انتشارها دراسة حالة الجزائر"، **مجلة الدراسات والبحوث القانونية**، المجلد 07، العدد 02، جوان 2022، ص 288.

[4] ميرفت محمد حبابية، مرجع سبق ذكره، ص29.

ثانيا: التعريف الاصطلاحي.

سيشمل كل من التعريف الفقهي والتعريف القانوني.

1. التعريف الفقهي.

على الرّغم من محورية مصطلح الجريمة الإلكترونية **"cyber crime"** في العديد من الدراسات الأكاديمية التي تتناول التهديدات الالكترونية في العصر الحديث،[1] إلاّ أن الفقه الجنائي قد بذل من أجل ذلك عدة محاولات لتعريف هذه الجريمة لكنّه لم يتفق على تسمية موحدة لها،[2] حيث إعتمد كل اتجاه على معيار معيّن في ذلك :

أ) تعريف الجريمة الإلكترونية بالاستناد إلى وسيلة ارتكابها.

يستند أنصار هذا الاتجاه في تعريف للجريمة الالكترونية على وسيلة ارتكابها، فيشترطون حدوثها بواسطة الكومبيوتر، لذلك عرّفها الفقيه تايدرمان **"Tiedermen"** بأنها:" **كل أشكال السلوك الغير مشروع (الضّار بالمجتمع) الذي يرتكب باستخدام الحاسب الآلي".**[3]

وعرّفها أيضا الفقيه الإنجليزي توم فورستر **"Tom Forester"** " **فعل إجرامي يستخدم الكومبيوتر ارتكابه كأداة رئيسية".**[4]

ب) تعريف الجريمة الإلكترونية بالاستناد إلى المعرفة بتقنية المعلوماتية:

يعتمد أصحاب هذا الاتجاه على معرفة الجاني بالتقنية المعلوماتية كمعيار لتعريف الجريمة الإلكترونية، حيث قاموا بتعريفها استنادًا إلى توفر المعرفة الفنية بتكنولوجيا المعلومات لدى مرتكبها، ومن أبرز أنصار هذا الاتجاه الفقيه البلجيكي سيتن ستشيولبيرج **"Stein Schiollberg"** الذي عرّف الجريمة

[1] الطاهر ياكر، **الجرائم للإلكترونية الأحكام الموضوعية والإجرائية**، د ط، دار بلقيس للنشر، الجزائر، 2024، ص 10.

[2] نصيرة بوحزمة ، **التحقيق الجنائي في الجرائم الالكترونية (دراسة مقارنة)**، أطروحة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2022، ص 13.

[3] المرجع نفسه، ص 14.

[4] ميرفت محمد حبايبة، مرجع سبق ذكره، ص31 .

الإلكترونية " **أي فعل غير مشروع تكون المعرفة بتقنية الكومبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائياً**".[1]

وعرّفها دافيد ثومسون **"David Tompson"** "**هي جرائم يكون متطلباً لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب**"، [2] من خلال هذا تبين أن كل من سيتن ستشيولبيرج و دافيد ثومسون ركزا على ضرورة توفر الجريمة الإلكترونية على شرط جوهري لا تقوم دونه وهو امتلاك الفاعل الإلكتروني المعرفة التقنية إذ يفترض أن كل جريمة إلكترونية تتطلب معرفة تقنية متقدمة.

ج) تعريف الجريمة الإلكترونية بالاستناد إلى موضوعها .

يستند أصحاب هذا الاتجاه في تعريفهم للجريمة الإلكترونية إلى اعتبار الحاسوب محلًا للجريمة حيث يُشترط أن يقع الاعتداء على الحاسوب أو على نظامه لتحدث الجريمة الإلكترونية، ومن أمثلة ذلك سرقة أو تقليد أو إتلاف أو تعطيل برامج الحاسوب، أو إفشاء محتوياته، أو حذف أو تغيير أو تزوير أو نسخ المعلومات المعالجة إلكترونيًا. ويمثل هذا الاتجاه الفقيه روزنبالث **"Rosenbelt"** الذي عرّف الجريمة الإلكترونية بأنها" **نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تُحول عن طريقه**"[3]، أما الفقيهان الفرنسيان "لي ستانس" و"فيفايت" **"Le Staince and Vivant"** فعرفا الجريمة الإلكترونية بأنها: " **مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب**".[4]

2. **التعريف القانوني.**

أصبحت الجريمة الإلكترونية في ظل التطور السريع لتكنولوجيا الإعلام والاتصال تشكّل تهديدًا للمجتمع الدولي، مما أدى إلى ضرورة تبنّي سياسات فعّالة لمكافحتها والحدّ منها، وتجدر الإشارة إلى أن معظم التشريعات قد تجنبت وضع تعريف قانوني صريح للجريمة الإلكترونية وأوكلوا مهمة ذلك للفقه

[1] ميرفت محمد حبايبة ، مرجع سبق ذكره، ص 32.

[2] غنية باطلي ، **الجريمة الإلكترونية (دراسة مقارنة)**، أطروحة دكتوراه في القانون الخاص، كلية الحقوق، جامعة باجي مختار، عنابة،2011 ، ص 13.

[3] نصيرة بوحزمة ، مرجع سبق ذكره، ص 16.

[4] ميرفت حبايبه، مرجع سبق ذكره، ص 32.

والقضاء.[1] في المقابل سعى بعض المشرّعين إلى تقديم تعريفات قانونية للجريمة الإلكترونية، وفي ما يلي أبرز النماذج التشريعية التي تناولت مفهوم الجريمة الإلكترونية:

أ) تعريف المشرع السويدي.

تعتبر السويد الدولة أولى التي سنت تشريعات خاصة بجرائم الحاسب الآلي والأنترنت، حيث صدر قانون البيانات السويدي سنة 1973 تتبعها الولايات المتحدة الأمريكية حيث شرعت قانونا خاص بحماية انظمة الحاسب الآلي سنة 1985 فأصدرت قانون بتاريخ 08 جانفي 1988 لمكافحة الجريمة الإلكترونية مع استحداث لمواد جديدة تخص الجرائم الإلكترونية في قانون العقوبات.[2]

ب) تعريف المشرع الأمريكي.

عرف المشرع الأمريكي الجريمة الإلكترونية بأنها: "**الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المعتمد الضار لأجهزة الكمبيوتر أو ملفات البيانات وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة**".[3]

ج) تعريف المشرع الفرنسي.

في الأمر الصادر 1945/06/30 والمتعلق بالتحقيق والمتابعة وقمع الجرائم الماسة بالتشريع الاقتصادي الفرنسي، وهذا ما نصت عليه المادة الأولى من هذا الأمر فالمادة 1/323 من قانون العقوبات الفرنسي تعاقب على فعل الدخول أو البقاء الغير المشروع في نظام المعالجة الآلية للمعلومات أو محو أو تغيير البيانات.[4]

---

[1] نصيرة بوحزمة ، مرجع سبق ذكره، ص 24.

[2] حاتم بن عزوز، مناني حليمة، "الأمن السيبراني و الجريمة الإلكترونية في الدول ما بعد الحداثية: الولايات المتحدة الأمريكية (نموذجا)"، **مجلة الرسالة للدراسات الاعلامية**، المجلد 06، العدد 02، جوان 2022، ص 583.

[3] يوسف خليل يوسف العفيفي، **الجرائم الإلكترونية في التشريع الفلسطيني(دراسة تحليلية مقارنة)**، رسالة ماجستير قسم القانون العام ، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2013، ص 07.

[4] حاتم بن عزوز، حليمة مناني، مرجع سبق ذكره، ص 583.

د) تعريف المشرع المصري.

قامت جمهورية مصر العربية ففي عام 2018 بإصدار قانون رقم 175 المتعلق بمكافحة جرائم تقنية المعلومات، والهدف منه التصدي للجرائم التي يتم ارتكابها من خلال تكنولوجيا المعلومات والاتصالات، [1] غير أن المشرع المصري لم يتطرق لتعريف الجريمة الإلكترونية بل اكتفى بتعريف المعالجة الإلكترونية ومجموعة من المصطلحات المتشابهة، كما أن القانون حدد مواد لمواجهة كل الجرائم التي من شأنها تضر بمصالح وحياة الناس باستخدام التقنيات التكنولوجية الحديثة. كما قام بتحديد الاجراءات المتبعة والعقوبات لكل نوع من الجرائم المنصوص عليها في نص هذا القانون.

هـ) تعريف المشرع الفلسطيني.

فإنه وبموجب قرار رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته، لم يضع تعريفا للجريمة الإلكترونية، واكتفى بتعريف تكنولوجيا المعلومات. [2] حيث نصت المادة1 منه على:" **أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية أو أي وسيلة أخرى سواء كانت مادية أم غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين البيانات أو الاتصالات تتعلق او تعمل بالاقتران مع مثل هذه الوسيلة.**"[3]

و) تعريف المشرع الجزائري.

عرف المشرع الجزائري الجريمة الإلكترونية من خلال ما نصت عليه المادة 2 فقرة (أ) من القانون رقم (09-04) المؤرخ في 05-09-2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنها :"**هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في**

[1] القانون رقم 175، المؤرخ في 14 أغسطس 2018، المتعلق بمكافحة جرائم تقنية المعلومات، ج. ر، العدد 32، 2018.

[2] ميرفت محمد حبابية، المرجع السابق، ص39.

[3] قرار بقانون رقم 10 ، المؤرخ في 03 ماي 2018، المتعلق بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، ج. ر الفلسطينية، العدد 16، 2018.

قانون العقوبات وأي جريمة من أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية". [1]

يتضح من نص هذه المادة أن مفهوم الجريمة الإلكترونية يرتبط ارتباطًا وثيقًا بالنظام المعلوماتي إذ لا يمكن تحقق هذه الجريمة إلا من خلاله، لكونه يمثل الوسيلة الأساسية في ربط الحواسيب بشبكة الاتصال العالمية وتداول المعلومات والبيانات، [2] وفي هذا السياق قام المشرع الجزائري بتجريم الأفعال التي تمس بأنظمة الحاسب الآلي، تأثرًا بالثورة المعلوماتية التي أفرزت أنماطًا مستحدثة من الإجرام، لم يشهدها العالم من قبل.[3]

وهذا ما دفع بالمشرع الجزائري إلى تعديل قانون العقوبات (الأمر رقم 66-155) بموجب قانون رقم 04-15 المؤرخ في 10نوفمبر 2004، حيث أفرد له القسم السابع مكرر وعنونه بالمساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن بدوره 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر07.[4]

يتّضح مما سبق، أن المشرع الجزائري تبنّى في تحديد مفهوم الجريمة الإلكترونية مقاربة متعددة المعايير حيث استند أولًا على معيار وسيلة ارتكاب الجريمة والمتمثل في نظام الاتصالات الإلكتروني ومعيار موضوع الجريمة من خلال الاعتداء على أنظمة المعالجة الآلية للمعطيات، وثالثًا معيار الركن الشرعي المنصوص عليه في قانون العقوبات، وأخيرا المعيار الرابع والذي يتعلق بنطاق الجريمة المعلوماتية، وهو ما أسهم في توسيع مفهوم الإجرام السيبراني ضمن الإطار القانوني الجزائري لمكافحة الجريمة الإلكترونية.[5]

---

[1] قانون رقم 09-04، المؤرخ في 05-09-2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، ج. ر، العدد 47، الصادر في 16 أوت 2009.

[2] الطاهر ياكر، مرجع سبق ذكره، ص 16 ص17 .

[3] شهرزاد بولحية، رشيد حلوفي، "تحديات الجريمة الإلكترونية في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، ، المجلد 04، العدد 02، جانفي 2020، ص 11.

[4] قانون رقم 04-15، المؤرخ في 10 نوفمبر2004، المتضمن قانون العقوبات، ج .ر، العدد 71، 2004 .

[5] نصيرة بوحزمة ، مرجع سبق ذكره، ص25.

وبموجب الأمر 11/21 المتضمن تعديل قانون الإجراءات الجزائية واستحداث القطب الجزائي الوطني المتخصص في هذه الجرائم، عرفت الجريمة الإلكترونية من خلال نص المادة211 مكرر22 الفقرة 03 أنها: **"أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام الاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام والاتصال".**[1]

الفرع الثاني: أسباب الجريمة الإلكترونية.

تُعد الجريمة الإلكترونية إحدى الظواهر الإجرامية المستحدثة التي جذبت اهتمامًا واسعًا في العصر الرقمي، وهناك عدة عوامل تدفع الأفراد إلى ارتكاب الجرائم الإلكترونية مما ساهم في توسع نطاقها وانتشارها، ويمكن تصنيف هذه العوامل إلى مستويات متعددة بعضها يرتبط بالجوانب الشخصية وبعضها بالبيئة الاجتماعية، وأخرى ناتجة عن ظروف دولية عامة، نتيجةً لذلك، تتداخل عدة عوامل فردية واجتماعية ودولية في نشوء هذه الجرائم. في هذا الفرع سنسلط الضوء على أبرز أسباب الجريمة الإلكترونية:

أولا: الأسباب الدولية.

1. التطور التكنولوجي:

فتح التطور التكنولوجيا آفاقًا جديدة أمام مجرمي الإنترنت، إذ يمكن استغلال تطورات الذكاء الاصطناعي والتقنيات الحديثة الأخرى لتطوير هجمات أكثر تعقيدًا ويصعب في الكشف عنها، علاوة على ذلك، قد يستمر نمو الجرائم الإلكترونية ما لم تُتخذ إجراءات مقابلة للحد منها.[2]

2. العولمة:

خلق ظهور "الفضاء الإلكتروني" ظواهر جديدة تتجاوز مجرد وجود أنظمة الحواسيب، إذ تظهر فروق في التزام الأفراد بالقوانين مقارنة بسلوكهم في العالم المادي، فقد يرتكب الأفراد جرائم عبر الإنترنت

[1] الأمر رقم 11/21 الذي يتمم الأمر 66-155، المؤرخ في 25 أوت 2021، المتضمن تعديل قانون الإجراءات الجزائية ج .ر، عدد 65، 2021.

[2]Idonet Taem,, " **Factors Causing Cyber Crims to Easily Occur**" Idonet, 31 Jan 2024, availablei in : https://indonet.co.id/factors-causing-cyber-crimes-to-easily-occur/, accesed :17 Apr 2025, at : 22:15.

قد لا يرتكبونها في الواقع، مستفيدين من مرونة الهوية وعدم ظهورها، وضعف عوامل الردع، مما يحفز السلوك الإجرامي الافتراضي.[1]

3. التفاوت في التشريعات والقوانين.

لا تزال العديد من الدول تفتقر إلى التشريعات الملائمة لمواكبة تطور الجرائم الإلكترونية وأساليبها المتجددة، مما يشمل ضعف قدرات الشرطة والقضاء في التعامل مع الأدلة الرقمية. ويؤدي هذا النقص إلى ضعف الملاحقة القانونية، مما يسمح بازدهار الجرائم الإلكترونية محليًا ودوليًا.[2]

ثانيا: الأسباب الاقتصادية.

1. البطالة "Unemployment":

ترتبط الجريمة الإلكترونية مثلها مثل الجريمة التقليدية، بظاهرة البطالة والظروف الاقتصادية الصعبة، فالبطالة بين الشباب خاصة من يمتلك منهم مهارات رقمية تشكل دافع لاستثمار معارفهم في أنشطة إجرامية إلكترونية.[3]

2. البحث عن الثراء " Quest of Wealth":

يُعد السعي وراء تحقيق مكاسب مالية سريعة دون عناء من أبرز الدوافع لارتكاب الجرائم الإلكترونية سواء عبر الابتزاز أو بيع البيانات المسروقة. مع التحول العالمي نحو الاقتصاد الرقمي أصبحت الجرائم الإلكترونية أكثر جاذبية لملاحقة الربح السريع.[4] يرى العديد من مرتكبي الجرائم الإلكترونية أن الفضاء الرقمي فرصة سهلة وآمنة لتحقيق الربح السريع كما عبّر عن ذلك سارق البنوك

---

[1] عفاف بوعون، نسيمة أولاد سالم، "الجريمة الإلكترونية (قراءة سوسيوتاريخية في النشأة والأثار)"، **مجلة القيس للدراسات النفسية والاجتماعية**، المجلد 05، العدد 20، ديسمبر 2023، ص 84.

[2] مرجع نفسه، ص 84.

[3] موسى ذياب البداينة، "**الجرائم الإلكترونية– المفهوم والأسباب**"، ورقة بحث مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، عمان– الأردن، المنعقد يومي 2–4 سبتمبر 2014، ص14 ص 15.

[4] **Christopher Hill**, "**What are the motives behind cybercrimes ?**", Chill Cyber Security, Idonet, 20 May 2024,availablei at : https://www.chillcybersecurity.co.uk/what-are-the-motives-behind-cybercrimes/ Accesed :18 Apr 2025 ,at : 23:31.

الأمريكي "ويل ساتون" بقوله الشهير" **:لأن هناك النقود"**، مما يعكس منطق استغلال غياب الرقابة القانونية لتحقيق المكاسب.[1]

3. انكشاف البنية التحتية المعلوماتية الدولية:

تتعرض البنية التحتية التقنية لمخاطر متعددة، مثل الكوارث الطبيعية والإهمال البشري. وقد حدد التقرير الرئاسي الأمريكي خمسة قطاعات حساسة تشمل:[2]

- ❖ قطاع الاتصالات والمعلومات **"Information and Communication"**: يضم شبكات الاتصالات العامة والإنترنت واستخدامات الحاسوب الأكاديمية والحكومية والتجارية.
- ❖ قطاع التوزيع المادي (الفيزيقي) **"Distribution Physical"**: يشمل طرق المواصلات السكك الحديدية، الموانئ، المطارات، وشركات النقل والشحن.
- ❖ قطاع الطاقة **"Energy"**: يضم صناعات إنتاج وتوزيع الكهرباء، البترول، والغاز الطبيعي.
- ❖ قطاع المال والبنوك **"Finance and Banking"**: يتضمن البنوك، وشركات الخدمات المالية ونظم الرواتب والاستثمار والتبادلات المالية.
- ❖ قطاع الخدمات الإنسانية الحيوية **"Services Human Vital"**: يشمل أنظمة إمداد المياه خدمات الطوارئ، والخدمات الحكومية مثل الضمان الاجتماعي وإدارة السجلات المدنية.[3]

ثالثا: الأسباب الاجتماعية والنفسية.

1. الاسباب الاجتماعية:

أ) **التحضر"Urbanization"**: يساهم التحضر والهجرة الداخلية نحو المدن في رفع معدلات الجريمة الإلكترونية، نتيجة مواجهة تكاليف المعيشة المرتفعة وضعف البنية التحتية الاجتماعية، كما

---

[1] نعمان عبد الكريم، **"الجرائم الإلكترونية وموقف المشرع الجزائري منها"**، مذكرة ماجستير، كلية الحقوق، الجزائر، 2017 ص 117.

[2] إسراء جبريل رشاد مراعي، " الجرائم الإلكترونية: الأهداف– الأسباب– طرق الجريمة ومعالجتها"، **مجلة الدراسات الإعلامية**، المركز الديموقراطي العربي، العدد الأول، يناير 2018، ص 438 ص 439.

[3] موسى ذياب البداينة ، مرجع سبق ذكره، ص 18.

يشير **"Meke" "أنّ التحضر سبب رئيسي للجرائم الإلكترونية في نيجيريا وأنّ التحضر بدون جريمة مستحيل والاستثمار في الجريمة الالكترونية مُربح "**.[1]

ب) **الضغوط العامة "Strains"**: تؤدي الضغوط الاجتماعية الناتجة عن الفقر والبطالة والأمية إلى دفع الأفراد، خاصة الشباب، إلى البحث عن أساليب سلبية للتكيف مع هذه الظروف، من ضمنها الانخراط في أنشطة إلكترونية غير قانونية.[2]

ج) **التفكك الأسري"Family disintegration"**: يؤدي ضعف الروابط الأسرية إلى آثار نفسية واجتماعية سلبية على الأطفال والمراهقين، مما يجعلهم أكثر عرضة للانحراف واستخدام الفضاء الإلكتروني كوسيلة للتعبير عن تمردهم.[3]

2. الأسباب النفسية:

أ) **إثبات الذات:** يسعى بعض الأفراد، خصوصًا الشباب، إلى إثبات قدراتهم عبر اختراق الأنظمة وكسر الحواجز الأمنية، في محاولة لجذب الانتباه ونيل التقدير.[4]

ب) **الرغبة في التعلم:** تشكل الرغبة العميقة في فهم آليات عمل أنظمة الحاسوب والشبكات دافعًا لبعض الأفراد لارتكاب الجرائم الإلكترونية. وقد أشار "ستيفن ليفي" في كتابه قراصنة الأنظمة إلى أن هؤلاء الأفراد يتبنون مبادئ تقوم على أن الوصول إلى المعلومات يجب ألا يكون مقيدًا وأن فهم النظام يساعد في فهم كيفية تسيير العالم.[5]

ج) **الانتقام:** تُعد مشاعر الانتقام والحقد من الدوافع النفسية القوية وراء ارتكاب الجرائم الإلكترونية. فكثيرًا ما يكون الدافع هو الانتقام من أفراد أو مؤسسات معينة، حيث تدفع مشاعر الكراهية العميقة

---

[1] حفيظة خلوف،" **تطور الجريمة الإلكترونية في ظل التغيرات الحاصلة**"، الملتقى العلمي الوطني بعنوان: الجرائم المستحدثة أنواعها ومخاطرها...وآليات مواجهتها، جامعة مولود معمري تيزي وزو، المنعقد يومي 27 و28 ديسمبر 2022، ص127.

[2] إسراء جبريل رشاد مراعي، مرجع سبق ذكره، ص 435.

[3] جعفر بن محمد بن ذيب بن شفلوت، "العوامل الاجتماعية المؤدية لارتكاب الجرائم الإلكترونية في المجتمع السعودي"، دراسة ميدانية على المحققين في النيابة العامة بمدينة الرياض، **مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية**، جامعة الفيوم، العدد 27، 2022، ص 243.

[4] نعمان عبد الكريم، مرجع سبق ذكره ، ص 118.

[5] المرجع نفسه ، ص118.

الجاني إلى التخطيط لهجمات إلكترونية بهدف الإضرار بالضحية وتحقيق نوع من الإشباع الشخصي.[1]

المطلب الثاني: مراحل تطور الجريمة الالكترونية وأنواعها.

شهدت الجريمة الإلكترونية تحولات جوهرية ارتبطت بتطور تكنولوجيا المعلومات والاتصالات وقد أفرز هذا التطور المتسارع أنماطًا جديدة من السلوك الإجرامي تجاوزت الحدود التقليدية للجريمة، سواء من حيث الوسائل أو من حيث الأهداف والضحايا، وبناءً على ذلك، يهدف هذا المطلب إلى تسليط الضوء على مراحل تطور الجريمة الإلكترونية من خلال تتبع تطورها التاريخي وتحليل العوامل التقنية التي ساهمت في نشوئها وتوسعها، وذلك في **الفرع الأول**، أما **الفرع الثاني** فيعالج تصنيفات هذه الجريمة من خلال إبراز أنواعها الرئيسية وفقًا لطبيعة الحقوق أو المصالح محل الاعتداء كالأشخاص والأموال وأمن الدولة.

الفرع الأول: مراحل تطور الجريمة الإلكترونية.

تُعد الجريمة الإلكترونية من أبرز التحديات التي تهدد الأمن المعلوماتي في العصر الرقمي، فمع الطفرة التكنولوجية المتسارعة والاعتماد المتزايد على الحواسيب والإنترنت في مختلف جوانب الحياة أصبحت هذه الجريمة أكثر تعقيدًا وخطورة. ونظرًا لأهميتها وتأثيرها العميق، أصبح من الضروري تتبع تطورها التاريخي لفهم طبيعتها وآلياتها بشكل أدق. **وفي هذا الفرع لجأنا إلى تقسيم الجريمة الإلكترونية إلى أربع مراحل رئيسية**، ارتبطت كل مرحلة منها بالتطورات التقنية والتكنولوجية التي عرفها العالم خلال العقود الماضية.

أولا: المرحلة الأولى (من الخمسينيات إلى الستينيات من القرن الماضي).

بدأت جرائم الحاسوب في الظهور مع بداية الخمسينيات بالتزامن مع انتشار الاستخدام التجاري للحواسيب، وقد اقتصرت هذه الجرائم في بداياتها على إساءة استخدام الحاسوب، حيث سُجلت في الولايات المتحدة الأمريكية أول حالة جرمية من هذا النوع سنة 1957.[2] لاحقًا، بدأت التقارير تصدر لرصد نسب وأعداد حالات إساءة استخدام الحواسيب، حيث صُنفت هذه الجرائم تحت عدة أنواع، منها:

[1] نهلا عبد القادر المؤمني، "**الجرائم المعلوماتية**"، ط 2، دار الثقافة للنشر والتوزيع، عمان،2010، ص 89 ص 90.

[2] ميرفت محمد حبايبة، مرجع سبق ذكره، ص25 ص26.

العبث والتخريب، سرقة المعلومات، الاحتيال، والاستخدام غير لاحقًا بدأت التقارير تصدر لرصد نسب وأعداد حالات إساءة استخدام الحواسيب، حيث صُنفت هذه الجرائم تحت عدة أنواع، منها: العبث والتخريب، سرقة المعلومات، الاحتيال، والاستخدام غير المصرح به لخدمات الحاسوب[1]. وكان تعامل مع هذه الجرائم كأي جريمة تقليدية أخرى ، دون تمييزها عن غيرها من الجرائم الجنائية المعروفة. وخلال هذه الفترة، شاعت الحواسيب بشكل أوسع، وبرز مفهوم إساءة استخدامها والتلاعب ببياناتها في مطلع الستينيات، وبدأت الصحف لأول مرة بنشر مقالات تتناول هذه الظاهرة، مركزةً على قضايا العبث بالبيانات المخزنة وتدمير أنظمة الحواسيب. [2]

ثانيا: المرحلة الثانية (من السبعينات الى الثمانينات من القرن الماضي).

شهدت هذه المرحلة بروز العديد من الدراسات القانونية والمسحية التي تناولت جرائم الكمبيوتر حيث بدأ وصفها بأنها ظاهرة إجرامية قائمة بذاتها، وليست مجرد سلوكيات مرفوضة. [3] ومع تزايد استخدام الحواسيب مقارنة بالمرحلة السابقة، وانتشار الجريمة الإلكترونية بشكل أوسع، برزت صعوبات كبيرة في التعامل مع هذه الجرائم بسبب تعقيد البيئة المعلوماتية، مما جعل الحاجة ملحة إلى وضع تشريعات قانونية خاصة لمكافحتها. وقد بادرت العديد من الدول إلى سن قوانين تهدف إلى تنظيم استخدام الحواسيب ومعاقبة إساءة استخدامها ومن الأمثلة على ذلك:

- ❖ صدور أول قانون لحماية البيانات وحق الوصول إليها في الولايات المتحدة الأمريكية سنة 1970 تلاه صدور أول تشريع فيدرالي خاص بجرائم الحاسوب عام 1977.
- ❖ إصدار السويد لقانون المعطيات المعلوماتية سنة 1973، والذي يُعد من أوائل القوانين التي تناولت حماية البيانات الإلكترونية.[4]

[1] نجاة بن مكي ، **السياسة الجنائية لمكافحة جرائم المعلومات** ، دار الخلدونية للنشر والتوزيع، الجزائر،2017، ص15.

[2] عفاف يعون ونسيمة أولاد سالم، مرجع سبق ذكره، ص 73.

[3] ميرفت محمد حبابية، مرجع سبق ذكره، ص 28.

[4] فتيحة سويسي ،"**التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها**"، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية، مركز البحوث القانونية والقضائية، المنعقد في 18 جانفي 2020، ص04 ص05.

بعد هذه المرحلة، استمرت الجهود القانونية في سن تشريعات تهدف إلى الحد من تطور الجريمة الإلكترونية. ومع بداية الثمانينيات، تبلور مفهوم جديد لجرائم الكمبيوتر والإنترنت، ارتبط بعمليات اقتحام أنظمة الكمبيوتر عن بُعد، وبأنشطة نشر وزرع الفيروسات الإلكترونية التي تؤدي إلى تدمير كامل للملفات أو البرامج. كما شاع في هذه الفترة استخدام مصطلح " الهاكرز" للدلالة على مقتحمي الأنظمة، بالإضافة إلى ظهور مصطلح " المجرم المعلوماتي المتفوق".[1]

ثالثا: المرحلة الثالثة (تسعينيات القرن الماضي).

شهدت هذه المرحلة توسعًا ملحوظًا في نطاق الجرائم الإلكترونية وتغير في مفهومها، حيث أسهم انتشار الإنترنت بشكل كبير في تسهيل تنفيذ العمليات الإجرامية ومع تصاعد عمليات اختراق الأنظمة واقتحام شبكات المعلومات، ظهرت أنماط جديدة وخطيرة من الجرائم الإلكترونية، وقد تطورت شبكة الإنترنت خلال هذه الفترة بشكل مذهل، حيث تحولت من مجرد شبكة أكاديمية محدودة إلى بيئة متكاملة[2] ومتاحة للاستخدام العام. كما شملت الجرائم الإلكترونية في هذه المرحلة جرائم التجسس الصناعي والأمني، والاستيلاء على بطاقات الائتمان البنكية واستخدامها بطرق غير مشروعة، بالإضافة إلى الاعتداء على سمعة الأفراد والإساءة إليهم عبر الرسائل الإلكترونية.[3]

رابعا: المرحلة الرابعة (من الألفية الجديدة إلى العصر الحالي).

لقد شهدت هذه الفترة تطورات متسارعة، ترافقت مع الارتفاع الكبير في عدد مستخدمي الإنترنت مما أدى بطبيعة الحال إلى زيادة معدلات الجرائم الإلكترونية وتضخم الخسائر المالية الناتجة عنها.[4] وقد استمرت أساليب الجريمة الإلكترونية في التطور توازيًا مع التقدم التكنولوجي. وبعد الهجمات الإلكترونية الشهيرة التي استهدفت دولة إستونيا عام 2008، أدركت العديد من الدول خطورة هذه التهديدات التي

[1] لامية طالة، مرجع سبق ذكره، ص70.

[2] غنية عباس، "الجريمة الإلكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية"، **المجلة الجزائرية للسياسات العامة**، المجلد 12، العدد 03، ديسمبر 2024، ص 91.

[3] عفاف بعون، مرجع سبق ذكره، ص 73 .

[4] فارس محمد العمارات، "**جرائم العصر من الرقمية إلى السيبيرانية**،" الطبعة الأولى، دار الخليج للنشر والتوزيع، الأردن، 2023، ص 34.

تستهدف البنى التحتية للمعلومات وتقنية الاتصالات والشبكات وتعطل المرافق الحيوية مما دفعها إلى التفكير بجدية في وضع استراتيجيات متخصصة لتعزيز الأمن السيبراني.[1]

أما في وقتنا الحالي ومع الانتشار الواسع لتقنيات الذكاء الاصطناعي، الذي يُعد أحد فروع علم الحاسوب وإحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا الحديثة،[2] فقد أصبح يمثل ثورة حقيقية بفضل تطوره السريع. ومن خلال هذه التقنية باتت الجريمة الإلكترونية مرشحة لأن تتطور وتصبح أكثر خطورة. وفي مواجهة ذلك، تسعى الدول إلى مكافحة هذه الجرائم عبر أنظمة الذكاء الاصطناعي التي تُعد أدوات قوية وفعالة، إذ تعتمد على تحليل كميات ضخمة من البيانات واستخلاص أنماط ومعلومات مهمة، مما يمكنها من اكتشاف السلوكيات الاحتيالية وغير القانونية على الإنترنت.[3] ومن هنا يمكننا أن نستنتج أن المجتمع الدولي يبذل جهودًا كبيرة لجعل هذه التقنية أداة للحد من الجريمة الإلكترونية، وليس وسيلة لتطويرها وتعزيزها .

الفرع الثاني أنواع الجريمة الإلكترونية:

أسفر الانتشار الواسع للتقنيات الحديثة عن تنوع الجرائم الإلكترونية واختلاف أساليبها وأهدافها مما جعلها تشكل تهديداً مباشراً لأمن الأفراد والمؤسسات والدول على حد سواء، ونظراً لأهمية تصنيف هذه الجرائم وفهم أبعادها، يتناول هذا الفرع أبرز أنواع الجرائم الإلكترونية، والمتمثلة في: الجرائم الواقعة على الأشخاص، والجرائم الواقعة على الأموال، والجرائم الماسة بأمن الدولة واستقرارها.

أولا: الجرائم الإلكترونية الواقعة على الأموال.

شهد ظهور شبكة الإنترنت تطورات متسارعة أثرت على مختلف المجالات، حيث أصبحت غالبية المعاملات التجارية تُجرى عبر هذه الشبكة، مما أدى إلى تطور وسائل الدفع والوفاء[4]، وقد وفر هذا

[1] فارس العمارات ،مرجع سبق ذكره، ص 34.

[2] خليل سعيدي، بن مهدي، **"الذكاء الاصطناعي كتوجه حتمي في حماية الامن السيبيراني"، مجلة الدراسات في حقوق الإنسان،** المجلد 06، العدد 01، جوان 2022، ص27.

[3] صباح عادل الرواشدة، "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة ميدانية في الأردن"، **المجلة الأردنية في إدارة الأعمال**، المجلد 21، العدد 01، ديسمبر 2023.

[4] يوسف صغير، "**الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير القانون الدولي للأعمال**"، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013 ، ص 44.

التطور فرصاً جديدة للمجرمين لتنفيذ عمليات السطو بسهولة وتكلفة منخفضة، حيث أصبح بإمكانهم سرقة البنوك مثلاً من خلال الوصول إلى بيانات المتعاملين وتحويل الأموال من حساباتهم إلى حسابات أخرى، سواء بتحويلات مالية صغيرة متكررة لا تثير الشبهات أو بتحويل مبالغ كبيرة دفعة واحدة.[1]

كما ساعد الفضاء السيبراني من أكثر الأسباب التي تشجع على ممارسة القمار عبر الأنترنت، اذ يمنح للراغب في ممارسة القمار من خلال الكازينوهات الافتراضية الخصوصية وخفاء الشخصية التي يبحث عنها الكثيرون.[2]

ثانيا: الجرائم الإلكترونية الواقعة على الأشخاص.

حرص المشرع في مختلف الأنظمة القانونية على سن تشريعات تهدف إلى حماية الأشخاص من جميع أشكال الاعتداء، ومع ظهور الفضاء الإلكتروني أصبحت الحياة الخاصة للأفراد عرضة لخطر الانتهاك نتيجة سهولة السطو والاطلاع على معلوماتهم الشخصية.[3] وتتمثل هذه الجرائم في الاعتداء على شخصية المجني عليه أو تشويه سمعته من التهديد والمضايقة، جريمة سرقة الهوية، جريمة انتحال الشخصية، جرائم القذف وتشويه السمعة، ونشر المواد الإباحية. ويُعد من أخطر مظاهر هذه الاعتداءات سرقة المعلومات والبيانات الخاصة أين يستغل الجناة رسائل البريد الإلكتروني للإيقاع بالضحايا، ومن أشهر الجرائم المرتبطة بالبريد الإلكتروني: الغش، إرسال الفيروسات، وعمليات التهكير.[4]

ثالثا: الجرائم الإلكترونية التي تهدد أمن الدولة.

استغلت الجماعات المتطرفة الطبيعة الاتصالية لشبكة الإنترنت لبث معتقداتها وأفكارها، متجاوزة ذلك إلى ممارسات تمثل تهديداً مباشراً لأمن الدولة، لا سيما من خلال دعم الإرهاب والجريمة المنظمة.[5] وقد أنشأت هذه الجماعات مواقع إلكترونية لنشر الفتن والتفرقة بين أفراد المجتمع، عبر بث أفكار مكتوبة

---

[1] محمد رحموني، مرجع سبق ذكره، ص 447.

[2] يوسف صغير، مرجع سبق ذكره، ص 46 .

[3] محمد رحموني، مرجع سبق ذكره، ص 444.

[4] مراد محمد غالب محمد قاسم، "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية(دراسة مقارنة)"، **المجلة العصرية للدراسات القانونية**، جامعة تغر باليمن، المجلد2، العدد 2، جوان 2024، ص 101 .

[5] اسمهان بوضياف، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، العدد 11، ماي 2018 ، ص 358.

أو مسموعة أو مرئية تُثير الانقسامات السياسية والعقائدية والدينية، [1] كما سهّلت شبكة الإنترنت من تنفيذ الأعمال التجسسية، حيث تُستهدف الأشخاص والدول والمؤسسات الوطنية والدولية، وتركز عمليات التجسس الإلكتروني على ثلاثة مجالات رئيسية هي: التجسس العسكري، التجسس السياسي، والتجسس الاقتصادي.[2]

كما يبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الأنترنت، حيث تعطي الأنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى.[3]

المطلب الثالث: خصائص و أركان الجريمة الإلكترونية.

أصبحت الجريمة الإلكترونية من أبرز صور الإجرام المعاصر التي تستند على البيئة الرقمية، وقد أوجد هذا النمط من الجرائم تحديات قانونية وعملية متزايدة نظراً لخصوصيتها التي تميزها عن غيرها من الجرائم خاصة التقليدية منها، لأجل ذلك، يستوجب الوقوف عند أبرز خصائص الجريمة الإلكترونية ومن ثم تحديد الأركان القانونية التي تقوم عليها وفقاً للقواعد العامة في القانون الجنائي، وبناءً عليه سنتناول في هذا المطلب في فرعه الأول الخصائص الجوهرية للجريمة الإلكترونية، وفي فرعه الثاني الأركان الأساسية التي تقوم عليها.

الفرع الأول: خصائص الجريمة الإلكترونية.

تتميز الجريمة الإلكترونية بسمات فريدة تجعلها تختلف بشكل جوهري عن الجرائم التقليدية، سواء من حيث طبيعة الوسائل المستعملة أو البيئة الافتراضية التي تُرتكب فيها، أو من حيث نوعية الجناة الذين غالبًا ما يمتلكون مهارات تقنية متقدمة، ونظرًا لأثر هذه الخصائص في تعقيد هذه الجريمة وصعوبة اكتشافها أو مكافحتها، سنتناول في هذا الفرع أبرز خصائصها مع إبراز ما تفرضه من تحديات قانونية وتقنية في مواجهتها.

[1] يوسف خليل العفيفي، مرجع سبق ذكره، ص 28.

[2] يوسف الصغير، مرجع سبق ذكره، ص 57.

[3] اسمهان بوضياف، مرجع سبق ذكره، 358.

أولا: الجريمة الإلكترونية من الجرائم العابرة للحدود.

أدى الانتشار الواسع لشبكة الإنترنت إلى ربط العالم في فضاء واحد من خلال أجهزة الحاسوب والهواتف المحمولة المتصلة بالشبكة العنكبوتية.[1] وهو ما جعل الجريمة الإلكترونية تتسم بطابعها العابر للحدود، فقد ألغت هذه الجريمة الحدود الزمانية والمكانية، مما أتاح للجاني إمكانية ارتكاب أفعال إجرامية متعددة في دول مختلفة دون الحاجة إلى مغادرة مكانه.[2] وفي المقابل قد يتواجد المجني عليه في دولة مغايرة تمامًا لمكان ارتكاب الجريمة، كما قد يمتد الضرر الناتج عنها إلى دولة ثالثة أو أكثر، كما هو الحال في عمليات اختراق الأنظمة، أو إتلاف المواقع والأجهزة، أو سرقة البيانات والمعلومات وقد أسهم هذا الامتداد الواسع في تعقيد سبل التصدي للجريمة الإلكترونية[3]. أفرز هذا الواقع حاجةً ملحّة إلى تنظيم قانوني دولي فعّال، تدعمه تشريعات وطنية متناغمة لمواجهة هذا النوع من الجرائم وملاحقة مرتكبيها. ويُرجع ذلك إلى اختلاف التشريعات الداخلية بين الدول مما يثير إشكاليات متعددة، أبرزها ما يتعلق بتحديد الاختصاص القضائي وآليات الملاحقة والتعاون القضائي.[4]

ثانيا: الجريمة الإلكترونية تقع في بيئة افتراضية(بواسطة الأنترنت).

ترتكب الجريمة الإلكترونية ضمن بيئة افتراضية لا مادية، [5] حيث تتم عبر وسائط إلكترونية تعتمد أساسًا على استخدام الحاسوب وشبكة الإنترنت كوسيلة وأداة لتنفيذ الفعل الإجرامي، ويتميز هذا النوع من الجرائم عن غيره بارتباطه الوثيق بالجانب التقني، إذ يتطلب معرفة متقدمة بالجوانب الفنية الخاصة بالحاسوب والإنترنت، وكلما ازدادت خبرة الأفراد في هذا المجال، ارتفعت احتمالية توظيف هذه المعارف لأغراض غير مشروعة.[6] وتعد هذه الخاصية في ذاتها تحديًا حقيقيًا أمام الجهات المختصة

[1] مراد محمد غالب محمد قاسم، مرجع سبق ذكره، ص99 .

[2] إسماعيل بن يحيى، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2021، ص19.

[3] يوسف خليل العفيفي، مرجع سبق ذكره، ص15.

[4] عبد الله دغش العجمي، **المشكلات العلمية والقانونية للجرائم الإلكترونية(دراسة مقارنة)**، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ص 201.

[5] بن يحيى إسماعيل، مرجع سبق ذكره، ص19.

[6] يوسف خليل العفيفي، مرجع سبق ذكره، ص14.

بالتحري والتحقيق، حيث يصعب على المحقق التقليدي التعامل مع هذا النوع من الجرائم ومتابعتها والكشف عنها، فضلًا عن صعوبة إقامة الدليل الفني اللازم لإثباتها.[1]

ثالثا: صعوبة الكشف و اثبات الجريمة الإلكترونية.

تتسم الجريمة الإلكترونية بدرجة عالية من التعقيد، الأمر الذي يُعقّد من عملية اكتشافها، إذ غالبًا ما يُصادف كشفها عرضًا، وذلك بسبب امتلاك الجاني لمهارات تقنية متقدمة تمكّنه من محو أدلة الإدانة خلال فترة وجيزة. ويرجع ذلك إلى غياب الأدلة الجنائية التقليدية، كالبصمات مثلًا، مما يجعل هذا النوع من الجرائم غالبًا لا يخلّف آثارًا مادية واضحة بعد ارتكابه، فضلاً عن الصعوبة التقنية في الحفاظ على ما قد يتبقى من دلائل رقمية، إن وُجدت.[2]

رابعا: جريمة ناعمة .

تُعد الجريمة الإلكترونية من الجرائم غير العنيفة، فهي تمتاز بطابعها "الناعم" الذي لا يعتمد على القوة الجسدية أو استخدام العنف لأنها تستهدف الجوانب المعنوية وليس المادية، فقيام الجاني بنقل بيانات من حاسوب إلى آخر، أو الاستيلاء الإلكتروني على أرصدة مصرفية، لا يتطلب أي احتكاك مباشر أو مواجهة مع الضحية، كما لا يستلزم استخدام القوة أو السلاح. [3] يعتمد مرتكب هذا النوع من الجرائم أساسًا على قدراته العقلية، ومستوى إلمامه بالتقنيات الحديثة إلى جانب تمكنه من التعامل مع البرمجيات واستغلال شبكة الإنترنت بمهارة لتيسير ارتكاب أفعاله الإجرامية. [4]

خامسا: نوعية المجرم المنفذ للجريمة الإلكترونية.

يتمتع مرتكبو الجرائم الإلكترونية بسمات خاصة تميزهم عن مرتكبي الجرائم التقليدية، أبرزها ارتفاع مستواهم الثقافي وإلمامهم العميق بالتكنولوجيا. فالجريمة الإلكترونية، لاسيما تلك التي تستهدف سرقة البيانات المشفرة، تتطلب مهارات تقنية متقدمة وخبرة احترافية في التعامل مع نظم المعلومات.[5] كما يتصف المجرم الإلكتروني بدرجة عالية من الذكاء والقدرة على التخطيط المحكم، حيث يتمكن من وضع

[1] بوحزمة نصيرة، مرجع سبق ذكره، ص32.

[2] محمد رحموني، مرجع سبق ذكره، ص441.

[3] الطاهر ياكر، مرجع سبق ذكره، ص32.

[4] إسماعيل بن يحيى، مرجع سبق ذكره، ص20.

[5] عبد الحكيم مولاي براهيم ، مرجع سبق ذكره ، ص 214.

تصور شامل لجريمته بما يضمن إخفاء آثاره الإلكترونية وصعوبة تعقبه عبر الشبكات.[1] وتتنوع الدوافع التي تحركه بين اللهو والتحدي وإثبات التفوق على الأنظمة المعلوماتية، أو تحقيق مكاسب مالية، وأحيانًا بدافع الانتقام[2].

سادسا: الجريمة الإلكترونية جريمة ذات أضرار وخيمة.

تؤدي الجريمة الإلكترونية إلى أضرار كبيرة، سواء كانت معنوية تمس الحياة الشخصية للأفراد أو تؤثر في عنصر الثقة بين الأفراد والمؤسسات، أو كانت مادية تلحق بالمؤسسات المالية والاقتصادية، أو تمس قطاعات حيوية كالمؤسسات العسكرية، الصحية، أو الإعلامية. وتُعد هذه الأضرار في كثير من الحالات مرتفعة للغاية.[3] وقد كشفت شركة "إنتل سكيوريتي"، المتخصصة في أمن المعلومات، أن مؤسسات الأعمال حول العالم تتعرض لخسائر سنوية تقدر بنحو 400 مليار دولار أمريكي، كما أوضحت أن الهجمات الإلكترونية أصبحت تشكل اقتصادًا متناميًا بذاته، بقيمة تقدر ما بين 2 إلى 3 تريليون دولار سنويًا، وهو ما يمثل ما بين 15 إلى 20 بالمئة من القيمة الاقتصادية الناتجة عن الإنترنت.[4]

سابعا: نقص الخبرة الفنية لدى الأجهزة الأمنية أثناء مرحلة التحقيق والمتابعة وعدم كفاية القوانين السارية.

نظرًا للطبيعة التقنية للجريمة الإلكترونية، فإن التحقيق فيها يتطلب أن يكون المحققون وأعوان الضبط القضائي على درجة من التخصص، بما يسمح لهم بالتعامل مع هذا النوع من الجرائم بكفاءة ومهارة خلال مرحلتي البحث والتحري.[5] غير أن هذا الجانب لا يزال غير متوفر بالشكل المطلوب لدى العديد من الأجهزة الأمنية والقضائية، إذ أن التصدي لهذه الجرائم يقتضي متابعة مستمرة للتطورات التكنولوجية، ومعرفة دقيقة بالوسائل التقنية والإجرائية اللازمة، إضافة إلى ضرورة التدريب المستمر وتبادل الخبرات بين المتخصصين.[6] كما أن القوانين التقليدية لم تتمكن من مواكبة السرعة المتزايدة في

[1] محمد رحموني، مرجع سبق ذكره ، ص 443.

[2] المرجع نفسه، ص444.

[3] إسماعيل بن يحيى ، مرجع سبق ذكره ، ص 20.

[4] ياسمينة بونعارة، مرجع سبق ذكره ، ص 282.

[5] فتيحة سويسي، مرجع سبق ذكره ، ص 09.

[6] المرجع نفسه، ص 09.

تطور التكنولوجيا، وهو ما ساهم في تنامي هذه الجرائم وتعدد أشكالها، مما جعل تلك القوانين غير كافية لمواجهتها. وقد أصبح من الضروري تدخل المشرع لوضع نصوص قانونية حديثة تتماشى مع طبيعة هذه الجرائم، مع تعزيز مبدأ الشرعية الجنائية، وتشجيع التعاون بين الجهات القانونية والخبراء في مجال المعلوماتية، إلى جانب دعم التعاون الدولي لمكافحتها[1] .

ومن خلال الخصائص السالف ذكرها، يتبين أن الجريمة الإلكترونية ليست مجرد سلوك إجرامي بسيط، بل هي ظاهرة معقدة ترتبط ارتباطًا وثيقًا بالتطور التكنولوجي المتسارع، وتعتمد اعتمادًا كليًا على الوسائط الرقمية في التخطيط والتنفيذ. وتقوم هذه الجريمة على وجود طرفين رئيسيين:

1. **المجرم الالكتروني(الجاني):** قد يكون شخصًا طبيعيًا (فردًا) أو معنويًا كالمنظمات الإرهابية أو الأجهزة الاستخباراتية،[2] يتميز بامتلاكه خبرات تقنية متقدمة تمكّنه من تنفيذ أفعاله الإجرامية،[3] مع الحرص دائما على إخفاء هويته باستخدام برامج وتقنيات متقدمة، مما يُصعّب تعقبه والكشف عن هويته الحقيقية. [4]
2. **الضحية** : هو كل شخص طبيعي أو معنوي تعرض لضرر مادي أو معنوي نتيجة الاستعمال غير المشروع للتكنولوجيا الرقمية، [5] وقد يكون فردًا، أو مؤسسة مالية، أو جهة حكومية، بل وقد يمتد الضرر إلى قطاعات حساسة تمس السيادة الوطنية. [6]

كما يمكن تصنيف الجناة الإلكترونيين إلى خمس طوائف رئيسية تتمثل في:

- المخادعون **"Pranksters "**: يرتكبون أفعالهم بدافع التسلية والمزاح دون نية الإيذاء.
- القراصنة **"Hackers"**: يتسللون بدافع الفضول أو التحدي، وليس للتخريب الربح.
- القراصنة الخبيثون **"Crackers"**: يهدفون إلى التخريب وإحداث الأضرار دون مكاسب مادية.

---

[1] يوسف الصغير، مرجع سبق ذكره، ص20.

[2] نصيرة بوحزمة ، مرجع سبق ذكره، ص 38.

[3] لامية طالة، كهينة سلام، "الجريمة الإلكترونية : بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعية"، **مجلة الرواق للدراسات الاجتماعية والإنسانية**، العدد 02، ديسمبر 2020، ص 73.

[4] فتيحة سويسي، مرجع سبق ذكره، ص 11.

[5] نصيرة بوحزمة ، مرجع سبق ذكره، ص 51.

[6] فتيحة سويسي ، مرجع سبق ذكره، ص 11.

- أفراد يحلون مشكلة "**Personal Problem Solvers**": يسعون لحل مشاكلهم الشخصية، خاصة المالية.
- دعاة متطرفون"**Extreme Advocates**": يسعون لفرض معتقداتهم الأيديولوجية أو الدينية باستخدام الوسائل الإجرامية.[1]

الفرع الثاني: أركان الجريمة الإلكترونية.

تخضع الجريمة الإلكترونية من الناحية القانونية لنفس المبادئ العامة التي تحكم الجرائم التقليدية على الرغم من وقوعها بيئة افتراضية باستخدام وسائل رقمية، خاصة فيما يتعلق بوجوب توافر الأركان الأساسية لقيامها وهي الركن الشرعي، والركن المادي، والركن المعنوي، إذ لا يمكن مساءلة الفاعل جزائيًا ما لم تتحقق جميع هذه العناصر مجتمعة. وفي هذا الفرع، سنعرض هذه الأركان على التوالي، بدءًا بالركن الشرعي الذي يقتضي وجود نص قانوني يُجرم الفعل، ثم الركن المادي الذي يتجسد في السلوك الإجرامي ونتيجته، وأخيرًا الركن المعنوي الذي يعبّر عن القصد الجنائي لدى الفاعل.

أولا: الركن الشرعي.

بعد استيفاء الشرط الأساسي والافتراضي للجريمة المعلوماتية، المتمثل في نظام معالجة البيانات الآلي يظهر الركن القانوني لها والذي يمثل النموذج القانوني والصفة غير المشروعة للفعل. ويعتبر الركن القانوني هو السند القانوني لتجريم الفعل، تطبيقًا لمبدأ الشرعية الذي ينص على أنه: "**لا جريمة ولا عقوبة إلاّ بنص**". هذا يعني حصر جميع الجرائم والعقوبات في نصوص قانونية، بحيث لا يمكن توجيه اتهام لشخص ما بسبب فعل معين إلا إذا كان هناك نص قانوني يجرم هذا الفعل، كما أيضًا لا يمكن فرض أي عقوبة إلا إذا كانت منصوص عليها ومحددة مسبقًا في القانون، وبناءً على ذلك، فإنه من غير الممكن للقاضي الجزائي أن يجتهد أو يقيس العقوبات.[2]

حيث أورد المشرع الجزائري قسما خاصا للمساس بأنظمة المعالجة الآلية للمعطيات ، وهو القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر7 بمقتضى القانون رقم: 04-15 المؤرخ في

[1] ياسمينة بونعارة، مرجع سبق ذكره، ص 284 ص 285.

[2] إيمان بغدادي ، "أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية"، **مجلة آفاق للبحوث والدراسات**، 2019، ص 188.

10 نوفمبر 2004 ولم يكتف المشرع الجزائري لذلك فرض حماية جنائية على الحياة الخاصة لأفراد من خلال القانون رقم 23-06 المؤرخ في 20 ديسمبر 2006 والذي مس المادة 303 واقراره بالمادة 303 مكرر3 وهذا تصديا للاستخدام السيئ لوسائل التكنولوجيا الحديثة.[1]

ثانيا: الركن المادي.

يُشير الركن المادي للجريمة إلى وجود فعل خارجي قابل للملاحظة الحسية، ويتعلق بشكل خاص بالحادث الإجرامي الذي يشكل السلوك الخارجي المحظور قانونًا. أي أن كل ما يتضمن الجريمة وله طبيعة مادية يمكن لمسه بالحواس، وهو عنصر أساسي لوجودها، حيث لا يعتبر القانون جريمة دون وجود ركن مادي، ولذلك أطلق عليه البعض اسم "ماديات الجريمة".[2]

يتكون الركن المادي للجريمة الإلكترونية من: السلوك الإجرامي والنتيجة والعلاقة السببية، يجب الإشارة إلى أنه يمكن أن يتحقق الركن المادي بدون وجود النتيجة، مثل الإبلاغ عن الجريمة قبل ان تحدث نتيجتها على سبيل المثال، إنشاء موقع لتشويه سمعة شخص معين دون نشر الموقع على الشبكة وبالتالي لابد من معاقبة الفاعل.[3]

تستند الجريمة الإلكترونية على صورتين أساسيين ، الأولى تتمثل في الاعتداء على نظام المعالجة الآلية، ويتضمن هذا النوع نوعين من الاعتداءات: الأول وهو الدخول والبقاء غير المشروع في نظام المعالجة الآلية، والذي يشمل أفعال مثل الدخول والبقاء وعرقلة أو التعطيل. أما النوع الثاني فهو الاعتداء العمدي على نظام معالجة البيانات، ويتضمن أفعالا مثل الإدخال والحذف والتعديل. والثاني يتضمن اعتداءات على منتجات تكنولوجيا المعلومات، بما في ذلك التزوير المعلومات.[4]

---

[1] علي إبراهيم بن دراح، "**محاضرات في الجرائم المعلوماتية**"، موجهة لطلبة السنة الثانية ماستر، المركز الجامعي آفلو، 2021، ص 13.

[2] الطاهر ياكر، مرجع سبق ذكره، ص 39.

[3] إسمهان بوضياف، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، العدد 11، 2018، ص 354.

[4] ايمان بغدادي ، مرجع سبق ذكره، ص 189.

1. الاعتداءات على أنظمة المعالجة للمعطيات.

أ) الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

وفقًا للمادة 394 مكرر من قانون العقوبات، [1] نستنتج وجود نوعين من الأفعال المتعلقة بالدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات. الأول هو الفعل البسيط الذي يتضمن مجرد الدخول والبقاء غير المشروع في النظام، بينما الثاني هو الفعل المشدد الذي يتحقق عند توفر ظروف مشددة، وهي:

- ❖ حذف أو تغيير معطيات المنظومة بعد الدخول أو البقاء غير المشروعين.
- ❖ تخريب انظام أشغال المنظومة بعد الدحول أو البقاء غير المشروعين.[2]

ب) الاعتداءات العمدية على أنظمة المعالجة الآلية للمعطيات:

لم يورد المشرع الجزائري نصا خاصا بالاعتداء العمدي على سير النظام، بل اكتفى بالإشارة إلى الاعتداءات المتعمدة على المعلومات الموجودة داخل النظام، وهذا يعود إلى اعتقاد أن الاعتداء على المعطيات قد يؤثر على صلاحية. [3]

2. التزوير المعلوماتي.

الاعتداءات على منتجات تكنولوجيا المعلومات تُعتبر الفعل الثاني الذي يُحقق الركن المادي للجريمة الإلكترونية. فهي تُعَد من أخطر صور الغش المعلوماتي نظرًا لما يتمتع به الحاسوب من خطورة يُشار إلى أن المشرع الجزائري قد اقتدى بالنموذج الفرنسي، حيث خضع أفعال التزوير المعلوماتي للقوانين العامة الخاصة بالتزوير ومع ذلك، هناك اختلاف في نصوص العقوبات بين قانون العقوبات الجزائري

[1] القانون رقم: 09/01 المؤرخ في: 25 فيفري 2009، **المتضمن قانون العقوبات الجزائري**، ج.ر، العدد 15، ص 03.

[2] أحمد نوي ، فاطمة الزهرة قداوري ، مداخلة: **بعنوان رؤية قانونية للجريمة الإلكترونية وضوابط التصدي لها في القانون الجزائري**، في الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، ط الأولى، الولايات المتحدة الأمريكية، المركز المغاربي شرق أدنى للدراسات الاستراتيجية، جانفي 2024، ص 282.

[3] إيمان بغدادي مرجع سبق ذكره، ص 189.

والفرنسي وبناءً عليه، يجب إجراء تعديلات على نصوص التزوير التقليدية. إدراج نص خاص بالتزوير المعلوماتي في قانون العقوبات الجزائري. [1]

ثالثا: الركن المعنوي:

تعد الجرائم الإلكترونية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم والإرادة) لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود القصد الخاص في الجرائم الإلكترونية، فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع أو ارتكاب الجريمة.[2]

ونستدل بذلك على أن المشرع استعمل عبارات "الغش" "العمد" الإعداد للجريمة" في المواد المشار إليها أعلاه. وهذا دليل على أن الجريمة الإلكترونية جريمة عمدية قصدية. ومثال ذلك جريمة الاحتيال الإلكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الجاني. والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم بأنه يخالف القانون بسلوكه مع نيته لتحقيق ربح غير مشروع له ولغيره وتجريد شخص من ممتلكاته على نحو غير مشروع[3].

من المؤكد أن هناك علاقة وثيقة بين الركن المعنوي وأركان أخرى، حيث لا يمكن للركن المعنوي الوجود دون توفر الركن القانوني للجريمة. فالإرادة لا تُعتبر إجرامية إلا إذا كانت موجهة نحو ما يتطلب وجود الركن القانوني لها، مما يجعلها تتسم بصفة غير قانونية.[4]

نستنتج من خلال ما تم عرضه في هذا المبحث أن الجريمة الإلكترونية تُعد نمطًا إجراميًا مستحدثًا، يختلف جوهريًا عن الجريمة التقليدية من حيث البيئة التي تُرتكب فيها، والوسائل المستخدمة، وطبيعة الجناة والضحايا. فقد تبيّن من خلال التعريفات، والأسباب، ومراحل التطور، والأنواع، والخصائص، والأركان، أن الجريمة الإلكترونية لا تقتصر على استخدام الوسائل التقنية فحسب، بل تنشأ

[1] أحمد نوي، فاطمة الزهرة قداوري، مرجع سبق ذكره، ص 282.

[2] اسمهان بوضياف، مرجع سبق ذكره، ص 354.

[3] بريزة زدام ، سمية بن سماعين، "الجريمة الإلكترونية والآليات الدولية لمكافحتها"، **مجلة علمية دولية نصف سنوية**، المجلد 08 ، العدد 01، 2023، ص 367.

[4] الطاهر ياكر، مرجع سابق الذكر، ص43.

داخل فضاء سيبراني معقّد يتطلب استجابات قانونية وتقنية متخصصة. وتُبرز هذه الفروقات الحاجة إلى فهم دقيق لطبيعتها وتمييزها عن الجريمة التقليدية، كما هو موضّح في الجدول الآتي:

الجدول رقم (01): مقارنة بين الجريمة الالكترونية والجريمة التقليدية.

وجه المقارنة	الجريمة الإلكترونية	الجريمة التقليدية
بيئة ارتكاب الجريمة	الفضاء الرقمي (الإنترنت ، الأجهزة الذكية..).	الواقع المادي (الشارع، المنزل ..).
الأداة المستخدمة	الوسائل التكنولوجية (أجهزة، برامج، شبكات).	أدوات مادية أو جسدية (سلاح، أدوات حادة ..).
النطاق الجغرافي	عابرة للحدود الجغرافية بسهولة.	غالبًا ما تكون محلية ومحددة بمكان معين.
سهولة الكشف	صعبة الكشف والتتبع بسبب التمويه والتشفير.	أسهل نسبيًا في الكشف والتحقيق.
طبيعة الجاني	يتطلب مهارات تقنية عالية وخبرة رقمية.	لا يتطلب مهارات خاصة، وقد يُرتكب من أي شخص.
وسائل الإثبات	تعتمد على أدلة رقمية وتقنيات تحقيق رقمية معقدة.	تعتمد على أدلة مادية (شهود بصمات..).
نوع الأثر أو الضرر	قد يكون معنويًا أو ماليًا دون آثار جسدية مباشرة.	غالبًا ما يُحدث أضرارًا مادية أو جسدية مباشرة.

المصدر: من اعداد الطالبتين بتصرف.

المبحث الثاني: ماهية الأمن السيبراني وعلاقته بالجريمة الإلكترونية.

برز مفهوم **الأمن السيبراني** كأحد الركائز الأساسية لحماية الأنظمة والمعلومات من التهديدات المتنامية خاصة بعد وتزايد اعتماد الأفراد والمؤسسات على الشبكات الإلكترونية في مختلف مجالات الحياة، ويُعنى الأمن السيبراني بوضع آليات تقنية وتنظيمية تهدف إلى تأمين الفضاء المعلوماتي وضمان استقراره، باعتباره عنصرًا استراتيجيًا في الحفاظ على الأمن الوطني والسيادة الرقمية.

ونظرًا لأهمية هذا الموضوع، يُخصص هذا المبحث لتوضيح المفهوم العام للأمن السيبراني، مع خلال ثلاث مطالب، يعالج **المطلب الأول** ببيان الإطار المفاهيمي للأمن السيبراني مع استعراض أبرز أبعاده التقنية والقانونية والاستراتيجية؛ أما **المطلب الثاني**، يتطرق إلى مراحل تطور الأمن السيبراني مسلطًا الضوء على العوامل التي أسهمت في تعزيز مكانته في ظل تصاعد الهجمات الرقمية؛ في حين يتناول **المطلب الثالث** العلاقة بين الأمن السيبراني والجريمة الإلكترونية، من خلال تحليل أوجه الترابط والتأثير المتبادل بينهما، إلى جانب استعراض أبرز الجهود الدولية المبذولة في هذا المجال.

المطلب الأول: مفهوم الأمن السيبراني وأبعاده.

يحتل مفهوم الأمن السيبراني مكانة مركزية في السياسات الأمنية للدول، نظرًا لتزايد المخاطر المرتبطة بالهجمات الإلكترونية وما تسببه من أضرار تمس الأفراد والمؤسسات وسيادة الدول. ونظرًا لتعدد استخداماته وارتباطه بمختلف القطاعات، تباينت التعريفات المتعلقة بالأمن السيبراني من حيث النطاق والمضمون.

كما اتخذ هذا المفهوم أبعادًا مختلفة تتجاوز الجوانب التقنية لتشمل أبعادًا سياسية واقتصادية واجتماعية، وعليه سنتناول في هذا المطلب، من خلال **الفرع الأول** مفهوم الأمن السيبراني بالاستناد إلى أبرز التعريفات الواردة في الأدبيات المتخصصة والتشريعات المقارنة، في حين نَخصص **الفرع الثاني** لبيان الأبعاد المختلفة لهذا المفهوم ومدى تداخله مع قضايا السيادة الوطنية والأمن القوم.

الفرع الأول: تعريف الأمن السيبراني.

مع تزايد الاعتماد على الفضاء الرقمي في مختلف مجالات الحياة، برز مفهوم الأمن السيبراني كعنصر أساسي في حماية الأفراد والمؤسسات والدول من التهديدات والمخاطر المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات. وقد تعددت المقاربات المفاهيمية لهذا المصطلح نظرًا لتداخله مع

مجالات تقنية وقانونية وأمنية، مما يجعل من الضروري الوقوف على معانيه اللغوية وأصوله الاصطلاحية، واستعراض أبرز التعريفات التي قدمتها الأدبيات الفقهية والدولية. ومن هذا المنطلق سنخصص هذا الفرع لبيان مفهوم الأمن السيبراني، من خلال تناول تعريفه اللغوي، وأصل مصطلح "السيبرانية"، والتعريفات الاصطلاحية المتداولة له في الأوساط الأكاديمية والرسمية.

أولا: التعريف اللغوي.

يتكون الأمن السيبراني من كلمتين:" الأمن"، و" السيبرانية".

1. **الأمن:** هو نقيض الخوف، أي بمعنى السلام، والأمن مصدر الفعل أَمِنَ من الشر، أي سَلِمَ منه وقد عرفه قاموس بنغوين للعلاقات الدولية بأنه:" **مصطلح يشير إلى غياب ما يهدد القيم النادرة** ".[1]

2. **السيبرانية:** مصطلح "السيبراني" من أكثر المفاهيم تداولًا في ميدان الأمن الدولي اليوم، وأصل الكلمة **"Cyber"** يوناني، مأخوذ من **"Kybernetes"** بمعنى من يدير دفة السفينة، واستخدمت مجازًا للدلالة على المتحكم. ويرى بعض المؤرخين أن عالم الرياضيات الأمريكي نوربرت وينر هو من أعاد إحياء المصطلح ليعبّر عن التحكم الآلي، ويُعتبر المؤسس للسبرنتيقية من خلال كتابه الشهير:

"Cybernetics or Control and Communication in The Animal and Machine" .[2]

حيث عرف نوربرت وينر **"Norbert Wieners "** السبرنتيقية **"Cybernetics "** "**التحكم والتواصل عند الحيوان والآلة** ".[3]

[1] فارس محمد العمارات، "**الأمن السيبراني مفهوم وتحديات العصر**"، ط الأولى، دار الخليج للنشر والتوزيع، الأردن– عمان، 2022، ص 13.

[2] فرح يحي زعاترة، مرجع سبق ذكره، ص 21.

[3] Neittaanmaki Pekka, Lehto Martti**, " Cyber Security : Analytics, Technology and Automation** ", Spnger international Publishing, volume 78, Inteellingent System, control and Automation Science and Enerineering, Switzerland, 2015, p 3.

ثالثا: التعريف الاصطلاحي.

هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يُعرف على بأنه" **مجموعة من الاجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة"**[1].

وهذا ما ذهب إليه الكاتبان **"Neittaanmaki Pekka, Lehto Martti"** في كتابهما **"Cyber Security : Analytics, Technology and Automation "**، حيث عرفا الأمن السيبراني بأنه:" **عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكومبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة**".[2]

عرّف التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في عام 2011-2010 الأمن السيبراني بأنه:" **مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسة فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين**".[3]

وقدمت وزارة الدفاع الأمريكية " البنتاغون " تعريفا دقيقا لمصطلح الأمن السيبراني فاعتبرته" **جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس، والحوادث**".[4]

نظراً للطابع الشامل لمفهوم الأمن السيبراني، فإن فهمه يستدعي التطرق إلى مجموعة من المفاهيم المتداخلة التي تُشكل أبعاده أو أدواته الأساسية، والتي تتكامل فيما بينها لضمان حماية الفضاء الرقمي.

---

[1] مني عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**، جامعة المنصورة، العدد 111، يوليو 2020، ص 9.

[2] Neittaanmaki Pekka, Lehto Martti ,Ibid ,p 25.

[3] راشد محمد المري،" الأمن السيبراني وحماية الأنظمة الإلكترونية (دراسة تحليلية تأصيلية)"، **مجلة الدراسات القانونية والاقتصادية**، المجلد 09، العدد 01، مارس 2023، ص 964.

[4] فرح يحي زعاترة، مرجع سبق ذكره، ص 22.

- **القوة السيبرانية** :تعبر عن قدرة الدولة أو الجهات الفاعلة على التحكم في المعلومات والبنى التحتية الرقمية من خلال موارد تقنية وبشرية متخصصة[1].
- **الدفاع السيبراني** :يتمثل في حماية الأنظمة الرقمية من خلال رصد التهديدات وتحليلها والتقليل من آثارها، مع القدرة على الرد في الوقت المناسب[2].
- **الردع السيبراني** :يهدف إلى منع الهجمات الإلكترونية عبر إظهار القدرة على الرد أو المعاقبة مما يشكل وسيلة ردع استراتيجية للخصوم[3].
- **الهجمات السيبرانية** :أفعال ضارة تستغل ثغرات رقمية لتعطيل أو التلاعب بالأنظمة، غالبًا لتحقيق أهداف سياسية أو شخصية[4].
- **الفضاء السيبراني** :عرفته الوكالة الفرنسية لأمن أنظمة الإعلام **"ANSSI"**، بأنه:" **فضاء تواصلي ناشئ عن الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"**[5].
- **أمن المعلومات** :يشير إلى الإجراءات والتقنيات المعتمدة لحماية المعلومات من الضياع أو التسريب أو التلاعب، ويُعد أحد مكونات الأمن السيبراني[6].

---

[1] تغريد صفاء مهدي، لبنى خميس مهدي، "أثر السيبرانية في تطور القوة"، **مجلة حمورابي للدراسات**، مركز حمورابي للبحوث والدراسات الاستراتيجية، العددان 33–34 السنة الثامنة (شتاء–ربيع)، 2020، ص 152.

[2] إيهاب خليفة، **الحرب السيبرانية (الاستعداد لقيادة المعارك العسكرية في الميدان الخامس)**، العربي للنشر والتوزيع، الطبعة الأولى، القاهرة، 2020، ص 188.

[3] وفاء مطروح، ابتسام أونيس، تداعيات جائحة كوفيد–19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر، **المجلة الدولية للاتصال الاجتماعي**، المجلد 09، العدد02 ، ص 222.

[4] المرجع نفسه، ص 223.

[5] Agence nationale de la sécurité des systèmes d'information (ANSSI)," **CyberDico de l'ANSSI (FR/EN)**", Gouvernement français, 2020, disponible sur : https://www.info.gouv.fr/upload/media/content/0001/11/a5fcaf7ccf1f6058d70e3a17570037569b979d84.pdf , consulté le 26 avril 2025 à 16h12.

[6] حياة حميدي، نسيمة طايلب، "مدخل مفاهيمي حول الأمن السيبراني"، **مجلة مدار للدراسات الاتصالية الرقمية**، المجلد 02، العدد 02، نوفمبر 2022، ص 07.

الفرع الثاني: أبعاد الأمن السيبراني.

في ظل التحول الرقمي المتسارع أصبح الأمن السيبراني مكوّنًا محوريًا من مكونات الأمن القومي نظرًا لاتساع نطاق تأثيره ليشمل الأبعاد السياسية والعسكرية والاقتصادية والاجتماعية والقانونية. توضح هذه الأبعاد أهمية التهديدات السيبرانية وانعكاساتها المباشرة على استقرار الدول وأمنها، وعليه سنتطرق في هذا الفرع الى أبرز الأبعاد المتصلة بالأمن السيبراني، والمتمثلة في ما يلي:

أولا: البعد السياسي:

يشكل الأمن السيبيراني حجر الأساس في الحياة السياسية، حيث أصبح أداة استراتيجية تؤثر على أمن واستقرار الدول، فهناك العديد من الامثلة التي تدفع نحو الاهتمام بالبعد السياسي للأمن السيبيراني كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جداً على المستوى الدولي كما أنه لا ينكر الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية تظاهرات افتراضية، حركات احتجاجية إلكترونية).[1]

ومن هذا المنطلق، يتضح أن تجسيد الأمن السيبراني كوسيلة فعّالة لحماية المعلومات والوثائق الحساسة التي ترتبط بعمل مؤسسات الدولة بات ضرورة ملحّة، إذ إن غياب هذا الأمن قد يؤدي إلى نشوء خلافات دبلوماسية بين الدول قد تصل إلى مرحلة النزاعات، وقد شهدت العلاقات الدولية في السنوات الأخيرة تجليات واضحة لهذا الخطر من أبرزها الحرب الروسية الأوكرانية عام 2022 والتي بدأت بهجمات سيبرانية استهدفت البنى التحتية الحيوية قبل أن تتصاعد إلى حرب فعلية مدمّرة. [2]

ثانيا: البعد العسكري:

تجلّت البدايات الأولى للإنترنت في بيئة عسكرية لتنتقل لاحقًا إلى الأوساط الأكاديمية والعلمية ومختلف القطاعات. وقد برز البعد العسكري من خلال قدرة الفضاء السيبراني على ربط الوحدات

[1] سمير بارة، "الأمن السيبيراني(cyber Security) في الجزائر: السياسات والمؤسسات"، **المجلة الجزائرية للأمن الإنساني**، المجلد 02، العدد 02، جويلية 2017، ص 263.

[2] جيلالي شويرب، فائزة مراد ، مرجع سبق ذكره، ص167.

العسكرية وتسهيل عملية تبادل المعلومات[1] فيما بينها سعيًا لبلوغ الغايات المرجوة. وفّر الأمن السيبراني للقوات العسكرية إمكانية التواصل وتبادل المعلومات والأوامر عن بُعد بشكل آمن، مع القدرة على صدّ محاولات الاختراق التي قد تستهدف تدمير البيانات العسكرية الحساسة، مما يشكّل تهديدًا مباشرًا للأمن القومي، كما تجلّى ذلك في حالة اختراق المنشآت النووية الإيرانية. [2]

ثالثا: البعد الاقتصادي:

يرتبط الأمن السيبراني ارتباطًا وثيقًا بحماية المصالح الاقتصادية للدول، في ظل العلاقة المتزايدة بين الاقتصاد والمعرفة، حيث تعتمد غالبية الدول على إنتاج وتداول المعلومات كمحرّك رئيسي للنمو الاقتصادي. وهو ما يفسر الأهمية البالغة للأمن السيبراني في حماية الأصول الاقتصادية من الاختراق والسرقة.[3]

ومع دخول العالم عصر المال الإلكتروني المرتبط بالبنى التحتية التقنية، ولا سيما مع التوسع في استخدام المحافظ الإلكترونية، اتجهت المؤسسات المالية والبنوك إلى الاستثمار المكثف في هذا المجال مما أدى إلى نمو ملحوظ في الخدمات المالية الرقمية. وهو ما يستدعي من الدول تعزيز معايير الأمن السيبراني، ووضع استراتيجيات شاملة لمواجهة التهديدات الإلكترونية المنظمة التي تستهدف هذا القطاع الحيوي.

رابعا: البعد الاجتماعي:

مع تزايد تواصل الأفراد عبر المدونات والبريد الإلكتروني ومواقع التواصل الاجتماعي، تشكّل ما يُعرف بجمهور العالم الافتراضي، وهو ما يفرض ضرورة تأمين الشبكات والمنصات، [4] خاصة وأن هذه الوسائط باتت تُهدد القيم الأخلاقية للمجتمع وتُعرض أمنه واستقراره للخطر، مما يستوجب ترسيخ ثقافة الأمن السيبراني وتوعية الأفراد بخطورة اختراقه.

---

[1] وفاء مطروح ، ابتسام أونيس، مرجع سابق، ص 228.

[2] جيلالي شويرب ، فائزة مراد ، مرجع سبق ذكره، ص 166.

[3] مني عبد الله السمحان، مرجع سبق ذكره، ص 15.

[4] خالد ظاهر عبد الله جابر السهيل المطيري، "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، **مجلة البحوث الفقهية والقانونية**، العدد 38، يوليو2022 ، ص 1007 ص 1008.

خامسا: البعد القانوني.

ارتبط نشوء المجتمعات المعلوماتية بظهور منظومة قانونية جديدة تُشكّل الإطار التنظيمي اللازم لحمايتها، من خلال سنّ تشريعات تُعنى بصون الحقوق الرقمية، وتنظيم التعاملات الإلكترونية، بما يضمن حماية هذا المجتمع المعلوماتي، ويساعد على تطبيق وإنفاذ تلك التشريعات بفعالية.[1]

ومن أبرز الممارسات القانونية في مجال الأمن السيبراني، السعي إلى ضمان عدد من الحقوق الأساسية، من بينها الحق في النفاذ إلى الشبكات المعلوماتية، إلى جانب الحقوق المستحدثة في سياق تطور تقنيات المعلومات والاتصالات، مثل الحق في إنشاء المدونات الإلكترونية، والحق في ملكية البرامج ذات الطابع الثقافي أو القضائي.[2]

المطلب الثاني: مراحل تطور الأمن السيبراني وأهميته.

مع تنامي الاعتماد على التكنولوجيا الرقمية في مختلف جوانب الحياة، أصبحت الحاجة إلى حماية الفضاء السيبراني أكثر إلحاحًا من أي وقت مضى. فالأمن السيبراني لم يعد مسألة تقنية فحسب بل تحول إلى عنصر حاسم في حماية المصالح الوطنية، وضمان استمرارية النشاطات الحيوية سواء على مستوى الأفراد أو المؤسسات أو الدول.

وقد عرف هذا المجال تطورًا تدريجيًا عبر مراحل متلاحقة فرضتها طبيعة التهديدات المتغيرة والتقدم التكنولوجي المستمر ولفهم الإطار العام للأمن السيبراني، سنتناول في هذا المطلب في الفرع الأول مراحل تطور الأمن السيبراني، مع الوقوف عند أبرز المحطات التي ساهمت في تشكيله. أما في الفرع الثاني أهمية الأمن السيبراني في العصر الحديث، والدور المحوري الذي يلعبه في حماية البيانات والمصالح الاستراتيجية للدول.

الفرع الأول: مراحل تطور الأمن السيبراني.

شهد مفهوم الأمن السيبراني تطورًا تدريجيًا فرضته التحولات المتسارعة في مجال التكنولوجيا الرقمية، حيث انتقل من كونه أداة تُستخدم في الإطار العسكري إلى أن أصبح أحد الركائز الأساسية في حماية المعلومات والبنى التحتية الحيوية في شتى القطاعات. وقد مرّ هذا المفهوم بعدة مراحل تاريخية

[1] وفاء مطروح، ابتسام أونيس، مرجع سبق ذكره، ص 228 .

[2] خالد ظاهر عبد اله جابر السهيل المطري، مرجع سبق ذكره، ص 1009.

تميزت كل منها بطبيعة خاصة للتهديدات الإلكترونية وتطور ملحوظ في أدوات وأساليب المواجهة. وفي هذا الفرع، سنتناول أبرز المراحل التي مر بها تطور الأمن السيبراني، مع التوقف عند العوامل التقنية والسياسية التي ساهمت في بلورة ملامحه الحالية.

تعود البدايات الأولى للأمن السيبراني إلى أوائل سبعينيات القرن الماضي، مع أولى محاولات الولوج غير المشروع إلى شبكات الحاسوب، فقد تم خلال تلك الفترة اكتشاف أول فيروس إلكتروني عرف باسم كريبر **"Creepe"**، الذي كان قادرًا على الانتقال عبر شبكة**"ARPANET "** ، تلاه بظهور فيروس مضاد له يسمى ريبر **"Reaper"**، وهو من أوائل البرامج في مجال مكافحة البرمجيات الخبيثة، [1] أما عام 1983 قام معهد ماساتشوستس للتقنية بتطوير نظام اتصالات يعتمد على التشفير والذي أصبح حجر الأساس لتطور تقنيات الأمن السيبراني الحديثة. شكل ظهور الإنترنت ثورة نوعية في حياة البشرية، حيث تم استخدامه لأول مرة في المجالين الأمني والعسكري. ومع بداية تسعينيات القرن العشرين، بدأت الدول في السباق لتطوير التكنولوجيا، مما أدى إلى تسميتها بـ"الحرب السيبرانية الباردة " أو "سباق التسلح السيبراني". وقد ظهرت حينها هجمات التصيد الاحتيالية **"Phishing"** والتجسس الإلكتروني والهجوم الموزع لحجب الخدمة **"DDoS"**. كما برزت الحاجة عالميًا لوجود قوة غير مادية بجانب القدرات العسكرية والاقتصادية، مما دفع الدول للاهتمام بالقوة السيبرانية وتأثيرها على المستويين المحلي والدول.[2]

مع حلول العقد الأول من القرن الحادي والعشرين، تزايدت وتنوعت التهديدات والهجمات الإلكترونية بشكل كبير، حيث بدأت العديد من الجماعات الإجرامية في تنفيذ عمليات احترافية مستخدمة تقنيات متقدمة. هذا الوضع دفع الكثير من الحكومات والدول إلى اتخاذ تدابير متعددة بهدف تشديد الخناق على هذه الكيانات. وتضمن ذلك عدة خطوات مثل؛ سن قوانين خاصة بهذا النوع من الجرائم إصدار أحكام

[1] Anurag Lal, "**The Evolution Of Cybersecurity And How Businesses Can prepare For The Future**",Forbes ", Idonet, 14 Aug 2023, availablei at : https://www.forbes.com/councils/forbesbusinesscouncil/2023/08/14/the-evolution-of-cybersecurity-and-how-businesses-can-prepare-for-the-future/, accesed in : 21 Apr 2025 ,at : 00:15.

[2] " **الأمن السيبراني مفهومة وتاريخه**"، الجزيرة نت، الرابط: https://www.aljazeera.net/encyclopedia/2024/9/19/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%85%D9%81%D9%87%D9%88%D9%85%D9%87-%D9%88%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE%D9%87. أطلع عليه بتاريخ :21 أفريل 2025، الساعة 00:30.

جنائية على الجناة، تحسين أمن وحماية المعلومات والبيانات على الإنترنت. رغم ذلك، لا تزال العديد من الأطراف تنتج أنواع مختلفة من الفيروسات بهدف اختراق هذا الأمن[1].

وفي ظل الوقت الراهن شهد مفهوم الأمن السيبراني تقدماً كبيراً نتيجة للتطور التكنولوجي السريع خاصة مع دمج تقنيات الذكاء الاصطناعي في نظم الحماية. تعد هذه التقنيات أداة فعالة لتحليل البيانات الكبيرة واكتشاف الأنماط والتهديدات الجديدة بطريقة تفوق القدرات البشرية التقليدية. تتمتع الأنظمة الذكية بقدرتها على التعلم من التجارب السابقة، مما يعزز قدرتها على توقع المخاطر والتعامل معها بكفاءة أعلى، وهذا ساهم في رفع مستوى الأمن السيبراني وتقليل احتمال وقوع انتهاكات.[2]

الفرع الثاني: أهمية الأمن السيبراني.

أصبح الأمن السيبراني ضرورة استراتيجية تمس الأفراد والمؤسسات والدول على حد سواء، نظرًا لتزايد الهجمات السيبرانية التي تستهدف الخصوصية وسلامة المعلومات واستمرارية الخدمات. وتُبنى أهمية الأمن السيبراني على ثلاث ركائز أساسية، تتمثل في : **السرية** "**confidentialité**" وتعني حصر الوصول إلى البيانات على المصرح لهم فقط ، ثم **السلامة** "**Intégrité**": وهي الحفاظ على البيانات من التلاعب أو السرقة. وأخيرا **الجاهزية** "**availability**": وتعني ضمان توفر الأنظمة والخدمات عند الحاجة إليها من قبل المستخدمين المصرح لهم، [3] وفي هذا الإطار، سنتناول في هذا الفرع أهمية الأمن السيبراني، والتي يمكن تلخيصها في ما يلي:

1. الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.

---

[1] **تاريخ الأمن السيبراني**، موضوع، الرابط:
https://mawdoo3.com/%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE_%D8%A7%D9%84%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A#google_vignette ، أطلع عليه بتاريخ 23 أفريل 2025، الساعة 00:50.

[2] Courtny Goodman, "**AI in Cybersecurity : Transforming Threat Detection and Prevention**", BalbixIdonet, Jan 16 2025, availablei at : https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ ,accesed in : 21 Apr 2025 ,at : :0315.

[3] وفاء مطروح، ابتسام أونيس، مرجع سبق ذكره، ص 224.

2. توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.[1]
3. ضمان استمرارية عمل المؤسسات المؤمنة ونجنب تعطيل مصالحها المتصلة باستخدام شبكة الأنترنت، مع تقليل وقت التوقف عن الخدمات الرقمية الحساسة منها. [2]
4. يساهم في تعزيز إنتاجية المؤسسات والأفراد من خلال فحص الفيروسات، وتفعيل جدران الحماية والقيام بالنسخ الاحتياطية بالإضافة إلى توعية المستخدمين بمخاطر الاحتيال عن طريق البريد الإلكتروني والروابط المشبوهة.
5. الأمن السيبيراني هو نظام إلكتروني يحمي الأجهزة الإلكترونية ويمنع أي مخاطر على مستخدمي الفضاء السيبيراني.
6. استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
7. تحسين مستوى حماية المعلومات وضمان استمرارية الاعمال.[3]
8. الأمن السيبيراني يحافظ، على أمن المجتمع واستقراره.
9. الحفاظ على سلامة عمل قطاعات الدولة الإلكترونية من أي اختراق. [4]

من خلال ما سبق ذكره، يمكن القول بأن أهمية الأمن السيبيراني لا تقتصر على حماية البيانات والمعلومات فحسب، بل تمتد إلى الحفاظ على أمن واستقرار المجتمعات والدول. كما يبرز الدور المهم للأمن السيبيراني خصوصا في مواجهة الجرائم الإلكترونية.

المطلب الثالث: علاقة الأمن السيبراني بالجريمة الإلكترونية.

أدى الانتشار الواسع للتكنولوجيا الرقمية وتطور الفضاء السيبراني إلى خلق بيئة خصبة لنمو الجريمة الإلكترونية التي لم تعد تقتصر على أفعال فردية معزولة، بل باتت تمثّل تهديدًا حقيقيًا للأمن السيبراني على المستويين المحلي والدولي، فقد أضحت الهجمات الإلكترونية أداة تُستخدم لزعزعة

[1] مني عبد الله السحمان، مرجع سبق ذكره، ص 12.

[2] حياة حميدي، نسيمة طايلب، مرجع سبق ذكره، ص 101

[3] وفاء مطروح، ابتسام أونيس، مرجع سبق ذكره، ص 224.

[4] جيلالي شويرب، فائزة مراد، مرجع سبق ذكره، ص 165.

الاستقرار واستهداف البنى التحتية الحيوية والتأثير على السيادة الرقمية للدول. وبالنظر إلى تعقّد هذا التهديد، أصبح من الضروري تحليل العلاقة القائمة بين الجريمة الإلكترونية والأمن السيبراني، من حيث التأثيرات المباشرة وغير المباشرة، وأيضًا من حيث جهود المواجهة والتصدي على الصعيد الدولي.

ولفهم أبعاد هذه العلاقة بشكل أعمق، سنتناول في هذا المطلب تأثير الجريمة الإلكترونية على الأمن السيبراني في **الفرع لأول**، بينما يركز **الفرع الثاني** على الجهود الدولية المبذولة لمكافحة الجريمة الإلكترونية وتعزيز الأمن السيبراني.

الفرع الأول: تأثير الجريمة الإلكترونية على الأمن السيبراني.

تمثل الجريمة الإلكترونية اليوم أحد أبرز التهديدات التي تُواجه الأمن السيبراني، نظراً لتعدد أشكالها واتساع نطاق تأثيرها على مختلف المستويات. فهي تستهدف الخصوصية وتؤدي إلى خسائر اقتصادية جسيمة، كما تمس البنية التحتية الحيوية وتشجع على التجسس ونشر الدعاية المتطرفة. وبناءً عليه سنتناول في هذا الفرع أبرز أوجه تأثير الجريمة الإلكترونية على الأمن السيبراني، بمختلف مستوياته الفردية والاقتصادية والدولية.

1. التأثير على الأفراد.

يمثّل الأثر المباشر للجريمة الإلكترونية على الأفراد أحد أخطر جوانب هذا النوع من الجرائم، إذ تستهدف المعتدين الرقميين الحياة الخاصة للضحايا بوسائل متنوعة، كسرقة البيانات الشخصية، وانتحال الهوية، والتشهير، والابتزاز. وتنبع هذه الاعتداءات من دوافع مختلفة، منها الطمع أو الانتقام، وقد تكون أحيانًا بدافع التسلية أو الفضول. وتنعكس هذه الممارسات سلبًا على الأفراد من الناحية النفسية والاجتماعية والمالية، حيث تؤدي إلى اضطرابات في العلاقات الأسرية، وتفكك الثقة داخل المجتمع فضلاً عن التسبب في خسائر مادية جسيمة.[1]

وقد تجلّى خطر الجريمة الإلكترونية بوضوح مع بداية سنة 2020 مع ظهور جائحة كورونا حيث استغل مجرمو الفضاء السيبراني حالة القلق والارتباك الصحي العالمي لشنّ موجة واسعة من هجمات التصيّد الإلكتروني مستهدفين الأفراد من خلال رسائل بريد إلكتروني خادعة، ومثال ذلك أنه تم إرسال

[1] فتيحة حيمر، "تأثير الجريمة الإلكترونية على الأمن في إفريقيا"، **مجلة أبحاث قانونية وسياسية**، المجلد 09، العدد 01، جوان 2024 ، ص 562.

رسائل إلى مواطنين في إيطاليا تزعم احتواءها على قائمة بأدوية لعلاج الفيروس، بينما كانت تلك المرفقات تحتوي على برمجيات خبيثة تؤدي إلى اختراق أجهزة الحواسيب وسرقة البيانات.[1] ويعكس هذا المثال كيف يمكن استغلال الأزمات الصحية لتوسيع نطاق الهجمات الإلكترونية على الأفراد، مما يشكّل تهديدًا مباشرًا لأمنهم السيبراني.

2. التأثير الاقتصادي.

نظرًا لتعدد صور الجريمة الإلكترونية، فقد أصبحت هذه الأخيرة تشكّل تهديدًا حقيقيًا على مختلف المستويات والمجالات، مما يؤدي بالضرورة إلى انعكاسات سلبية مباشرة تمسّ الأمن السيبراني. ومع تطور أدوات وأساليب الإجرام الرقمي، بات المجرمون يوظفون تقنيات متقدمة في سرقة المعلومات وتزويرها، كاستنساخ المطبوعات، والملفات الصوتية، والبرمجيات المستخدمة في أنظمة الحاسوب، ليقوموا لاحقًا بإعادة توزيعها وبيعها بأسعار زهيدة مقارنة بالسعر الأصلي، في انتهاك صارخ لحقوق المؤلف أو الشركة المنتجة.[2]

ومن أمثلة ذلك ما تعرّضت له شركة "تويوتا" اليابانية سنة 2019 التي تم اختراق أنظمتها وسرقة البيانات الشخصية لما يقارب 3.1 مليون من عملائها، رغم كونها من كبرى الشركات الرائدة في مجال التكنولوجيا الصناعية. وقد أدى ذلك إلى زعزعة ثقة المستخدمين وتكبيد الشركة خسائر اقتصادية ومعنوية جسيمة[3].

كما يُعتبر الهجوم الذي وقع في ماي 2017، والمعروف بهجوم **"WannaCry"**، من بين أكبر الهجمات الإلكترونية التي استهدفت الاقتصاد العالمي. فقد صنّفته شركة "فورسبوينت سيكيوريتي" كأحد أضخم العمليات التي نفذها قراصنة الويندوز، حيث بلغ معدل انتشار الهجمات مع نهاية اليوم الأول فقط حوالي 5 ملايين رسالة في الساعة. وقد أعلنت شركة "أفاست" للأمن المعلوماتي أنها رصدت أكثر من

[1] ليلى بعوني،" التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نمودجا"، **مجلة ستراتيجيا**، العدد 16، السداسي الثاني،2021، ص 16.

[2] صباح كزيز، "أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية نموذجا"، **مجلة الناقد للدراسات القانونية**، العدد 03، أكتوبر 2018، ص 131.

[3] ليلى بعوني، مرجع سبق ذكره، ص 18.

75 ألف هجوم في 99 دولة، وهو عدد ارتفع لاحقًا ليتجاوز 100 دولة، مخلّفًا خسائر اقتصادية هائلة على المستويين الفردي والمؤسسي[1].

3. التأثير على مفاهيم القوة والأمن.

أدى تطور الفضاء السيبراني إلى تغيير مفهوم القوة والأمن، حيث ساهم في تحويل طبيعة النزاعات من تقليدية إلى حروب سيبرانية، شملت حتى استهداف الجيوش. ويمكن تحديد أهداف استخدام هذا الفضاء في النزاعات من خلال التأثير على سلوك طرف آخر، ودفعه للقيام بأفعال لم يكن لينفذها لولا هذا الضغط، كما هو الحال في استهداف البنية التحتية للدولة عن طريق نشر فيروسات تؤدي إلى تدمير أجهزتها. ويشمل ذلك أيضًا قدرة الفاعل على التحكم في أجندات الآخرين وترتيب أولوياتهم.[2] كما أن هذه الهجمات على البنية التحتية تؤدي إلى إرباك في العمليات اليومية، بما في ذلك المصارف، ونظم الاتصالات، ووسائل النقل. وفي ظل هذا التحدي، أصبحت الدول تواجه مخاطر غير مسبوقة نتيجة تصاعد الهجمات السيبرانية التي تمس أمنها واستقرارها. [3] وقد تجلى ذلك في عدة حالات، من بينها كما تعرّضت السعودية في عام 2017 لهجوم بفيروس "الصخرة الدوارة" "**Stone Drill**" من قراصنة إيرانيين استهدف قطاعي الطيران والبتروكيماويات، مما ألحق أضرارًا كبيرة بالشركات العاملة في تلك المجالات الحيوية.[4]

ومن أبرز العمليات التي أثارت جدلًا واسعًا في الأوساط الأمنية والسياسية داخل الولايات المتحدة الأمريكية، حادثة تسلل قراصنة يُعتقد أنهم من روسيا خلال سنة 2016، إلى البريد الإلكتروني الخاص بالحملة الانتخابية للمرشحة الديمقراطية هيلاري كلينتون، حيث تم تسريب عدد كبير من الوثائق إلى موقع "ويكيليكس". وقد دفعت هذه الواقعة الإدارة الأمريكية، بقيادة باراك أوباما، إلى اتخاذ قرار بطرد

---

[1] جمال بوزيادية، "**الأمن السيبراني**"، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص استراتيجية ودولية، جامعة الجزائر 3 كلية العلوم السياسية والعلاقات الدولية،2021، ص 21.

[2] إيمان عبد القادر، "أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من2011 حتى 2023"، **مجلة الأكاديمية العسكرية للدراسات العليا والاستراتيجية**، العدد 3، يناير2024 ، ص 108.

[3] سيناء علي محمود،" التحديات الأمنية للدول في الفضاء السيبراني"، **مجلة قضايا سياسية**، كلية العلوم السياسية جامعة النهرين العدد 80، مارس 2025، ص 319.

[4] شريفة كلاع، "الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"، **مجلة الحقوق والعلوم الإنسانية** ، مجلد 15، العدد 01، 2022، ص 301.

35 دبلوماسيًا روسيًا. ورغم نفي الرئيس دونالد ترامب لهذه الاتهامات في لقائه مع نظيره الروسي فلاديمير بوتين بهلسنكي عام 2018، إلا أن الحادثة تظل مثالًا صريحًا على كيف يمكن للهجمات السيبرانية أن تهدد السيادة السياسية للدول.[1]

4. التجسس الإلكتروني.

لقد سهّلت شبكة الإنترنت العمليات الجاسوسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو الهيئات الرسمية. وتستهدف عمليات التجسس في العصر الرقمي ثلاث مجالات رئيسية: العسكري، السياسي، والاقتصادي.[2] ومن أبرز الأمثلة على ذلك، ما قام به قراصنة صينيون من اختراق أنظمة شركة " لوكهيد مارتن" الأمريكية، وسرقة معلومات حساسة تتعلق بتكنولوجيا تصنيع المقاتلة **"F-35"**، والتي استخدمتها الصين لاحقًا في تطوير مقاتلتها، **"J-20"** وهو ما شكّل تهديدًا مباشرًا للتفوق العسكري والتكنولوجي للولايات المتحدة.[3]

5. التأثير على استراتيجية عمل التنظيمات الإرهابية.

تستخدم الجماعات الإرهابية الفضاء الإلكتروني كأداة أيديولوجية لنشر أفكارها وتجنيد الأفراد خاصة عبر مواقع التواصل الاجتماعي.[4] وتُعدّ تنظيمات مثل "داعش" من أبرز الفاعلين في هذا المجال حيث استغلّت الإنترنت لنشر الدعاية المتطرفة وتجنيد الأتباع وجمع التبرعات وشنّ هجمات إلكترونية. وتشير التقارير إلى امتلاك التنظيم لأكثر من 53 ألف موقع إلكتروني، و93 ألف صفحة باللغة العربية وآلاف الصفحات بلغات أخرى، تُستخدم كلها في شن حرب نفسية على الدول، وتحقيق أهداف التنظيم من تمويل وابتزاز وتجنيد.[5] وفي مثال عملي على المواجهة، قامت الحكومة الأمريكية في مايو 2012، من خلال مركز الاتصالات الاستراتيجية، بالتعاون مع وزارة الخارجية ودوائر الاستخبارات، بالرد خلال 48 ساعة على مواد دعائية إلكترونية نشرها تنظيم القاعدة، بنشر رسائل مضادة على نفس المواقع تظهر

[1] جمال بوزيادية، مرجع سبق ذكره، ص 21.

[2] صباح كزيز، مرجع سبق ذكره، ص 130.

[3] شريفة كلاع، مرجع سبق ذكره، ص 302

[4] إيمان عبد القادر، مرجع سبق ذكره، ص 108

[5] جمال بوازدية، مرجع سبق ذكره، ص 21.

كيف أن ضحايا التنظيم هم من المواطنين اليمنيين، بهدف تحجيم التأثير الدعائي للجماعات الإرهابية.[1]

ينبغي في ظل تفاقم هذا الخطر على الأمن السيبيراني، بحيث أنه أصبح تحديا عالميا يتطلب تعاونًا دوليا ويتطلب إيجاد استراتيجية شاملة. باختصار فإن مواجهة الجرائم الإلكترونية ضرورة حتمية للحفاظ على الأمن السيبيراني، الذي أصبح ركيزة أساسية لاستقرار المجتمعات في عصر التطور التكنولوجي الهائل.

الفرع الثاني: الجهود الدولية والإقليمية في مكافحة الجريمة الإلكترونية.

شكلت الطبيعة المعقدة للجريمة الإلكترونية والتي باتت توصف جريمة عابرة للحدود الوطنية الدافع الأولى نحو تفعيل التعاون الدولي لمكافحتها، كونه من الصعب التعامل معها بشكل منفرد من قبل كل دولة على حدى، لذلك، برزت الحاجة الملحّة إلى تنسيق الجهود الدولية ووضع أطر قانونية مشتركة بالإضافة إلى تعزيز آليات تبادل المعلومات والخبرات لمكافحة هذا النوع من الجرائم، وسنتناول في سياق هذا الفرع أبرز الجهود المبذولة على المستويين الدولي والإقليمي من خلال استعراض مساهمات عدد من المنظمات الدولية والإقليمية في هذا المجال.

أولًا: الجهود على المستوى الدولي.

1. جهود منظمة الأمم المتحدة:

عملت الأمم المتحدة منذ نشأتها على رسم سياسة ناجعة في مجال منع الجريمة وتحقيق العدالة الجنائية، عبر إقرار العديد من التوصيات وإنشاء لجان متخصصة، من بينها اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين.[2]

والتي تتمثل مهامها أساسًا في إعداد البرامج والدراسات والتقارير حول التطورات، وتقديم المشورة للأمين العام، وتعزيز التعاون الدولي بين الدول، والمساهمة في تنظيم المؤتمرات الدولية الدورية كل خمس

[1] تقرير: **استخدام الإنترنت لأغراض إرهابية** ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة **(UNDC)**، الأمم المتحدة، نيويورك، 2012، الرابط:https://www.unodc.org/documents/congress/background-information/Terrorism/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf

[2] فريد ناشف، مرجع سابق، ص436

سنوات، وذلك لتعزيز وتبادل المعارف والخبرات بين الإخصائيين من مختلف الدول من أجل تدعيم التعاون الدولي والإقليمي في مجال مكافحة الجريمة، [1] ومن بين أهم هذه المؤتمرات:

- ❖ المؤتمر الخامس المنعقد في جنيف سنة 1975.
- ❖ المؤتمر الدولي السادس بكاراكاس (فنزويلا) المنعقد سنة 1980.
- ❖ مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاقبة المجرمين المنعقد بمدينة ميلانو (إيطاليا) سنة 1985.
- ❖ مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء المنعقد في هافانا سنة 1990.
- ❖ مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين المنعقد في القاهرة سنة 1995.

وقد أكدت هذه المؤتمرات جميعًا على أهمية التعاون الدولي في مكافحة الجريمة. وتُعد هذه الجهود مجرد جزء من مبادرات عديدة بذلتها الأمم المتحدة في مواجهة الجريمة الإلكترونية، وذلك انسجامًا مع أهدافها الرامية إلى حفظ السلم والأمن الدوليين وتعزيز التعاون بين الدول.

2. منظمة التعاون الاقتصادي والتنمية (OECD).

بدأت هذه المنظمة الاهتمام بالجرائم المرتكبة عبر الإنترنت منذ عام 1978، حيث أعدت مجموعة من الأدلة والقواعد الإرشادية المرتبطة بتقنية المعلومات. وكان من أبرزها الدليل الخاص بحماية الخصوصية ونقل البيانات، الذي تبناه مجلس المنظمة سنة 1980[2]، مع التوصية للدول الأعضاء بضرورة الالتزام به. وفي عام 1983، أصدرت المنظمة تقريرًا بعنوان "**الجرائم المرتبطة بالحاسوب وتحليل السياسات الجنائية.** واستعرض السياسية الجنائية الحالية وتقديم مقترحات خاصة بعدة دول أعضاء، وتضمن التقرير الحد الأدنى من الأفعال المتعلقة بإساءة استخدام الحاسوب التي على عدة دول

[1] محمود محمد صفاء الدين على شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الأنترنت، **مجلة البحوث القانونية والاقتصادية**، كلية الحقوق جامعة المنوفية، ع51، مايو2020، ص529.

[2] بن علية بن جدو، تحديات الأمن السيبيراني لمواجهة الجريمة الإلكترونية، **المجلة الجزائرية للأمن الإنساني**، المجلد 07، العدد 02، جويلية 2022، ص 309.

تجريمها.[1]وتعقد المنظمة سنويًا ملتقيات وورش عمل متخصصة في هذا المجال، تركز فيها على معايير الأمن المعلوماتي ومستويات تطبيق القانون، بهدف مواكبة تطورات الجريمة الإلكترونية[2].

3. المنظمة العالمية للملكية الفكرية (WIPO) .

أنشأت هذه المنظمة فريق عمل متخصصًا في مجال التكنولوجيات الحديثة والإعلام الآلي، بهدف دراسة السبل الكفيلة بحماية برامج الحاسوب وقواعد البيانات من خلال إخضاعها لقوانين الملكية الفكرية وحقوق المؤلف. [3] فقد أولت هذه المنظمة اهتمامًا بالمجال المعلوماتي، وسعت إلى توفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، فبعد أن استقر الرأي لديها بعدم إمكانية توفير الحماية لهما في تشريعات براءات الاختراع، تم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية، خاصة اتفاقيتي "التريبس" و"بيرن"،[4] اللتان دعتا الدول الأعضاء إلى تطوير تشريعاتها الوطنية، لا سيما في ما يتعلق بحقوق المؤلف، وإلى فرض عقوبات صارمة على كل من يرتكب أفعالًا تمس بالملكية الفكرية، بما في ذلك تزوير العلامات التجارية.

ثانيًا: الجهود على المستوى الإقليمي.

1. جهود الاتحاد الأوروبي والمجلس الأوروبي.

أسفرت جهود الاتحاد الأوروبي والمجلس الأوروبي عن إصدار اتفاقية بودابست بشأن الجريمة السيبرانية سنة 2001 والتي دخلت حيز التنفيذ سنة 2004. وتُعد هذه الاتفاقية أول إطار قانوني دولي لمكافحة الجرائم الإلكترونية، حيث تقدم نموذجًا قانونيًا يمكن للدول تكييفه مع تشريعاتها الوطنية، تركز الاتفاقية على جرائم مثل النفاذ غير المشروع (القرصنة) واعتراض البيانات [5] . كما تنص على تعزيز

[1] آسيا السبتي ،عمر بوقريط، الجرائم السيبيرانية: مفهومها وآليات مكافحتها، **مجلة الحقوق والعلوم الإنسانية**، المجلد 18، العدد01، أفريل2025، ص211.

[2] يوسف صغير، مرجع سبق ذكره، ص98.

[3] جمال براهيمي، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراه في العلوم تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص276 .

[4] بن علية بن جدو، مرجع سبق ذكره، ص310.

[5] سيناء علي محمود، مرجع سبق ذكره، ص 327 ص 328.

التعاون القضائي والأمني لاسيما في مجال تسليم المجرمين، ورغم أن الاتفاقية لا تغطي كافة التهديدات السيبرانية الحديثة، فإنها تُعد خطوة مهمة نحو تعزيز التعاون الدولي في هذا المجال.

2. مجموعة الدول الثمانية (G8).

تناولت مجموعة الدول الثمانية والتي تضم كل من: الولايات المتحدة، اليابان، المانيا، روسيا الاتحادية ،المملكة المتحدة فرنسا، كندا.[1] موضوع الجريمة الإلكترونية في اجتماعها المنعقد بباريس سنة 2000، حيث شددت على ضرورة مكافحة ما يُعرف بـ "الملاذات الرقمية" الخارجة عن الرقابة القانونية وكانت المجموعة قد ربطت منذ ذلك الوقت محاولاتها الرامية إلى إيجاد حلول دولية تتماشى مع اتفاقية مجلس أوروبا. [2] اعتمدت وزارات العدل للدول الأعضاء، خلال اجتماع عقد في واشنطن في يومي التاسع والعاشر من ديسمبر 1997، المبادئ التي تُشكل الأساس لشبكة نقاط اتصال وطنية وبجانب هذه المبادئ تم وضع خطة عمل لإنشاء شبكة متابعة لتقديم تقارير،[3] تتعلق بمدى التزام الدول الأعضاء ورغم ضيق نطاق التوصيات الصادرة عن المجموعة، إلا أنها شكّلت أساسًا لتطوير آليات التنسيق بين الدول لمواجهة الجريمة الإلكترونية.

3. الجهود المبذولة على المستوى العربي.

تمثلت أبرز الجهود الإقليمية العربية في مكافحة الجريمة الإلكترونية في إصدار القانون العربي النموذجي لمكافحة الجريمة الإلكترونية بموجب القرار رقم 495 الصادر عن مجلس وزراء العدل العرب في دورته التاسعة سنة 2003،[4] يتضمن هذا القانون 27 مادة موزعة على أربعة أبواب، حيث يتناول الباب الأول الجرائم الإلكترونية والعقوبات المقررة. قد صدر عن جامعة الدول العربية دليل استشاري ثم ثم من ذلك التوقيع على الاتفاقية العربية لمكافحة الجرائم التقنية للمعلومات سنة2010. ودعا المجلس

---

[1] الجزيرة، "**مجموعة الثماني**"، الجزيرة نت، 6 يوليو 2008، الرابط :
https://www.aljazeera.net/news/2008/7/6/%D9%85%D8%AC%D9%85%D9%88%D8%B9%D8%A9-%D8%A7%D9%84%D8%AB%D9%85%D8%A7%D9%86%D9%8A ، اطلع عليه بتاريخ: 16 ماي 2025، الساعة 20:20 .

[2] بن علية بن جدو، مرجع سبق ذكره، ص 312.

[3] يوسف الصغير، مرجع سبق ذكره، ص 102.

[4] جمال إبراهيمي، مرجع سبق ذكره، ص 287

الدول العربية المصدقة للاتفاقية إلى إبلاغ الأمانة الفنية للمجلس بالإجراءات التي تتخذها من أجل موالمة تشريعاتها مع أحكام الاتفاقية وتجريم أشكال الجرائم الإلكترونية.[1]

يلاحظ أن الجهود المبذولة على المستوى العربي تعتمد على معالجة النقص التشريعي والتنظيمي في مجال مكافحة الجريمة الإلكترونية عبر تحديد ماهي الأفعال التي يمكن ممارستها عبر الأنترنت.

[1] آسيا السبتي، عمر بوقريط، مرجع سبق ذكره، ص 214.

خلاصة الفصل الأول:

من خلال ما سبق، يتّضح أن الجريمة الإلكترونية تمثّل نمطًا مستحدثًا من الجرائم، فرضه تطوّر تكنولوجيا المعلومات والاتصال، وترافق مع تحوّل عميق في بيئة النشاط الإجرامي. فقد توصّلنا إلى أن هذه الجريمة تتميز بعدة خصائص تجعلها أكثر تعقيدًا من الجرائم التقليدية، سواء من حيث طبيعتها العبر–حدودية، أو من حيث الفاعلين فيها والوسائل المستعملة، مما يصعّب من عملية الكشف عنها وتتبع مرتكبيها. كما اتّضح أن أسباب انتشارها متعددة ومتداخلة، تشمل أبعادًا دولية، اقتصادية، اجتماعية ونفسية كذلك، سمح لنا هذا الفصل بتحديد مختلف مراحل تطور الجريمة الإلكترونية، وأنواعها المتنوعة سواء تلك التي تستهدف الأفراد أو الأموال أو أمن الدول. كما وقفنا عند أهم أركان هذه الجريمة، لنبيّن كيف أنها رغم احتفاظها بالبنية التقليدية للجريمة، إلا أنها تكتسي طابعًا خاصًا مرتبطًا بالبيئة الرقمية. وفي المقابل، عرّفنا الأمن السيبراني باعتباره الإطار الذي تُبذل ضمنه الجهود لحماية الفضاء الرقمي من مختلف التهديدات، سواء كانت ذات طابع تقني، اقتصادي، سياسي أو قانوني، مما جعله يشكّل اليوم إحدى ركائز الأمن القومي للدول.

وعليه، فإن هذا الفصل مهّد لفهم الجوانب النظرية للموضوع، ويمثل قاعدة ضرورية للانتقال إلى الفصل الثاني، الذي سنتناول فيه واقع الجريمة الإلكترونية في الجزائر، والجهود القانونية والاستراتيجيات المعتمدة لمواجهتها وضمان الأمن السيبراني.

الفصل الثاني:

سبل تعزيز الأمن السيبراني في ظل تنامي الجريمة الإلكترونية في الجزائر

تمهيد:

أضحت الجريمة الإلكترونية من الظواهر الإجرامية المستحدثة التي تفرض تحديات متزايدة على المنظومات القانونية والأمنية في مختلف الدول، بالنظر إلى طبيعتها المعقدة والمتغيرة باستمرار، وارتباطها الوثيق بالتطور التكنولوجي المتسارع. وفي السياق الجزائري، تزايدت هذه الجرائم بشكل لافت خلال السنوات الأخيرة، نتيجة ارتفاع نسبة استخدام الإنترنت ووسائل التواصل الرقمي، وضعف الوعي السيبراني، فضلًا عن هشاشة بعض البنى التحتية المعلوماتية، مما جعل من الفضاء السيبراني بيئة خصبة لارتكاب أنماط جديدة من الأفعال الإجرامية.

وأمام هذا الواقع المتنامي، بات لزامًا على الدولة الجزائرية تطوير سياسات واستراتيجيات فعالة تهدف إلى مكافحة هذه الظاهرة والحد من آثارها السلبية على الأفراد والمؤسسات، وذلك من خلال تعزيز الإطار القانوني، وبناء قدرات تقنية ومؤسساتية قادرة على مجابهة التحديات السيبرانية، بما يضمن تحقيق مستوى مقبول من الأمن السيبراني الوطني.

وانطلاقًا من ذلك، يسعى هذا الفصل إلى دراسة الجريمة الإلكترونية في الجزائر من زاويتين أساسيتين: يتناول المبحث الأول منها واقع الجريمة الإلكترونية، من حيث مظاهرها، خصائصها واتجاهاتها الإحصائية، في حين يركز المبحث الثاني على الاستراتيجية الجزائرية في التصدي لهذه الجرائم وتحقيق الأمن السيبراني، من خلال عرض الجهود القانونية، التقنية، والمؤسساتية المعتمدة في هذا المجال.

المبحث الأول: واقع الجريمة الإلكترونية في الجزائر

لقد أصبحت الجريمة الإلكترونية في الجزائر واقعًا ملموسًا يفرض نفسه على أجندة الأمن الوطني، مع ازدياد اعتماد الأفراد والمؤسسات على تكنولوجيا المعلومات والاتصالات، واتساع رقعة الفضاء السيبراني. فقد شهدت البلاد خلال السنوات الأخيرة تزايدًا ملحوظًا في وتيرة الجرائم المرتكبة عبر الوسائط الرقمية، من حيث الكم والنوع، وتنوعت بين المساس بالأفراد، والممتلكات، والمؤسسات، وصولًا إلى التهديدات ذات الطابع السيادي والأمني. كما ساهمت التحولات المجتمعية والاقتصادية، إلى جانب ضعف الثقافة الرقمية، في جعل البيئة الجزائرية مهيأة لتنامي هذه الظاهرة.

وتكمن أهمية تناول واقع الجريمة الإلكترونية في الجزائر في الكشف عن طبيعة هذا التحدي الأمني المستحدث، ومدى تأثيره على استقرار المجتمع والدولة، وذلك من خلال رصد تطورها وتحديد أبرز أنماطها، وكذا تحليل الانعكاسات الأمنية والاستراتيجية التي تفرضها على الأمن السيبراني الوطني. ولهذا الغرض، ينقسم هذا المبحث إلى مطلبين أساسيين: يُخصص أولهما لتتبع تطور الجريمة الإلكترونية وتصنيف أبرز أصنافها، في حين يتناول الثاني التحديات الميدانية والمؤسساتية التي تعيق مواجهتها ومدى تأثيرها المباشر على بنية الأمن السيبراني في الجزائر.

المطلب الأول: تطور وأنواع الجريمة الالكترونية في الجزائر.

شهدت الجزائر خلال العقد الأخير تطورًا ملحوظًا في مجال الجرائم الإلكترونية، وذلك نتيجة لتسارع انتشار الإنترنت وتزايد استخدام الأجهزة الذكية وشبكات التواصل الاجتماعي. وقد انعكس هذا التطور على طبيعة الجريمة، حيث تحولت من ظاهرة فردية محدودة إلى نشاط إجرامي منظّم يتسم بتعدد الأشكال والأنماط، ما شكل تحديًا جديدًا للأمن الوطني والأمن السيبراني، يعكس تصاعد عدد القضايا الإلكترونية في الجزائر، كما تظهره الإحصائيات الرسمية، مدى اتساع هذه الظاهرة وأبعادها المتنوعة حيث تنوعت بين جرائم النصب والاحتيال، الابتزاز، المساس بالخصوصيات، واستغلال الأطفال وغيرها من الجرائم الرقمية.

يناقش هذا المطلب في فرعه الأول مراحل تطور الجريمة الإلكترونية في الجزائر من حيث الكم والنوع، بينما يسلط الفرع الثاني الضوء على أنواع الجرائم الإلكترونية المنتشرة في البلاد وتأثيرها على المجتمع والأمن الوطني.

الفرع الأول: تطور الجريمة الإلكترونية في الجزائر.

يُعد فهم التطور الزمني للجريمة الإلكترونية في الجزائر مدخلًا أساسيًا لتقييم مدى خطورة هذه الظاهرة واتساع نطاقها، خاصة في ظل التحولات الرقمية المتسارعة التي تشهدها البلاد. فقد أدى الانتشار المتزايد لاستخدام الإنترنت ووسائل التواصل الاجتماعي إلى خلق بيئة خصبة لنشوء أنماط جديدة من الجرائم، تطورت تدريجيًا من جرائم فردية بسيطة إلى جرائم منظمة ومعقدة. ويُبرز هذا الفرع أبرز المحطات التي عرفتها الجريمة الإلكترونية في الجزائر، مستعرضًا أهم الإحصائيات والبيانات الرسمية التي تعكس تصاعد حجم الظاهرة وتحولها النوعي، في سياق وطني يتسم بتزايد الاعتماد على الفضاء السيبراني.

عرفت الجزائر تصاعدًا مقلقا في حجم الجرائم الإلكترونية، نتيجة عوامل متعددة أهمها: الانتشار المتسارع للإنترنت، ارتفاع نسبة مستخدمي الهواتف الذكية، وتوسع نشاط الأفراد عبر شبكات التواصل الاجتماعي، ووفقًا لتقرير Digital 2024 ، بلغ عدد مستخدمي الإنترنت في الجزائر في بداية عام 2024 نحو 33.49 مليون مستخدم، أي ما يعادل 72.9% من إجمالي السكان فيما بلغ عدد مستخدمي وسائل التواصل الاجتماعي 24.85 مليون مستخدم، أي بنسبة 54.1% من السكان.[1] وفي بداية سنة 2025 ارتفع عدد مستخدمي الإنترنت إلى 36.2 مليون مستخدم، ما يعادل 76.9% من إجمالي السكان مسجلًا زيادة بنسبة 1.4% مقارنة بالعام السابق.[2] ويعكس هذا الانتشار الواسع للتكنولوجيا الاعتماد المتزايد على الفضاء الرقمي، ما ساهم في تفشي الجريمة الإلكترونية بمختلف أنواعها.

بدأت الجريمة الإلكترونية في الجزائر كظاهرة محدودة النطاق، إلا أن المؤشرات الإحصائية في السنوات الأخيرة تُظهر تصاعدًا مقلقًا في عدد القضايا:

[1] Kepios, "**Digital 2024: Algeria**", DataReportal, 2024, available in: https://datareportal.com/reports/digital-2024-algeria, accessed: 10 May 2025, at: 00:00.

[2] Kepios, "**Digital 2025: Algeria**", DataReportal, 2025, available in: https://datareportal.com/reports/digital-2025-algeria, accessed: 10 May 2025, at: 00:00.

في سنة 2015، سُجّل عدد محدود من القضايا الإلكترونية لم يتجاوز 500 قضية حسب تصريح الملازم الأول مطمط أمين، وهذا ما يعكس الطبيعة الفردية للجريمة الإلكترونية في بداياته. [1]

أما في سنة 2017، فقد عالجت مصالح الشرطة القضائية ما يقارب 2130 قضية متعلقة بجرائم إلكترونية، تم حل 1570 منها، وهو ما يشير إلى تطور نسبي في حجم وانتشار هذه الجرائم، خصوصًا تلك المتعلقة بالسب والتشهير، الابتزاز الإلكتروني، والتحرش عبر الإنترنت[2].

وبحلول سنة 2018، سُجل ارتفاع في قضايا الابتزاز والتشهير، بحسب ما أفادت به وكالة الأنباء الجزائرية، مع بداية تشكّل أنماط أكثر تنظيمًا للجرائم الرقمية[3].

شكلت سنة 2020 نقطة تحوّل محورية في تطور الجريمة الإلكترونية، بسبب تداعيات جائحة كوفيد-19، التي فرضت الحجر الصحي وزادت من الاعتماد على الإنترنت في مختلف مناحي الحياة. وقد كشفت المديرية العامة للأمن الوطني عن تسجيل 5200 قضية خلال هذه السنة، [4] في ارتفاع حاد مقارنة بسنوات ما قبل الجائحة، ما يعكس انفجارًا رقميا في حجم الجرائم السيبرانية.

استمرت الظاهرة في التصاعد، إذ كشف الرائد فريد درامشية عن تسجيل:

[1] الإذاعة الجزائرية، "**الأمن الوطني: تسجيل 5200 جريمة إلكترونية في 2020**"، 7 سبتمبر 2021، الرابط : https://radioalgerie.dz/news/ar/article/20210907/217404.html ، اطلع عليه في 13 ماي 2025، الساعة 10:00.

[2] لإذاعة الجزائرية "**مجلة الشرطة: معالجة 2130 جريمة إلكترونية خلال 2017**"، 17 أبريل 2018، الرابط : https://radioalgerie.dz/news/ar/article/20180417/139053.html ، تم الاطلاع عليه بتاريخ: 13 مايو 2025، الساعة 10:00.

[3] وكالة الأنباء الجزائرية، "**الجريمة الإلكترونية: معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني**." نُشر في 17 ديسمبر 2018، الرابط: https://www.aps.dz/ar/sante-science-technologie/63173-1100-2018 ، تم الاطلاع عليه في 13 مايو 2025، الساعة 10:00

[4] الإذاعة الجزائرية، مرجع سبق ذكره.

2838 قضية سنة 2021، 4600 قضية سنة2022، 500 قضية خلال الأشهر الأولى فقط من سنة 2024.[1]

في عام 2023، شهدت الجزائر زيادة ملحوظة في عدد الجرائم الإلكترونية، حيث تم تسجيل 14,000 جريمة مقارنة بـ12,000 جريمة في عام 2022، ما يعكس زيادة قدرها 2,000 قضية. تم توزيع هذه القضايا على مختلف الجهات الأمنية، حيث سجل الأمن الوطني 3325 قضية بين يناير وأكتوبر 2023، شملت 2315 ضحية و4138 مشتبها فيهم.

ومن جهة أخرى، عالج الدرك الوطني 4500 قضية في نفس العام، بينما سجل الأمن العسكري قرابة 4000 قضية سرية تتعلق بالجرائم الإلكترونية.[2]

أما بالنسبة الى سنة 2024، فقد بلغت القضايا المسجلة 5298 قضية سيبرانية بحسب المديرية العامة للأمن الوطني[3].

وقد رافق هذا التصاعد الكمّي تحولٌ نوعي في طبيعة الجرائم، إذ لم تعد تقتصر على أفراد معزولين، بل اصبحت تنفذ من قبل شبكات اجرامية منظمة تشمل:

- عصابات لاستغلال الاطفال جنسيا عبر الأنترنت.

- شبكات لتزوير الوثائق والأختام الرسمية.

---

[1] الإذاعة الجزائرية، "**الرائد درامشية للإذاعة: معالجة 500 جريمة سيبرانية منذ بدء 2023**" ،15 فبراير 2023، الرابط: https://news.radioalgerie.dz/ar/node/21741 ، اطلع عليه بتاريخ 13 مايو 2025، الساعة 10:00.

[2] نوارة باشوش ،"**14 ألف جريمة سيبرانية في 2023 والتسوق الإلكتروني في الصدارة** "، الشروق أونلاين، الرابط : https://www.echoroukonline.com/14-%D8%A3%D9%84%D9%81-%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%81%D9%8A-2023-%D9%88%D8%A7%D9%84%D8%AA%D8%B3%D9%88%D9%82-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA18 ، فبراير 2024. تم الاطلاع عليه في 13 مايو 2025، الساعة 10:00 .

[3] نوارة باشوش ،"**توقيف 1410 شخص ينشطون في 'تيك توك' ومواقع أخرى** "، الشروق أونلاين، 14 مارس 2025، الرابط: https://www.echoroukonline.com/%D8%AA%D9%88%D9%82%D9%8A%D9%81-1410-%D8%B4%D8%AE%D8%B5-%D9%8A%D9%86%D8%B4%D8%B7%D9%88%D9%86-%D9%81%D9%8A-%D8%AA%D9%8A%D9%83-%D8%AA%D9%88%D9%83-%D9%88%D9%85%D9%88%D8%A7%D9%82%D8%B9-%D8%A3%D8%AE ، اطلع عليه بتاريخ: 01 ماي 2025، الساعة 10:00.

- تنظيمات للنصب والاحتيال والابتزاز والتشهير.

- مجموعات لترويج الفكر الإرهابي إلكترونيا.

- عصابات قرصنة وتخريب مواقع إلكترونية حساسة.[1]

الفرع الثاني: الجرائم الإلكترونية في الجزائر.

تشهد الجزائر، على غرار باقي دول العالم، تصاعدًا مستمرًا في وتيرة الجريمة الإلكترونية مدفوعة بتزايد الاعتماد على تكنولوجيا المعلومات والاتصالات، ولا سيما الإنترنت ووسائل التواصل الاجتماعي. هذا الواقع أفرز أشكالًا جديدة من الانحرافات الإجرامية التي انتقلت من الفضاء التقليدي إلى الفضاء الرقمي مما جعل هذه الجرائم تمثل تحديًا حقيقيًا للأمن السيبراني في البلاد.

وتتنوع الجرائم الإلكترونية في الجزائر بين ما هو موجه ضد الأفراد أو المؤسسات، وما هو موجه ضد النظام العام وأمن الدولة. وقد كشفت الإحصائيات الرسمية للمديرية العامة للأمن الوطني لسنة 2024 التي صرح بها عميد أول للشرطة نسيم بوطانة، عن تسجيل أكثر من 5000 قضية إلكترونية،[2] توزعت على عدة أنماط جرمية، نعرضها فيما يلي:

الجدول رقم (02): توزيع الجرائم الإلكترونية المسجلة في الجزائر لسنة 2024.

نوع الجريمة الالكترونية	عدد القضايا المسجلة	عدد الموقوفين
نشر محتويات مخالفة للنظام عبر الأنترنت	1164	1410
نصب واحتيال غبر الأنترنت	1387	2659
المساس بالأشخاص عبر الأنترنت	1647	1496
المساس بأنظمة المعالجة الآلية للمعطيات	335	282
المساس بالأطفال عبر الأنترنت	129	120
بيع السلع المحضورة عبر الأنترنت	156	276

المصدر: من إعداد الطالبتين بتصرف

[1] فيروز لطرش، حاتم بن عزوز، "الجريمة الالكترونية في الجزائر : من جريمة فردية الى جريمة منظمة"، **مجلة آفاق للعلوم**، الطبعة01 ، العدد 01، جانفي 2016، ص 331 ص 332.

[2] نوارة باشوش ، مرجع سبق ذكره.

يتبين من تحليل هذه المعطيات أن نشر المحتويات المخالفة للنظام عبر الإنترنت يحتل المرتبة الأولى من حيث عدد القضايا، ما يدل على انتشار ظواهر رقمية تهدد القيم العامة، مثل التحريض والكراهية والمحتوى الإباحي. ويليها النصب والاحتيال الإلكتروني، مما يعكس تنامي الأنشطة الاحتيالية مستغلّة الطابع المجهول للفضاء السيبراني. كما أن الجرائم الماسة بالأشخاص، كالتشهير والابتزاز سجلت بدورها نسبًا مقلقة، خاصةً في ظل تفشي استخدام الشبكات الاجتماعية. بناءً على هذا الواقع سنستعرض فيما يلي أبرز أصناف الجرائم الإلكترونية المنتشرة في الجزائر، مع توضيح طبيعتها وآثارها:

أولا: جريمة التهديد والابتزاز الإلكتروني .

تتمثل هذه الجريمة في توجيه تهديدات للضحية باستخدام الوسائط الرقمية، إما بنشر صور أو فيديوهات أو تسريب معلومات شخصية، مقابل دفع مبالغ مالية أو تنفيذ أوامر مجرّمة.[1] غالبًا ما يتم اصطياد الضحايا عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني. وتُعد النساء والأطفال أكثر فئات المجتمع عرضة لهذا النوع من الجرائم، بسبب هشاشتهم الرقمية. وتشير الإحصائيات سالفة الذكر إلى أن هذا النوع من الجرائم يشكّل خطرًا فعليًا على سلامة الأفراد النفسية والاجتماعية.

ثانيًا: جريمة النصب والاحتيال الإلكتروني.

يقصد بها الاستيلاء على أموال الغير باستخدام الحيلة والخداع الإلكتروني.[2] وتعد من أكثر الجرائم شيوعًا نظرًا لتوسع التجارة الإلكترونية وانتشار المعاملات الرقمية. وقد شهدت الجزائر تزايدًا ملحوظًا في هذا النوع من الجرائم، الذي أصبح يشكل تهديدًا للاقتصاد الرقمي وأمن المعاملات.

ثالثًا: جريمة الاعتداء على حرمة الحياة الخاصة.

أدى التطور التكنولوجي إلى ظهور ممارسات اعتدائية على خصوصيات الأفراد،[3] من خلال التصوير دون إذن، أو التنصت، أو نشر معلومات وصور شخصية. وتندرج تحت هذا النوع جرائم السب

[1] مريم عراب، "جريمة التهديد والابتزاز الإلكتروني"، **مجلة الدراسات القانونية المقارنة**، المجلد 07، العدد 01، جوان 2021، ص 1207.

[2] سامية العايب، منال عرابة، "الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني"، **مجلة هيرودوت للعلوم الإنسانية والاجتماعية**، مؤسسة هيرودوت للبحث العلمي والتكوين، المجلد 05، العدد 03، أكتوبر 2021، ص 04.

[3] عاسية زروقي، "جرائم الاعتداء على الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات الحماية"، **مجلة القانون والعلوم السياسية**، المجلد 08، العدد 02، جويلية 2022، ص 13.

والقذف الاعتداء على الشرف، انتحال الهوية،[1] وغيرها من الممارسات التي تمس بحقوق الإنسان الأساسية، وقد عرفت الجزائر تسجيل عدة حالات مشابهة خلال السنوات الأخيرة.

رابعًا: الجرائم المرتكبة ضد الأطفال عبر الإنترنت.

تُعد هذه الفئة من أخطر الجرائم الرقمية، لما لها من أثر نفسي واجتماعي خطير. وتشمل الاعتداءات الجنسية، التحريض على الفسق، التحرش، والمضايقات. وغالبًا ما يتم استغلال الأطفال عبر الإنترنت من خلال الألعاب أو تطبيقات الدردشة،[2] كما يتم استهدافهم بناءً على معلومات منشورة من طرف أسرهم، ما يتطلب وعيًا رقميًا أكبر لدى الأولياء[3] .

خامسًا: جريمة نشر الأخبار الكاذبة عبر الإنترنت.

تصنف ضمن الجرائم الموجهة ضد النظام العام وأمن الدولة، حيث يتم تداول معلومات مغلوطة أو ملفقة تهدف إلى زعزعة الاستقرار أو التأثير على الرأي العام.[4] وقد تزايد هذا النوع من الجرائم في الجزائر، خاصة مع انتشار منصات التواصل الاجتماعي، مما دفع المشرع الجزائري إلى تشديد العقوبات المرتبطة بها في إطار الحفاظ على الأمن المجتمعي والمؤسساتي.

المطلب الثاني: تحديات وانعكاسات الجريمة الإلكترونية على الأمن السيبراني في الجزائر.

رغم تزايد الاهتمام بالتحول الرقمي في الجزائر، وما يرافقه من جهود لتعزيز منظومة الأمن السيبراني، لا تزال الجريمة الإلكترونية تمثل تهديدًا حقيقيًا لهذا التوجه الاستراتيجي، لاسيما في ظل تنامي الهجمات الإلكترونية وتعقّد أساليبها. ويُعد فهم التحديات التي تواجه الجزائر في هذا المجال وتحليل الانعكاسات المترتبة عنها خطوة أساسية لتقييم واقع الأمن السيبراني واقتراح حلول فعالة. وفي هذا السياق، يتناول هذا المطلب تحليلًا مزدوجًا: في الفرع الأول سنبرز التحديات التي تحد من فاعلية

---

[1] عاسية زروقي، مرجع سبق ذكره ، ص 13 ص 14 ص15 .

[2] زهور دقايشية، "الحماية الجنائية للطفل غلى ضوء قانون العقوبات الجزائري"، **مجلة الحقوق والعلوم السياسية**، العدد 02، جوان2016، ص 269 ص 270.

[3] فيروز لطرش، عزوز حاتم، "الجريمة الإلكترونية في الجزائر: من جريمة فردية إلى منظمة"، **مجلة آفاق العلوم**، المجلد 01، العدد 01، جانفي 2016، ص 332.

[4] بشير عبد العالي، "استراتيجية المشرع الجزائري في مكافحة جريمة نشر الأخبار الكاذبة"، **مجلة دفاتر السياسة والقانون**، المجلد 14، العدد 03، جوان 2022، ص 147.

التصدي للجريمة الإلكترونية، كضعف البنية التقنية، ونقص التشريعات، وانخفاض مستوى الكفاءات؛ وفي الفرع الثاني سنبرز الآثار الاقتصادية والاجتماعية والمؤسسية التي تخلّفها هذه الظاهرة على منظومة الأمن السيبراني الوطني، ما يفرض ضرورة تبني رؤية شاملة ومتكاملة في التعامل معها.

الفرع الأول: تحديات الجريمة الالكترونية في الجزائر.

رغم الجهود المبذولة لمكافحة الجريمة الإلكترونية، تواجه الجزائر تحديات متعددة تحدّ من فعاليتها في هذا المجال. وتعود هذه الصعوبات إلى عوامل تقنية وتشريعية وبشرية، أهمها ضعف البنية التحتية الأمنية، وتأخر المنظومة القانونية في مواكبة التطورات الرقمية، إلى جانب محدودية الثقافة الأمنية ونقص الكفاءات المتخصصة. كما تعاني الجزائر من صعوبات في تحصيل الأدلة، وضعف في التنسيق الدولي فضلاً عن عزوف الضحايا والمؤسسات عن الإبلاغ. وتُمثل هذه العوامل مجتمعة عقبات حقيقية أمام تحقيق أمن سيبراني فعّال.

1. ضعف الاستثمار في الأمن السيبراني.

يُشكّل ضعف الاستثمار في الأمن السيبراني أحد أبرز التحديات التي تواجه الجزائر في ظل التحول الرقمي العالمي المتسارع. ويتجلى هذا التراجع بوضوح من خلال نتائج مؤشر تطور الحكومة الإلكترونية **(EGDI)** لعام 2024، الذي يقيس مستوى جاهزية الدول في مجالي البنية التحتية الرقمية والأمن السيبراني. فقد جاءت الجزائر في المرتبة 116 عالميًا بقيمة 0.5956، مقارنة بدول متقدمة مثل اليابان. (13 عالميًا، 0.9577)، الولايات المتحدة (19 عالميًا، 0.9194)، وفرنسا(34 عالميًا 0.8744).[1] هذه الأرقام تعكس بوضوح اتساع الفجوة في حجم الاستثمارات المخصصة لتعزيز التحول الرقمي والقدرات السيبرانية بين الجزائر والدول الرائدة.

[1] United Nations Department of Economic and Social Affairs ," **E-Government Survey 2024*:*** **Accelerating Digital Transformation for Sustainable Development** ", New York: United Nations, 2024, , available at:. https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf Accessed in : May 132025, at 10:00 AM.

1. ضعف البنية التقنية والتجهيزات الأمنية

تُواجه الجزائر تحديًا تقنيًا واضحًا في مجال الأمن السيبراني يتمثل في ضعف البنية التحتية الأمنية المستخدمة لحماية الأنظمة الحكومية وضمان استمرارية التشغيل. وفي هذا السياق، تبرز الحاجة إلى تحسين شامل لمختلف الجوانب التقنية، لا سيما من خلال تعزيز استخدام تقنيات التشفير المتقدمة كبرتوكولات **HTTPS** و **TLS** لحماية البيانات أثناء النقل، إلى جانب اعتماد خوارزميات تشفير قوية مثل **AES** و **RSA**[1].

الجدول رقم (03): مؤشرات الأمن السيبراني في الجزائر مقارنة بالدول المتقدمة (2024).

الدولة	الترتيب العالمي (NCSI)	مؤشر التعرض للأمن السيبراني	مؤشر الأمن السيبراني العالمي (GCI)
الجزائر	34	28	34
استراليا	66	87	97
اليابان	64	86	98
الو م أ	65	86	100
فرنسا	84	77	98

المصدر: MixMode "Global Cybercrime Report 2024"

تشير بيانات الجدول إلى أن الجزائر، رغم احتلالها المرتبة 34 في مؤشر الأمن السيبراني **(NCSI)**، إلا أنها تعاني من مؤشر تعرض مرتفع (28)، وهو ما يكشف عن قصور في البنية التقنية والتجهيزات الأمنية الأساسية في المقابل، تتفوق دول مثل الولايات المتحدة **(GCI: 100)**، واليابان وفرنسا **(GCI:98)** بفضل اعتمادها تقنيات متقدمة في التشفير وحماية الشبكات، مما يقلل من مستوى تعرضها

[1] Mohammed Reda BENDOUKHA, Kalloum BOUFELDJA," **Strengthening Cybersecurity of Public Accounting Data in Algeria: A Comparative Analysis of Gaps and Challenges with Developed Countries**", Revue des Arts, Linguistique, Littérature & Civilisations, vol 2, no11 September 2024 , Université Peleforo Gon Coulibaly – Korhogo, p20. Available at : file:///C:/Users/user/OneDrive/Documents/%D8%A7%D9%83%D8%B3%D9%84/01-Art.-Bendou-1.pdf, Accessed in : May 13 2025, at 14 :52.

للمخاطر السيبرانية. وهذا التباين يؤكد أن جاهزية الجزائر في مجال الأمن السيبراني تبقى محدودة مقارنة بالمعايير الدولية.

2. ضعف التشريع.

يعاني التشريع الوطني من ضعف في مواكبة التطورات السريعة لتقنيات المعلومات والاتصالات مما يؤدي إلى وجود فجوات قانونية في معالجة قضايا الأمن السيبراني وحماية البيانات. هذا الضعف يظهر في بطء التشريعات الوطنية في الاستجابة للتحديات الرقمية، مما يعيق تطبيق القوانين بشكل فعال في مواجهة التغيرات التكنولوجية.[1]

الجدول رقم (04): التدابير القانونية للأمن السيبراني (2024).

الدول	التدابير القانونية
استراليا	20
اليابان	20
الو م أ	20
فرنسا	20
الجزائر	19,18

المصدر: الاتحاد الدولي للاتصالات **(ITU).**

تُظهر بيانات الجدول تأخر الجزائر في مجال التدابير القانونية الخاصة بالأمن السيبراني، حيث حصلت على 19.18 من أصل 20، وهو أقل من العلامة الكاملة التي حققتها دول متقدمة كأستراليا اليابان، الولايات المتحدة، وفرنسا .(20/20) هذا التفاوت يعكس ضعفًا في ملاءمة الإطار التشريعي الجزائري مع متطلبات الأمن السيبراني الحديثة.

[1] كمال قريني، "**تحديات الأمن السيبراني في مكافحة الجرائم السيبرانية في المجتمع الجزائري**"، من مؤلف جماعي، بعنوان: الجرائم الالكترونية في المجتمع الجزائري(تشخيص الواقع وتحديات الأمن السيبراني)، د. ط، مارس 2022، ص 242.

3. محدودية الثقافة الأمنية الرقمية.

تواجه الجزائر تحدياً بارزاً يتمثل في ضعف برامج التوعية والتكوين الخاصة بالأمن السيبراني حيث تظل المبادرات الإعلامية والتثقيفية محدودة النطاق والتأثير، ولا تصل إلى الفئات الأكثر عرضة للمخاطر الإلكترونية. بالإضافة إلى ذلك، تفتقر المناهج التعليمية في مختلف المراحل إلى إدراج مفاهيم ومهارات الأمن السيبراني بشكل منهجي ومستدام، الأمر الذي يسهم في استمرار ضعف الثقافة الأمنية الرقمية لدى الأفراد والمؤسسات على حد سواء.[1]

الجدول رقم (05): التدابير التنظيمية والتقنية للأمن السيبراني (2024).

الدول	التدابير التقنية	التدابير التنظيمية
استراليا	17,99	20
اليابان	19,6	20
الو م أ	20	20
فرنسا	18,98	20
الجزائر	8,57	11,02

المصدر: الاتحاد الدولي للاتصالات **(ITU)** .

تشير بيانات الجدول إلى أن الجزائر تواجه ضعفًا كبيرًا في التدابير التنظيمية والتقنية للأمن السيبراني مقارنةً بدول متقدمة مثل أستراليا واليابان والولايات المتحدة وفرنسا. حيث سجلت الجزائر 11.02 في التدابير التنظيمية و8.57 في التدابير التقنية، بينما تصل هذه القيم في الدول الأخرى إلى 20 في التدابير التنظيمية، و بين 17.99 و20 في التدابير التقنية. هذا الفارق يعكس محدودية الثقافة الأمنية الرقمية في الجزائر، ما يبرز الحاجة إلى تعزيز برامج التوعية والتكوين وتطوير البنية التنظيمية والتقنية للأمن السيبراني بشكل ملحوظ.

4. ضعف الكفاءات التقنية لدى الجهات المكلفة بمكافحة الجريمة الإلكترونية.

تعاني الجزائر من نقص الخبرات الفنية والمعرفة التقنية اللازمة لدى العديد من القضاة، رجال الأمن، وأعضاء الهيئات المختصة، مما يُضعف قدرتهم على فهم الجرائم الإلكترونية المعقدة والمتطورة

[1] كمال قريني، مرجع سبق ذكره، ص 243.

بسرعة، ويؤثر سلبًا على فعالية الكشف والتحقيق والملاحقة.[1] تبرز في هذا السياق قضية التحقيق في عمليات التجسس التي استهدفت مصالح وشخصيات جزائرية عبر برمجيات متقدمة مثل "بيغاسوس" كمثال حي على تعقيد تحصيل الأدلة الرقمية .إذ أمر وكيل الجمهورية لدى محكمة سيدي محمد بفتح تحقيق ابتدائي في هذه العمليات، مكلفًا به مصالح الضبطية القضائية المختصة بمكافحة الجرائم السيبرانية والمعلوماتية .ورغم خطورة القضية، لم يتم الإعلان عن نتائج التحقيق،[2] ما يعكس التحديات التقنية والقانونية التي تواجهها الجزائر في تتبع هذا النوع من الجرائم ذات الطبيعة العابرة للحدود.

الجدول رقم (06): تطوير الكفاءات التقنية لمكافحة الجريمة الإلكترونية (2024).

الدول	تطوير الكفاءات
استراليا	19,44
اليابان	19,07
الو م أ	19,86
فرنسا	20
الجزائر	13,91

المصدر: الاتحاد الدولي للاتصالات (ITU) .

يوضح الجدول أن الجزائر تعاني من ضعف ملحوظ في تطوير الكفاءات التقنية لمكافحة الجريمة الإلكترونية، حيث سجلت 13.91 نقطة فقط، مقارنةً بالدول الأخرى مثل فرنسا والولايات المتحدة واليابان

[1] فتيحة حيمر، "الجرائم المعلوماتية في الجزائر: المواجهة والتحدي"، **مجلة الحقوق والعلوم السياسية** ، المجلد 12 العدد 01، جانفي 2025، ص 281.

[2] محمد مسلم، **"تحذيرات من الاختراق والتجسس على هواتف الجزائريين"**، الشروق أونلاين، 24 جانفي 2022، الرابط : https://www.echoroukonline.com/%D8%AA%D8%AD%D8%B0%D9%8A%D8%B1%D8%A7%D8%AA-%D9%85%D9%86-%D8%A7%D9%84%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D9%88%D8%A7%D9%84%D8%AA%D8%AC%D8%B3%D8%B3-%D8%B9%D9%84%D9%89-%D9%87%D9%88%D8%A7%D8%AA%D9%81#google_vignette، اطلع عليه بتاريخ: 16 ماي 2025، الساعة 12:00.

وأستراليا التي تتراوح نقاطها بين 19 و20 نقطة. هذا الفارق يشير إلى نقص الخبرات والمعرفة التقنية اللازمة لدى الجهات المختصة، مما يحد من قدرة الجزائر على مواجهة الجرائم الإلكترونية بفعالية.

5. عزوف الضحايا والمؤسسات عن الإبلاغ.

يُعد تردد الضحايا والمؤسسات في التبليغ عن الجرائم الإلكترونية من أبرز العوامل التي تعيق جهود مكافحتها، إذ غالبًا ما يُحجم الأفراد عن تقديم الشكاوى أو يتأخرون في ذلك بسبب جهلهم بحقوقهم القانونية، أو خشيتهم من العواقب الاجتماعية والقانونية المحتملة. وتظهر هذه الإشكالية بشكل أكثر وضوحًا في القطاع المالي، حيث تتجنب البنوك والمؤسسات المماثلة الإبلاغ عن هذه الجرائم خشية المساس بثقة المتعاملين والإضرار بسمعتها التجارية، وهو ما يساهم في تفاقم الظاهرة وصعوبة مواجهتها بفعالية.[1]

6. ضعف التنسيق مع الدول.

تواجه الجزائر، على غرار العديد من الدول، تحديًا كبيرًا يتمثل في غياب التنسيق الدولي الفعّال في مجال مكافحة الجريمة الإلكترونية. إذ أن الطبيعة العابرة للحدود لهذه الجرائم تُمكّن مرتكبيها من استغلال الفوارق القانونية والتقنية بين الدول، مما يُصعّب على السلطات الجزائرية تتبع المجرمين أو جمع الأدلة الرقمية اللازمة، خاصة عندما تكون مخزّنة أو معالَجة في دول أجنبية. وتزداد هذه الصعوبات في ظل التفاوت الكبير في مستويات الجاهزية القانونية والتقنية بين الجزائر والدول الأخرى، إضافة إلى محدودية اتفاقيات التعاون القضائي والأمني الدولي، وهو ما يضعف قدرتها على التصدي الفعّال لهذا النوع من التهديدات السيبرانية.[2]

---

[1] فتيحة حيمر، مرجع سبق ذكره، ص 281.

[2] بارة سمير، **الدفاع الوطني والسياسات الوطنية لألمن السيبراني (Security Cyper) في الجزائر: الدور والتحديات** ، ص 439، الرابط: https://dspace.univ-ouargla.dz/jspui/bitstream/123456789/14049/1/%D8%AF-%D8%A8%D8%A7%D8%B1%D8%A9_%D8%B3%D9%85%D9%8A%D8%B1.pdf ، أطلع عليه بتاريخ: 10 ماي 2025، الساعة 20:02 .

جدول 07: التدابير التعاونية الدولية في مجال الأمن السيبراني (2024).

الدول	التدابير التعاون
استراليا	18,85
اليابان	18,91
الو م أ	20
فرنسا	20
الجزائر	13,19

المصدر: الاتحاد الدولي للاتصالات (ITU)

يوضح الجدول أن الجزائر تواجه تحديًا ملموسًا في مجال التنسيق الدولي لمكافحة الجريمة الإلكترونية، حيث حصلت على 13.19 نقطة، وهي أدنى بكثير مقارنة بالدول الأخرى مثل الولايات المتحدة وفرنسا التي سجلت 20 نقطة، واليابان وأستراليا بنقاط تقارب 19. هذا الفارق يعكس ضعف اتفاقيات التعاون القضائي والأمني الدولي، وكذلك الفجوة في الجاهزية القانونية والتقنية، مما يعرقل قدرة الجزائر على متابعة الجرائم الإلكترونية العابرة للحدود وجمع الأدلة الرقمية اللازمة لملاحقة المجرمين بفعالية.

الفرع الثاني: انعكاسات الجريمة الإلكترونية على الأمن السيبراني في الجزائر

أصبحت الجريمة الإلكترونية في الجزائر تمثل تهديدًا فعليًا للاستقرار الرقمي، بفعل تصاعد حجم الهجمات وتطور أساليبها في ظل بيئة رقمية تعاني من ضعف التأمين والتشريعات المواكبة. إذ لم تعد آثار هذه الجرائم تقتصر على الخسائر التقنية، بل امتدت لتشمل أبعادًا اقتصادية حساسة، وأخرى سياسية وأمنية بالغة الخطورة. ويتجلى ذلك في تزايد الخسائر المالية، تراجع ثقة المستثمرين، وتعرض البنية التحتية الحيوية للاختراق، فضلًا عن انعكاسات سلبية على صورة الدولة وعلاقاتها الدولية. انطلاقًا من ذلك، يتناول هذا الفرع أبرز الانعكاسات الاقتصادية والسياسية والأمنية للجريمة الإلكترونية على الأمن السيبراني في الجزائر، بالاستناد إلى بيانات وإحصائيات حديثة تكشف حجم التحدي وعمق تأثيره.

أولا: الانعكاسات الالقتصادية.

1- الخسائر المالية.

تشكل الجرائم الإلكترونية تهديدًا بالغ الخطورة على الاقتصاد الوطني في الجزائر، حيث تظهر الأرقام العالمية والمحلية حجم الخسائر المالية والآثار السلبية لهذه الظاهرة. وفقًا لتقرير مكتب التحقيقات الفيدرالي **(FBI)** لعام 2024، بلغت الخسائر المالية العالمية الناجمة عن الجرائم الإلكترونية حوالي 16.6 مليار دولار أمريكي،[1] مما يعكس تزايدًا ملحوظًا في حجم هذه الظاهرة وتأثيرها الخطير على الاقتصاد العالمي. وفي هذا السياق، تحتل الجزائر المرتبة الرابعة عالميًا من حيث التعرض لمخاطر الجريمة الإلكترونية،[2] مما يشير إلى أنها من بين أكثر الدول استهدافًا من قبل شبكات الجرائم الرقمية الأمر الذي يتوقع معه تكبدها خسائر مالية معتبرة رغم غياب إحصائيات دقيقة على المستوى المحلي.

2- ضعف ثقة المستثمرين.

تؤدي الهجمات السيبرانية إلى انخفاض ثقة المستثمرين، حيث تبين الدراسات أن الهجمات التي تؤدي إلى تسريب أو فقدان بيانات مالية حساسة تسبب خسارة مباشرة في ثروة المساهمين بنسبة تصل إلى 1.09%. [3] يشمل هذا التأثير مختلف القطاعات في الجزائر، حيث تتآكل ثقة المواطنين في المؤسسات الحكومية والخاصة، مما يؤدي إلى انخفاض التعاملات الإلكترونية وتراجع جاذبية السوق الوطنية للاستثمار الأجنبي. وقد انعكس هذا الضعف في الجاهزية الرقمية للجزائر في تراجعها إلى المرتبة 116

[1] FBI, **"The FBI Released Its Internet Crime Report 2024"** , Federal Bureau of Investigation, April 16 2024, , available at: https://www.fbi.gov/contact-us/field-offices/atlanta/news/the-fbi-released-its-internet-crime-report-2024, Accessed in : May 12 2025,at 22:00.

[2] MixMode, Ibid.

[3] موسى عمرو عادل عبد الفتاح، "قياس تأثير الإفصاح عن مخاطر الإنترنت على تكاليف رأس المال المقترض والمال المملوك: دراسة تطبيقي"، **مجلة الدراسات المالية والإدارية**، المجلد 16، العدد 04، ديسمبر 2024، ص 424، الرابط : https://masf.journals.ekb.eg/article_396234_4d460fe7842005bfb947b81b9758dec1.pdf أطلع عليه في 13 ماي 2025، الساعة 23:00.

عالميًا في مؤشر تنمية الحكومة الإلكترونية **(EGDI)** لعام 2024،[1] مما يؤكد محدودية القدرات الوطنية في تأمين بيئة رقمية موثوقة.

3- تهديد البنية التحتية الرقمية ونمو الاقتصاد.

تتزايد التهديدات على البنية التحتية الرقمية في الجزائر، خصوصًا الحواسيب الصناعية **(ICS)** حيث أظهرت الإحصاءات أن 39.73% من هذه الحواسيب تعرضت لهجمات برمجيات خبيثة منذ بداية عام 2025، مما يعكس حجم الأضرار التي تلحق بالبنية التحتية الحيوية التي تدعم العديد من القطاعات الاقتصادية. تعد الإنترنت المصدر الرئيسي للهجمات بنسبة 20.23% تليها الوسائط القابلة للإزالة بنسبة 5.22%، وبرامج البريد الإلكتروني 1.76%والمجلدات الشبكية المشتركة بنسبة 0.11% تزيد هذه الهجمات من التكاليف التشغيلية للمؤسسات وتؤدي إلى تعطيل الخدمات الحيوية، [2] مما يعرقل النمو الاقتصادي المستدام ويزيد من التحديات التي تواجه التنمية الرقمية في البلاد.

4. فقدان الثقة في المعاملات الرقمية.

تعكس حملات الاحتيال الإلكتروني الأخيرة، مثل تلك التي استهدفت مستخدمي تطبيق "بريدي موب" التابع لبريد الجزائر، [3] هشاشة الوعي الرقمي لدى المواطنين، حيث استخدم المهاجمون أساليب خداع اجتماعي متقدمة لسرقة بياناتهم الحساسة. لا يقتصر تأثير هذه الهجمات على الأفراد فقط، بل يمتد

---

[1] United Nations **, "E-Government Survey 2024",** Department of Economic and Social Affairs, United Nations. Published in **2024**, available at:
https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf, accessed in : May 13 2025**,** at :20 :00.

[2] Kaspersky ICS CERT**, "Statistics",** Published by AO Kaspersky Lab in 2025**,** available at: https://ics-cert.kaspersky.com/statistics/ ,accessed in : May 13 2025**,** at : 22 :00**.**

[3] **حماية المستهلك تحذّر مستخدمي "بريدي موب" من الاحتيال**، جريدة الإخبارية الجزائرية ، الرابط:
https://elikhbaria.dz/%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B3%D8%AA%D9%87%D9%84%D9%83-%D8%AA%D8%AD%D8%B0%D8%B1-%D9%85%D8%B3%D8%AA%D8%AE%D8%AF%D9%85%D9%8A-%D8%A8%D8%B1%D9%8A%D8%AF%D9%8A-%D9%85%D9%88/ اطلع عليه بتاريخ: 13 ماي 2025 ، الساعة 10:00.

ليؤثر على ثقة المجتمع في المعاملات الرقمية، مما يحد من انتشار الخدمات الإلكترونية ويعرقل التحول الرقمي.

ثانيا: التأثير السياسي والأمني للجريمة الإلكترونية في الجزائر

1. تهديد الأمن الوطني واستقرار الدولة

تُعد الهجمات السيبرانية، خصوصًا هجمات حجب الخدمة **(DDoS)** ، من أبرز التهديدات التي تواجه الأمن الوطني الجزائري. حيث سُجلت 205 هجمة ضد قطاع الاتصالات السلكية بلغت ذروتها بسرعة 71.93 جيجابايت في الثانية، ما يهدد بشلّ البنية التحتية الحيوية للدولة ويقوض قدرتها على إدارة الأزمات الأمنية.[1] كما يعكس تصنيف الجزائر المتدني في مؤشر الأمن السيبراني (درجة 33.95) ضعف القدرات الوطنية في صدّ الهجمات الإلكترونية،[2] مما يجعل المؤسسات السيادية هدفًا سهلاً لهجمات تجسسية معقدة، مثل تلك التي استهدفت وكالة الأنباء الجزائرية من جهات دولية معروفة.[3]

2. تشويه صورة الدولة وتهديد العلاقات الدولية.

تكرار الاختراقات الإلكترونية الناجحة لمؤسسات حكومية جزائرية ينعكس سلبًا على صورة الدولة داخليًا وخارجيًا. فقد كشفت تقارير دولية عن استهداف أرقام هواتف جزائرية ببرامج تجسس متطورة مثل "بيغاسوس"، [4] مما أضعف من مصداقية الجزائر في حماية البيانات الشخصية لمواطنيها. هذا الوضع لا

---

[1] NETSCOUT Systems, Inc, **"Algeria - Latest Cyber Threat Intelligence Report,"** NETSCOUT DDoS Threat Intelligence Report, published for July–December 2024 available at: https://www.netscout.com/threatreport/emea/algeria/, accessed in: May 13, 2025, at 23:20

[2] MixMode Threat Research, **"Global Cybercrime Report 2024: Which Countries Face theHighest Risk?"** MixMode, May 8 2024, , https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/. accessed May 13, 2025,at 22:20

[3] **"الحرب السيبرانية تتصاعد ضد الجزائر"**، جريدة الإخبارية ، 15فيفري 2023، الرابط: https://elikhbaria.dz/الحرب-السيبرانية-تتصاعد-ضد-الجزائر/ ، اطلع عليه بتاريخ 13ماي 2025، الساعة 14:40.

[4] محمد مسلم، **"تحذيرات من الاختراق والتجسس على هواتف الجزائريين"**، الشروق أونلاين، 24 جانفي 2022، الرابط : https://www.echoroukonline.com/%D8%AA%D8%AD%D8%B0%D9%8A%D8%B1%D8%A7%D8%AA-%D9%85%D9%86-%D8%A7%D9%84%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D9%88%D8%A7%D9%84%D8%AA%D8%AC%D8%B3%D8%B3-%D8%B9%D9%84%D9%89-%D9%87%D9%88%D8%A7%D8%AA%D9%81#google_vignette اطلع عليه بتاريخ: 16 ماي 2025، الساعة 23:00.

يقتصر على تهديد الأمن السيبراني فحسب، بل يفتح المجال لتوترات دبلوماسية ومخاطر جيوسياسية قد تعقد علاقات الجزائر مع شركائها الدوليين، في ظل بيئة رقمية تفتقر لمقومات الحماية الفعالة.

المبحث الثاني: الاستراتيجية الجزائرية لمكافحة الجريمة الإلكترونية وتحقيق الأمن السيبراني.

تعد الجريمة الإلكترونية في الجزائر ظاهرة متنامية تواكب التطور الحاصل في المجتمع، مما زاد قلق المجتمع والدولة وقد واجهت الجزائر تحديات كبيرة في ظل هذا التطور ولمحاربتها بشتى الطرق القانونية. وفي هذا السياق سارع المشرع الجزائري كغيره من المشرعين إلى التصدي الجريمة الإلكترونية وسن نصوص قانونية وقيامه بتعديلات وفقا للتطورات الحاصلة، وإنشاء مؤسسات وهيئات أمنية التي تهدف إلى تعزيز الأمن السيبيراني وعليه قمنا بدراسة في هذا **(المبحث الثاني)** الذي قسمناه إلى ثلاث مطالب في **(المطلب الأول)** خصصناه لمكافحة الجريمة الإلكترونية في التشريع الجزائري أما **(المطلب الثاني)** تطرقنا إلى الآليات الأمنية لمكافحة الجريمة الإلكترونية وضمان الأمن السيبيراني، أما بالنسبة **(المطلب الثالث)** الآليات الإدارية المختصة لمكافحة الجريمة الإلكترونية وضمان الأمن السيبيراني.

المطلب الأول: مكافحة الجريمة الإلكترونية في التشريع الجزائري.

لقد سعى المشرع الجزائري إلى مكافحة الجريمة الإلكترونية عبر قوانين عامة وقوانين خاصة كما أنه قام بتعديل القوانين تبعا للتطورات المستمرة لهذه الجريمة قصد محاربتها والحد من انتشارها والحفاظ على أمن واستقرار المجتمع والدولة ككل. وعليه قمنا في هذا المطلب الذي قسمناه إلى فرعين **(الفرع الأول)** مكافحة الجريمة الإلكترونية بموجب القوانين العامة أما **(الفرع الثاني)** تطرقنا إلى مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة.

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب القوانين العامة.

في ظل الطابع المستحدث والمعقد للجريمة الإلكترونية، لم تكن المنظومة القانونية الجزائرية في البداية مزوّدة بنصوص خاصة ومباشرة لمواجهتها، مما دفع بالمشرّع إلى الاستناد على القوانين العامة وفي مقدمتها الدستور والقانون المدني، كأساس لحماية الأفراد وحقوقهم في الفضاء الرقمي. ورغم أن هذه القوانين لم توضع خصيصًا لمكافحة الجريمة الإلكترونية، إلا أنها تضم مبادئ وأحكامًا يمكن تكييفها قانونيًا للتصدي للاعتداءات الإلكترونية، لاسيما تلك التي تمس الحياة الخاصة وحرمة الأشخاص.

وبذلك، يهدف هذا الفرع إلى إبراز كيف ساهم الدستور، من خلال تكريسه للحقوق الأساسية وحماية الخصوصية، والقانون المدني، من خلال قواعد المسؤولية عن الأفعال الضارة، في بناء أرضية قانونية لمواجهة الجريمة الإلكترونية، وذلك في انتظار تطوير تشريعات أكثر تخصصًا ومواكبة للتحديات الرقمية الراهنة.

أولا: مكافحة الجريمة الإلكترونية بواسطة الدستور.

بموجب الدستور الجزائري لقد كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل لسنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان.[1] وقد تم تجسيد هذه المبادئ الدستورية على شكل نصوص قانونية جاءت في قانون العقوبات وقانون الإجراءات الجزائية وبعض القوانين الخاصة والتي تمنع أي اعتداء على هذه

كما ان دستور 2020 جاء وأكد عليها وقد وردت أهم المبادئ الدستورية نجد ما نصت عليهم المواد:

المادة 47" **لكل شخص الحق في حماية حياته الخاصة وشرفه، ولكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت**". [2] وعليه لا يمكن المساس بالحقوق المذكورة مع ضمان حماية خصوصية الأشخاص عند معالجة البيانات التي لها طابع شخصي.

كما نصت المادة 55 " **يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والحصول عليها وتداولها. لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم وبالمصالح المشروعة للمؤسسات وبمقتضيات الأمن الوطني.**" يحدد القانون كيفيات ممارسة هذا الحق.[3]

وعليه فإن الدستور يكفل الحقوق ويضمن للأشخاص عدم انتهاك خصوصية معلوماتهم الشخصية بأي شكل من الأشكال.

[1] اسمهان بوضياف، مرجع سبق ذكره، ص 361.

[2] المادة 47 من الفصل الأول تحت عنوان الحقوق والحريات العامة، من دستور 2020، المؤرخ في 30 ديسمبر 2020، ج. ر، العدد 82، 2020.

[3] المادة 55 من الفصل الأول تحت عنوان الحقوق والحريات العامة، من دستور2020، المؤرخ في 30 ديسمبر 2020، ج. ر، العدد 82، 2020.

ثانيا: مكافحة الجريمة الإلكترونية بموجب القانون المدني.

انطلاقا من الأهمية الدستورية لحماية حرمة الحياة الخاصة للأفراد، بادر المشرع إلى تجريم كل اعتداء غير مشروع على الحقوق الملازمة لشخصية الفرد فقد نصت المادة 124 من القانون المدني على أن" **كل فعل أيا كان يرتكبه الشخص بخطئه، ويسبب ضررا يلزم من كان سببا في حدوثه بالتعويض.**"[1]

من خلال هذه المادة نستنتج أن هذه المادة وردت شاملة وعامة على أي حق من الحقوق الشخصية للفرد كما تلزم على الشخص الذي كان سببا في الضرر، على دفع تعويضات للضحية عما لحقه من ضرر وأذى باعتبار ان الفعل الضار عليه تقوم المسؤولية وهو ركن الضروري والأساسي لرفع الدعوى القضائية عن الاعتداء الإلكتروني الذي يمس بالحياة الخاصة الذي يرتكب بواسطة شبكة الأنترنت ومختلف وسائلها.

الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة.

تماشيًا مع تطور الجريمة الإلكترونية وتعقيدها، سعى المشرع الجزائري إلى سن قوانين خاصة تتلاءم مع طبيعتها التقنية. فإلى جانب تعديل قانون العقوبات وقانون الإجراءات الجزائية، تم إصدار قانون خاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، إضافة إلى قوانين داعمة مثل قانون الملكية الأدبية والفنية وقانون الموصلات السلكية واللاسلكية، ما يعكس توجهًا تشريعيًا شاملًا يجمع بين التجريم، الوقاية، والإجراءات الخاصة بالتحري والمتابعة.

أولا: مكافحة الجريمة الإلكترونية في قانون العقوبات.

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية، من أشكال جديدة للإجرام التي لم تشهدها البشرية من قبل مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-155.[2] المتضمن قانون العقوبات بحيث أفرز لها القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي تضمن 08 مواد من (المادة 394 مكرر مكرر7).

[1] القانون 05-10 المؤرخ في20 يونيو2005 ، المتعلق بالقانون المدني، ج. ر، العدد 44، 2005.

[2] حنان مسكين، "واقع مكافحة الجريمة المعلوماتية واتجاهاتها التشريعية في الجزائر"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 04، العدد 01، مارس 2020، ص 619.

نصت المادة 394 مكرر من القانون 24-06 مؤرخ في 28 أبريل 2024 الذي يعدل ويتمم الأمر 66-155 المتضمن قانون العقوبات على أن" **يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة مالية من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الإلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.**"[1] فعند قراءة وتحليل نصوص المواد يتضح لنا أن المشرع خصص في كل مادة نوع من الجرائم وقسمها إلى طوائف:

- **الطائفة الأولى:** وتتضمن جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات،[2] هذا ما جاءت به المادة 394 مكرر1 من القانون 24-06.
- **الطائفة الثانية:** تخص الجرائم الإلكترونية عن طريق حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم وكذلك بحث أو تخزين معطيات هذا ما نصت عليه المادة 394 مكرر2 من القانون 24-06.
- **الطائفة الثالثة:** الجرائم الإلكترونية التي تمس الدولة وأمنها والهيئات والمؤسسات الخاضعة للقانون العام هذا ما نصت عليه المادة394 مكرر3 من القانون 24-06.
- **الطائفة الرابعة:** الجرائم الإلكترونية التي تخص الشخص المعنوي هذا ما نصت عليه المادة 394 مكرر4 من القانون 24-06، كما يلاحظ بأن الغرامة بالنسبة للشخص المعنوي تعادل خمس أضعاف العقوبة المقررة للشخص الطبيعي.
- **الطائفة الخامسة:** التي تخص جريمة تكوين مجموعة أشخاص تختص في الجرائم الماسة بأنظمة المعالجة الآلية طبقا لما نصت عليه المادة394 مكرر5 من قانون 24-06.

[1] المادة 394 من القانون رقم 06-24 المؤرخ في 28 أبريل 2024، الذي يعدل ويتمم الأمر 66-155، المتعلق بقانون العقوبات، ج. ر، العدد 30، 2024.

[2] الطاهر ياكر، مرجع سبق ذكره، ص 45.

أما بالنسبة للمادة 394 مكرر6 فهي نصت على العقوبات التكميلية، و المادة 394 مكرر7 نصت على العقاب على الشروع في جريمة إلكترونية. فالمشرع الجزائري حاول جاهدا للإحاطة بجميع أنواع الجريمة الإلكترونية عن طريق فرض عقوبات صارمة سواء تخص الشخص الطبيعي أو المعنوي.

ثانيا: مكافحة الجريمة الإلكترونية بموجب قانون الإجراءات الجزائية.

في إطار العمل والسعي على استكمال، ومباشرة السياسة الجنائية الخاصة لمكافحة الجرائم الإلكترونية في شقها الإجرائي كان لزاما على المشرع الجزائري أن يعدل قانون الإجراءات الجزائية، وذلك بغية استحداث إجراءات جديدة تتوافق مع الطبيعة الخاص للجرائم الإلكترونية.[1] وقد تم ذلك من خلال القانون رقم 06-22 المؤرخ في 20-12-2006 يعدل ويتمم قانون الإجراءات الجزائية، حيث نص فيه على جملة من الإجراءات المستحدثة وذلك في الفصل الرابع تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وهذا ما نصت عليه المادة 65 مكرر5:" **إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال .... يجوز لوكيل الجمهورية المختص أن يأذن بما يلي: اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية. وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص.... تنفد العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص. في حالة فتح تحقيق قضائي تتم العمليات المذكورة بناءا على إذن من قاضي التحقيق وتحت مراقبته المباشرة."**[2]

قد جاء في الفصل الخامس من هذا القانون تحت تسمية "في التسرب" ونصت عليها المادة 65 مكرر 11 والمادة 65 مكرر18 وهي إجراءات جديدة تسمح لضباط الشرطة القضائية من ممارسة سلطات التحري والبحث والكشف عن المجرم في البيئة الافتراضية نظرا لطبيعتها الخاصة والمعقدة.

[1] عفيف بن عبو، "الآليات القانونية في الجزائر وتطورها في مكافحة الجريمة الإلكترونية"، **مجلة حقوق الإنسان والحريات العامة**، المجلد 09، العدد01، جوان 2024، ص 32.

[2] المادة 65 مكرر 5 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، الذي يعدل ويتمم الأمر 06-155، المتضمن قانون الإجراءات الجزائية، ج. ر، العدد 84، 2006.

يدرك المشرع الجزائري أن التصدي الفعال للجرائم الإلكترونية لا يقتصر على وضع أحكام موضوعية ذات طابع ردعي فقط، بل لا بد من مرافقتها بأحكام إجرائية وقائية وتحفظية تسهم في منع وقوع هذه الجرائم او على الأقل الكشف عنها في وقت أبكر ما يسمح بتدارك مخاطرها.[1] وهذا ما قام به المشرع من خلال إدراج تدابير إجرائية مستحدثة تتناسب مع طبيعة الجرائم الإلكترونية.

ثالثا: التعديلات على بعض القوانين الخاصة لمواجهة التطورات المستجدة في مجال الجرائم الإلكترونية.

1. القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها رقم 09-04.

تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تمسح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم كل الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة.[2]

يتميز هذا القانون بكون أن المشرع الجزائري قام باستحداث إجراءات جديدة في إطار مكافحة الجريمة الإلكترونية، والتي تتمثل في إجراءات وقائية وتدابير أحرى مكملة لتلك الإجراءات التي جاء بها قانون الإجراءات الجزائية. فعند استقرائنا لهذا القانون نلاحظ أن المشرع قسمه إلى ستة فصول، فالفصل الأول خصصه للأحكام العامة والهدف الذي جاء به هذا القانون ذلك حسب ما نصت به المادة الأولى منه، والمادة الثانية التي نصت على التفريق بين بعض المصطلحات المشابهة، والمادة الثالثة التي خصصت لمجال التطبيق.

أما بالنسبة للفصل الثاني فقد حدد الحالات التي يسمح بها بإجراء مراقبة الاتصالات الإلكترونية في جرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة أو في حالو توفر معلومة حول أن هناك اعتداء على منظومة معلوماتية هذا ما نصت عليه المادة الرابعة. والفصل الثالث الذي تناول القواعد الإجرائية التي تخص التفتيش والحجز في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وفي الفصل الرابع الذي خصصه لتحديد الالتزامات التي تقع على مقدمي الخدمات. ثم الفصل الخامس الذي أكد على ضرورة

[1] أسماء بن لعربي ومديحة الفحلة، "مكافحة الجريمة الإلكترونية في الجزائر: رؤية تشريعية واستراتيجيات عملية"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 09، العدد 01، مارس 2025، ص 1246.

[2] فاروق خلف، "الآليات القانونية لمكافحة الجريمة المعلوماتية"، **مجلة الحقوق والحريات**، العدد 02، 2015، ص 18.

إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أما الفصل السادس فقد نص على التعاون والمساعدة القضائية الدولية بخصوص مكافحة هذه الجرائم وتبادل المعلومات.

يستنتج في الأخير أن أحكام القانون رقم 09-04 جاءت عامة ومطلقة في مكافحة الجرائم المتصلة بتكنولوجية الإعلام والاتصال، بحيث تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال ويطبق على كافة التكنولوجيات القديمة والجديدة بما فيها شبكة الانترنت وعلى أي تقنية يمكن أن تظهر مستقبلا.[1] هذا ما يجعل من القانون ساريا مع للتطورات التكنولوجية.

2. الحماية من خلال قانون الملكية الأدبية والفنية.

الهدف من وضع قوانين الملكية الفكرية هو حماية حق الإنسان في التفكير والإبداع والابتكار الذي يعد بمثابة العامل الأساسي لتقدم المجتمعات وتطورها، ولما كانت مكونات الحاسب الآلي بمثابة العامل الأساسي لتقدم المجتمعات وتطورها كان لزوما على المشرع اشتمال هذه المكونات بالحماية المقررة في قانون الملكية الفكرية.[2]

اتجه المشرع الجزائري إلى حماية الملكية الفكرية للغير وذلك من خلال قانون الملكية الأدبية والفنية والمتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05 المؤرخ في 19جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة.[3] وقام بموجب هذا الأمر في توسيع في قائمة المصنفات حيث أدمج برامج ومصنفات معلوماتية كما شدد في العقوبات التي تضر وتمس بالمؤلفين خاصة تلك المصنفات التي تكون محمية وشملتها الحماية.

3. الحماية المتعلقة بالموصلات السلكية واللاسلكية.

لقد تضمن الفصل الثاني من الباب الرابع من القانون رقم 2000-03 المؤرخ في 6 أوت 2000 والمتعلق بالقواعد العامة المتعلقة بالبريد والموصلات السلكية واللاسلكية، والذي جاء في هذا الفصل الأحكام الجزائية التي ترتب في حالة مخالفة القانون حيث نصت المادة 127 من القانون 2000-03: **"تطبق العقوبات المنصوص عليها في المادة 137 من قانون العقوبات على كل شخص مرخص له**

[1] حنان مسكين، مرجع سبق ذكره، ص 622.

[2] راضية عمور، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 06 ، العدد 01 ، مارس 2022، ص 103.

[3] الأمر 03-05، المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج. ر، العدد 44، 2003.

بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه والذي في إطار ممارسة مهامه يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال."[1]

المطلب الثاني: الآليات الأمنية لمكافحة الجريمة الإلكترونية وضمان الأمن السيبيراني.

تعد التدابير التنظيمية والهيكلية العنصر الأساسي في نجاح الاستراتيجيات التي تعتمدها الدول في مجال مكافحة الجرائم الإلكترونية، ويتحقق ذلك من خلال استحداث هياكل وطنية مختصة في هذه الجرائم وفقط. وفي هذا السياق تبنت الجزائر استراتيجية حيث انها أنشت هيئات ومؤسسات لها طابع خاص والتي يكون هدفها الحفاظ على أمن المعلومات وحماية الشبكات وطنيا، حيث أنها تلعب دورا محوريا في حماية المجتمع وتعزيز الأمن السيبراني، وهذا ما يعزز من قدرات الدولة على التصدي لمختلف الجرائم الإلكترونية. ومن بين استراتيجية التي اعتمدتها الجزائر هي إنشاء هيئات أمنية وعليه قمنا في هذا **(المطلب الثاني)** بدراسة الآليات الأمنية المعتمدة لمكافحة الجريمة الإلكترونية وضمان الأمن السيبيراني، وقسمنا هذا المطلب إلى ثلاث فروع في **(الفرع الأول)** تطرقنا إلى المصلحة المركزية لمكافحة الإجرام السيبيراني للدرك الوطني. أما **(الفرع الثاني)** المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، وفي **(الفرع الثالث)** المصلحة المركزية لمكافحة الجريمة الإلكترونية التابعة للأمن الوطني (SCLC) أما في **(فالفرع الرابع)** المنظومة الوطنية لأمن المعلوماتية الموضوعة لدى وزارة الدفاع الوطني.

الفرع الأول: المصلحة المركزية لمكافحة الإجرام السيبيراني للدرك الوطني.

كانت بداية هذه الهيئة في سنة 2008 ويتواجد مقرها في بئر مراد رايس، ولقد أنشأت هذه المصلحة في البداية تحت تسمية مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية بموجب قرار وزاري سنة 2018، يهدف المركز إلى تحليل معطيات وبيانات الجرائم المعلوماتية وتحديد هوية أصحابها لها امتداد وطني من خلال محققي الجرائم تكنولوجيا الإعلام والاتصال عبر المجموعات الإقليمية.[2] كما

[1] المادة 127 من القانون رقم 2000- 03، المؤرخ في 5 أوت 2000، المتعلق بالقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج. ر، العدد 48، 2000.

[2] سيد علي بدرين، "استراتيجية الجزائر لمواجهة التهديدات السيبرانية"، **مجلة الشرطة**، المديرية العامة للشرطة الجزائرية، العدد 156، أكتوبر 2023، ص 51.

يسعى إلى حماية الانظمة المعلوماتية خصوصا تلك المستخدمة في البنوك والمؤسسات الحكومية والتي تخص الأفراد.

كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، وقد تمكنت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها وكذا من خلال الملتقيات ذات الطابع الوطني والدولي وتبادل الخبرات مع دول أخرى، أنه توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي ورجال القانون وذلك ما أجل التفهم الصحيح للجريمة المعلوماتية والتصدي لها.[1]

من بين مهامها أيضا ضمان المراقبة الدائمة والمستمرة على شبكة الأنترنت، القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية، مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة المشاركة في عمليات التحري والتسرب عبر شبكة الإنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.[2] كما لها دور فعال مكافحة وقمع الجرائم الإلكترونية وتجسيد داخل الفضاء السيبراني وذلك بتعاونها مع مصالح الأمن الوطني ومختلف الهيئات.

الفرع الثاني: المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني

بمقتضى المرسوم الرئاسي رقم 04-183 المؤرخ 26 يونيو 2004 الذي يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، **وحسب ما نصت المادة الثانية منه على:" المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ويوضع تحت وصاية وزير الدفاع الوطني ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه وبهذه الصفة فإنه يخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية."**[3]

---

[1] سميحة بلقاسم وحميد بوشوشه، "الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابهتها"، **مجلة العلوم الإنسانية** المجلد 10، العدد 01، جوان2023، ص 552.

[2] سعاد رابح، "ضوابط مكافحة الجريمة المعلوماتية"، **مجلة القانون العام الجزائري والمقارن**، جامعة جيلالي ليابس بسيدي بلعباس، المجلد 07، العدد 01، جوان 2021، ص 281.

[3] المادة 2 من المرسوم الرئاسي رقم 04-183، المؤرخ في 26 يونيو 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج. ر، العدد 41، 2004.

يقع مقره في مدينة الجزائر بالتحديد ببوشاوي كما يمكن ذلك نقله إلى أي مكان في التراب الوطني وذلك بقرار كم وزير الدفاع الوطني. يتولى مهام رئاسة المعهد ضابط سامي من الدرك الوطني والتي يتم تعيينه بموجب مرسوم رئاسي وذلك بناء على اقتراح من وزير الدفاع الوطني، وعند إنهاء مهامه كذلك تنهى بموجب مرسوم رئاسي، وحسب ما نصت عليه المادة 4 من المرسوم 04-183 التي حددت مهام المعهد حيث " يكلف المعهد بما يأتي:

- **إجراء بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، الخبرات والفحوص العلمية التي تخضع للاختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.**
- **تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة.**
- **المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.**
- **تصميم بنوك معطيات وإنجازها طبقا للقانون، بما في ذلك تلك الخاصة بالبصمات الجينية التي ستكون في متناول المحققين والقضاة بغرض وضع المقاربات...**
- **المشاركة بصفته هيئة تضمن الفحوص والخبرات في مجال علم الإجرام، في تحديد سياسة جنائية مثلى لمكافحة الإجرام.**
- **المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة.**
- **المشاركة في كل الملتقيات والمحاضرات أو الندوات، على الصعيدين الوطني والدولي.**
- **... المشاركة في تنظيم دورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية...."[1].**

كما يحتوي هذا المعهد على عدة مخابر التي تكون جهات قضائية فضلا عن اضطلاعها بنشاطات علمية في مجال البحث العلمي، وتقديم المساعدة للمحققين في مجال التحري عن الجرائم

[1] المادة 4 من المرسوم الرئاسي رقم 04-183، المؤرخ في 26 يونيو 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج. ر، العدد 41، 2004.

ويتكون المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني من 11 دائرة متخصصة في مجالات مختلفة.[1]

فنظرا للتطورات المستمرة للجريمة وتعدد أشكالها المستجدة، بات من الضروري على أجهزة الأمن من تطوير أساليب عملها بالاعتماد على التقنيات التكنولوجية الحديثة خصوصا في مجال التحري والبحث عن الأدلة والكشف على هوية الجناة وتحديد أماكنهم، وهذا ما فرض على المعهد ضرورة مواكبة التطور من خلال ربط العلوم الجنائية النظرية بالتطبيقات العلمية الحديثة. ولهذا تسعى دائرة الإعلام الآلي للمعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني لتحقيق هذا المسعى.

فالدرك الوطني يعمل سواء من مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية أو من خلال المعهد الوطني للأدلة الجنائية وعلم الإجرام، على ترقية أداء وحداته ويتخذ كل التدابير اللازمة من حيث التنظيم والتكوين واقتناء الوسائل والتجهيزات للرفع من مستوى وفعالية القيام بمهامه،[2] للتصدي لظاهرة الجريمة الإلكترونية التي تتطور باستمرار والتي تتخذ أشكال جديدة.

الفرع الثالث: المصلحة المركزية لمكافحة الجريمة الإلكترونية التابعة للأمن الوطني (SCLC) .

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية، التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية والتي كانت عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية.[3] ولقد أنشئت سنة2011 على مستوى المديرية العام للأمن الوطني، كما سعت المديرية إلى خلق وحدات متخصصة كل وحدة تعالج نوع معين من الجرائم. ولذلك قامت المديرية العامة للشرطة القضائية باستحداث أربع مصالح متخصصة في شكل نيابة مديرية وهي:

- **نيابة مديرية الشرطة العلمية.**

---

[1] دليلة العوفي، **آليات محاربة الجريمة المعلوماتية (دراسة حالة الجزائر2009-2006)**، أطروحة دكتوراه علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة ابراهيم سلطان شيبوط، الجزائر، 2020، ص323 ص 324.

[2] دليلة العوفي، مرجع سبق ذكره، ص 325

[3] إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، **مجلة مصداقية**، صادرة عن المدرسة العليا العسكرية للإعلام والاتصال، المجلد 01، العدد 01، سبتمبر 2019، ص 114.

- **نيابة مديرية الاقتصادية والمالية.**
- **نيابة القضايا الجنائية.**
- **مصلحة البحث والتحليل.**[1]

تتمثل الوحدات التابعة للسلك الأمن الوطني في المخبر المركزي للشرطة العلمية بالجزائر العاصمة ومخبرين جهويين للشرطة العلمية أحدهما بقسنطينة، والآخر بمدينة وهران وفي سبيل تقديم الدعم والمساعدة لمصالح الشرطة القضائية قامت المديرية العامة للأمن الوطني عام 2010 بإنشاء ما يقارب عن 23 خلية استعلام لمكافحة هذا النوع من الجرائم الفتاكة بأمن المعلومات وذلك على مستوى ولايات الشرق والغرب الوسط والجنوب.[2] وفي سنة 2016 بدأت على العمل لتعزيزها في كافة التراب الوطني يتولى كل مخبر مهام البحث وتحليل الأدلة الجنائية لكل مخبر دائرتين ويتم التحقيق في الجرائم الإلكترونية على مستوى الدائرة التقنية لكل مخبر.

تسعى هذه المديرية إلى مواجهة الجرائم الإلكترونية عبر عدة جوانب أساسية منها جانب التوعية والوقاية، وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الإلكترونية ودائما في إطار مكافحتها.[3] كذلك تقوم بعمليات التوعية والتحسيس عبر الفضاء السيبيراني كما يبزر دور المديرية العامة للأمن من خلال التعاون الدولي في مجال تبادل الخبرات والمعلومات وتقديم المساعدة القضائية.

الفرع الرابع: المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني.

[1] حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016، ص 177.

[2] فتيحة حيمر، الجرائم المعلوماتية في الجزائر: المواجهة والتحدي، **مجلة الحقوق والعلوم السياسة**، المجلد12، العدد 01، جانفي 2025، ص 274.

[3] عائشة فاضل،" المسؤولية الجزائية في الجرائم الإلكترونية(الجزائر نموذجا)"، **مجلة الحقوق والحريات**، المجلد11، العدد 01، أفريل 2023، ص638.

حاول المشرع الجزائري التدخل من جديد، وذلك من خلال استحداث آليات تحت رعاية وزارة سيادية وهي وزارة الدفاع الوطني كون قضايا الأمن السيبيراني تمس سيادة الدولة الجزائرية.[1] فحسب المادة 1 و2 من المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي2020 الذي يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، وقد نصت المادة 3 منه على: " **تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدو وزارة الدفاع الوطني ما يأتي:**

- **مجلس وطني لأمن الأنظمة المعلوماتية، يدعى في صلب النص "المجلس" ويكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها وتوجيهها.**
- **وكالة لأمن الأنظمة المعلوماتية تدعى في صلب النص "الوكالة" وتكلف بتنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية.**

ولممارسة مهامه يتوفر المجلس بالإضافة إلى الوكالة على هياكل متخصصة لوزارة الدفاع الوطني في هذا المجال."[2]

وبهذا هذه المنظومة تتشكل من هيئتين ولكل منها تشكيلة ومهام خاصة بها وهما:

- **المجلس الوطني لأمن الانظمة المعلوماتية:** يترأسها وزير الدفاع الوطني أو ممثله وحسب نص المادة 4 من المرسوم الرئاسي 20-05 تتمثل مهام المجلس فيما يلي: " **يتولى المجلس في إطار إعداد الاستراتيجية الوطنية في مجال أمن المعلوماتية على المهام الآتية:**
- **البث في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.**
- **... دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها.**

[1] أم الخير معتوق، كسب رهان الأمن السيبيراني ضمان لتعزيز الأمن والدفاع الوطنيين في الجزائر، **مجلة البحوث في الحقوق والعلوم السياسية**، المجلد 09، العدد 02 ، مارس 2024، ص 69.

[2] المادة 3 من المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر، العدد 4، 2020.

- **الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.**
- **.... اقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الانظمة المعلوماتية عند الحاجة.... ويبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صبة بأمن المعلوماتية."**[1]
- **وكالة أمن الأنظمة المعلوماتية:** هي مؤسسة عمومية إدارية يقع مقرها في الجزائر وتتمتع بالشخصية المعنوية والاستقلال المالي وتكلف الوكالة بعدة مهام وقد نصت عليها المادة 18 من المرسوم الرئاسي 20-05: " تكلف الوكالة بالخصوص على ما يأتي:
- **تحضير الاستراتيجية الوطنية لأمن الانظمة المعلوماتية وعرضها على المجلس.**
- **تنسيق تنفيذ استراتيجية وطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس.**
- **اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.**
- **إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبيرانية التي تستهدف المؤسسات الوطنية.**
- **السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال الأمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشئات المؤسسات الوطنية.**
- **... تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية من أجل وضع استراتيجية أمن الأنظمة المعلوماتية.**
- **... مرافقة الإدارات والمؤسسات والهيئات، بالتشاور مع الهياكل الخاصة في هذا المجال في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية...تقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في مجال أمن الأنظمة المعلوماتية.**

[1] المادة 4 من المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر، العدد 04، 2020.

- **... التنظيم والمشاركة في الأحداث والتظاهرات العلمية والتقنية المتعلقة بأمن الأنظمة المعلوماتية."[1]**

لهذا فإن هذه المصالح أوكلت لها مهمة في غاية الحساسية وهي حماية الأنظمة والمنشآت الحيوية للبلاد ضد كل الجرائم الإلكترونية وللحفاظ على الأمن السيبيراني.

المطلب الثالث: الآليات الإدارية المختصة لمكافحة الجريمة الإلكترونية وضمان الأمن السيبراني.

تلعب الهيئات الإدارية دورا مهما في مكافحة الجريمة الإلكترونية وضمان الأمن السيبيراني حيث تساهم وبشكل فعال في رسم سياسات التي تنظم عملية استخدام الإنترنت وتحمي الأفراد والمؤسسات كما تساهم في رفع الوعي لديهم في سبيل الوقاية والحماية ضد الجرائم الإلكترونية بكل أنواعها. وتعددت الاستراتيجيات التي اعتمدتها الجزائر في سبيل مجابهتها ولهذا قمنا في هذا المطلب بتقسيمه إلى ثلاث فروع وتتمثل فيما يلي في **(الفرع الأول)** تطرقنا إلى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، أما **(الفرع الثاني)** خصصناه للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. **(الفرع الثالث)** القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، **(الفرع الرابع)** تطرقنا إلى تنظيم دورات تكوينية ومؤتمرات حول الجريمة الإلكترونية لتحقيق الأمن السيبيراني.

الفرع الأول: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

حسب ما جاء به القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي **ونصت المادة 22 منه على:** " تنشا لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي شار إليها أدناه "السلطة الوطنية" يحدد مقرها في الجزائر العاصمة تتمتع السلطة الوطنية بالشخصية المعنوية والاستقلال المالي والإداري. تقيد ميزانية السلطة الوطنية في ميزانية الدولة وتخضع للمراقبة المالية طبقا للتشريع المعمول

[1] المادة 18 من المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر، العدد04، 2020.

به..."[1] كما أنها تتكون من 13 عضو يتم تعيينهم بموجب مرسوم رئاسي لمدة 5 سنوات قابلة للتجديد وهم ملزمون بتأدية اليمين أما مجلس قضاء الجزائر وهذا حسب ما جاء في المادة 23 من نفس القانون.

أما عن مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي قد نصت عليها المادة 25 من القانون 18-07 على ما يلي: " **تكلف السلطة الوطنية بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون... وتتمثل مهامها في هذا الصدد لاسيما في:**

- **منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.**
- **إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.**
- **تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي ...**
- **... الترخيص ينقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون.**
- **الأمر بالتغيرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.**
- **الأمر بإغلاق معطيات أو سحبها أو إتلافها.**
- **تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.**
- **... تطوير علاقات التعاون مع السلطات الأجنبية..."[2] ومن هنا تتلخص مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في مراقبة الإجراءات المسبقة للمعالجة، ويجب إيداع تصريح مسبق للمعالجة من المعني بعد إيداعه تمنحه إياه السلطة الوطنية بعدها يجب أن تتم عملية مراقبة للإجراءات بعد المعالجة، طيلة كل مدة المعالجة للشخص مجموعة من الحقوق والواجبات التي يجب احترامها. كما يلزم على رئيس السلطة وأعضائها المحافظة على سرية المعطيات حتى لو بعد انتهاء مهامهم.**

[1] المادة 22 من القانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج. ر، العدد 34، 2018.

[2] المادة 25 من القانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج. ر، العدد 34، 2018.

كما تكلف السلطة الوطنية بإنشاء ومسك سجل وطني لحماية المعطيات الشخصية تقيد فيه كل الملفات التي تعالجها الهيئات العمومية والخاصة، وكذا التصريحات والتراخيص المسلمة وكذا هويات الأشخاص المسؤولين عن المعالجة وكل المعطيات والمعلومات التي ينص عليها التنظيم الخاص بتحديد شروط وكيفيات مسك سجل وطني.[1]

بالرغم من صدور القانون 18-07 الذي يضمن حماية خصوصية الأشخاص عند معالجة المعطيات الشخصية، وتعزيزه لاستراتيجية الجزائر في إطار مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبيراني إلى أن التأخر في تنصيب هذه السلطة على أرض الواقع هذا ما يؤدي إلى التعطيل في تطبيق أحكام هذا القانون ويؤدي إلى تفاقم الوضع وتعرض خصوصية الأفراد إلى الخطر.

الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

أنشئت هذه الهيئة في أكتوبر 2015 بموجب المرسوم الرئاسي رقم 15- 265 المؤرخ في 08 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،[2] حسب المادة 2 منه: " **الهيئة سلطة إدارية مستلقة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى وزير المكلف بالعدل.**"[3] ويوجد مقر الهيئة بالجزائر العاصمة وتضم أساسا أعضاء من الحكومة معيين بالموضوع ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، وتضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.[4]

---

[1] محمد العيداني، يوسف زروق، "حماية المعطيات في الجزائر في ضوء القانون رقم 18-07 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)"، **مجلة معالم للدراسات القانونية والسياسية**، العدد 05، ديسمبر 2018، ص 124.

[2] المرسوم الرئاسي رقم 15- 265، المؤرخ في 8 أكتوبر 2015، المتعلق يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر، العدد 53، 2015.

[3] المادة 2 من المرسوم الرئاسي رقم 15- 265، المؤرخ في 8 أكتوبر 2015، المتعلق يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر، العدد 53، 2015.

[4] شهرزاد بولحية ورشيد خلوفي، مرجع سبق ذكره، ص 1995.

أما عن المهام التي تكلف بها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال فقد نصت عليها المادة 14 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جاء نص المادة على: تتولى الهيئة بالمهام الآتية:

1- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

2- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

3- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم."[1]

كما أن المرسوم الرئاسي رقم 15-261 الذي ذكرناه سابقا تطرق إلى مهام أخرى كما فصل في بعض المهام التي تطرقت إليها المادة 14 من القانون رقم 09-04 وعليه نصت المادة 04 من المرسوم الرئاسي على: **تكلف الهيئة في ظل احترام الأحكام التشريعية المبينة أعلاه على الخصوص بما يأتي:**

- **اقتراح عناصر الاستراتيجية الوطنية للرقابة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.**
- **تنشيط وتنسيق عمليات الوقاية من الجرائم ...**
- **مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها من خلال الخبرات القضائية.**

[1] المادة 14 من القانون رقم 09-04، المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر، العدد 47، 2009.

- **ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.**
- **تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.**
- **السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.**
- **تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.**
- **المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.**
- **المساهمة في تحديث المعايير القانونية في مجال اختصاصها."[1]**

بناءً على ما سبق يمكن التأكيد على أن دور الهيئة يرتبط أساساً بالجرائم الإلكترونية التي تمس أمن الدولة والدفاع الوطني والجرائم الإرهابية، حيث تمارس المديرية التقنية للهيئة مهامها المرتبطة بالشرطة القضائية وفقا لقانون الإجراءات الجزائية، وهذا ما يعني أن المشرع قد منح لهذه اختصاص البحث والتحري عن الجرائم الإرهابية أو الماسة بأمن الدولة عبر الوسائط الإلكترونية.[2] كما سمح باللجوء إلى المراقبة الإلكترونية وتفتيش وحجر المنظمات المعلوماتية لكن في حالات فقط حددها القانون ووفقا لمجموعة من القواعد حدتها نصوص المواد 4 و5 و6 من القانون رقم 09-04، كما أن الأشخاص المعنين بإجراء هذه الإجراءات ملزمون بكتمان السر وإلا تعرضوا لعقوبة إفشاء أسرار التحري والتحقيق. كما أن الهيئة تعمل على مد يد المساعدة للسلطات القضائية والأمنية وحتى التعاون والمساعدة مع السلطات القضائية الدولية.

[1] المادة 4 من المرسوم الرئاسي رقم 15- 265، المؤرخ في 8 أكتوبر 2015، المتعلق يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر، العدد 53، 2015.

[2] الطاهر زخمي، "الجرائم المعلوماتية في التشريع الجزائري وتدابير الوقاية منها"، **مجلة التشريع الإعلامي**، المجلد 02، العدد 01، أكتوبر 2023، ص 12.

الفرع الثالث: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

لقد تدخل المشرع وأنشأ هذا القطب لأن في ذلك حقيقة ضرورة حتمية لمجابهة هذا النوع من الإجرام بالنظر لخصوصيته وخصوصية مرتكبيه، والذي يمثل تهديدا صارخا على المصالح أساسية في الدولة كأمن الدولة، واقتصادها والنظام العام فيها والسلم الاجتماعي وكذلك العلاقات الدولية والإقليمية بما لها من بعد دولي عابر للحدود.[1]

لقد أنشأ هذا القطب وذلك بموجب الأمر رقم 21-11 المؤرخ في 25 أوت 2021 والذي يتمم الأمر رقم 66-155 المعدل والمتمم لقانون الإجراءات الجزائية، والمتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ونصت المادة 211 مكرر22 من الأمر21-11 على: " **ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها. كما أنه يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا.**"[2]

ويتكون هذا القطب من قضاة ومستخدمي أمانات الضبط للجهات القضائية والقضاة التي يضمهم القطب هم ونصت عليهم **المادة 211 مكرر 23: " يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني.**"[3] ويهذا القطب يضم جهة الحكم والمتمثلة في رئيس القطب وجهة متابعة وهي وكيل الجمهورية ومساعديه، وجهة التحقيق التي تتمثل في قاضي التحقيق لهم الحق في تمديد اختصاصهم لكامل الإقليم الوطني وموظفون أمانات الضبط.

---

[1] سلمى عبد النبي، "دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في مواجهة الاعتداءات الواقعة على المعطيات المعلوماتية"، **مجلة الحقوق والعلوم السياسية**، المجلد 11، العدد 02، جوان 2024، ص 20.

[2] المادة 211 مكرر22 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

[3] المادة 211 مكرر23 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021

أما عن اختصاص القطب فهو يختص في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أي أنه يختص في نوع واحد من الجرائم وكل الجرائم المرتبطة بهذا النوع.

وباستقراء نصوص الأمر 21-11 المنشأة للقطب الجزائي الوطني، نجدها قد ميزت في إطار اختصاصه النوعي بين نوعين متميزين من الاختصاصات منها الاختصاص الحصري واختصاص مشترك، كما تطرقت لمسألة بالغة الأهمية تتعلق بتزامن اختصاص بينه وبين يعض الجهات القضائية اذ منح هذه الأخيرة الأفضلية.[1] وتتمثل اختصاصات هذا القطب فيما يلي:

1. **الاختصاص الحصري:** وينحصر هذا الاختصاص في المادة 211 مكرر 24 و 25 والذي يتضمن حالتين:

- **الحالة الأولى:** نصت عليها المادة 211 مكرر 24 حيث نصت على أنه:" **مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:**

  - **الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.**
  - **جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.**
  - **جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.**
  - **جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.**
  - **جرائم الإتجار بالأشخاص والأعضاء البشرية أو تهريب المهاجرين.**
  - **جرائم التمييز وخطاب الكراهية."[2]**

[1] سلمى عبد النبي، مرجع سبق ذكره، ص 22.

[2] المادة211 مكرر 24 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

ما نلاحظه أن المشرع أوكل للقطب الجزائي الاختصاص الحصري لمكافحة جرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم ذات الطابع المقعد والخطير، كالجرائم التي تمس بأمن الدولة ومؤسسات الدولة وتمس بالدفاع الوطني والتي تضر بأمن واستقرار المجتمع وسكينته.

- **الحالة الثانية:** وتنص المادة 211 مكرر25 على: " مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيداً والجرائم المرتبطة بها. ويقصد .... بها الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، والتي تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون دولي."[1]

يتضح من هذه المادة أن انعقاد الاختصاص للقطب له مجموعة من الشروط هو أن تكون الجريمة مرتكبة الوارد تعريفها في الفقرة الثانية من المادة 211 مكرر22، وأن تتسم الجريمة بمجموعة من المواصفات المعينة التي تمييزها عن غيرها.

2. **الاختصاص المشترك:** هو ذلك الاختصاص المشار إليه في نص المادة 211 مكرر27 ونصت على:" **دون الإخلال بأحكام المادتين 211 مكرر24 ومكرر25 أعلاه يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب اختصاص مشتركا مع الاختصاص الناتج عن تطبيق المواد 37 و40 و329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها."**[2]

يفهم من هذه المادة أن القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يمارس اختصاص مشترك مع اختصاص الأقطاب الجزائية ذات الاختصاص الموسع إذا

[1] المادة 211 مكرر من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

[2] المادة 211 مكرر 27 من لأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

تعلقت بإحدى الجرائم المنصوص عنها في المواد 37، 40، 329 من ق إ ج، بالرجوع إلى هذه المواد يلاحظ أن هذه الجرائم محصورة على وجه التحديد في جرائم المخدرات، الجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبيض الأموال والإرهاب.[1] إضافة إلى جرائم الفساد غير أن الاختصاص لا ينعقد في جميع الجرائم المذكورة بل استثنى المشرع البعض منها فقط، فالاختصاص المشترك للقطب الجزائي مع الأقطاب الجزائية المختصة يخص ثلاث جرائم فقط وهي: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والجريمة المتصلة بتكنولوجيا الإعلام والاتصال وجرائم المخدرات والجرائم المنظمة إذا معا اتصفت على أنها جريمة إلكترونية وفقا لتعريف المنصوص عليه في المادة 211 مكرر22.

3. **مسألة تزامن الاختصاص:** إن المشرع تطرق إلى مسألة تزامن الاختصاص في حالتين وهما:

- **الحالة الأولى:** وقد نصت عليها المادة 211 مكرر28 على:" **إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص القطب الاقتصادي والمالي، يؤول الاختصاص وجوبا لهذا الأخير.**"[2]
- **الحالة الثانية:** وقد نصت عليها المادة 211 مكرر 29 على:" **إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص محكمة مقر مجلس** قضاء الجزائر طبقا لأحكام المواد211 مكرر16 إلى 211 مكرر 21 من هذا القانون يؤول الاختصاص وجوبا لهذه الأخيرة."[3]

وتعليقا على مسألة تزامن الاختصاص المتضمنة في نص المادتين المشار إليهما أعلاه، فيمكن تصور ذلك في الحالة التي ترتكب فيها الجرائم المشار إليها أعلاه والتي يختص بها القطب الجزائي الاقتصادي والمالي، أو محكمة مقر مجلس قضاء الجزائر باستعمال تكنولوجيا الإعلام والاتصال وبذلك

---

[1] شريفة سوماتي، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، **مجلة الدراسات القانونية (صنف ج)**، المجلد 08، العدد 02، جوان 2022، ص497.

[2] المادة 211 مكرر28 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021

[3] المادة 211 مكرر 29 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

تكون مسألة التخلي لصالحها مسألة طبيعية ومنطقية للغاية كون تلك التقنيات المستعملة مجرد وسيلة مسهلة،[1] ويبقى الفعل الرئيسي المرتكب ضمن اختصاصاتها.

في هذا الإطار فإن الاستراتيجية الجزائرية تسعى إلى تعزيز أمنها في مواجهة الجرائم الإلكترونية والتهديدات السيبيرانية، من خلال تبنيها لاستراتيجية متنوعة تقوم على التنسيق بين مختلف القطاعات الأمنية والمدنية حيث أن مهمة تعزيز الحماية في الفضاء السيبيراني واجبة على الجميع. وقد أكدت الأجهزة الأمنية الجزائرية على أهمية اعتماد استراتيجية وطنية موحدة لتحقيق الأمن السيبيراني.

الفرع الرابع: تنظيم دورات تكوينية ومؤتمرات حول الجريمة الإلكترونية لتحقيق الأمن السيبيراني

حتى تتمكن الهيئات من السيطرة على مختلف الجوانب المتعلقة بعملية تحقيق الأمن السيبيراني وفق ما تم ترسيمه في الاستراتيجية الوطنية، توجهت المؤسسات السيادية (رئاسة الجمهورية، وزارة الدفاع، المؤسسات الأمنية ، الوزارات) إلى تنظيم دورات تكوينية وسخرت لها كافة الوسائل المادية والبشرية، كما استنجدت الجزائر بخبراء دوليين لتمكين الإطارات الناشئة في المجال لمعرفة أفضل الممارسات في تكنولوجيا الأمن.[2] كما عملت الجزائر على إرسال بعثات للخارج لحضور والمشاركة في مؤتمرات بهدف الحصول على خبرات في مجال الأمن السيبيراني.

اعتمدت الجزائر كذلك على الجانب التحسيسي بقيام المصالح الأمنية والدرك الوطني بحملات توعية، من شأنها توعية المواطنين بمخاطر التهديدات السيبيرانية التي تهدد الدولة والمجتمع والتأكيد على ضرورة تحقيق الأمن السيبيراني. وهو ما عبرت عنه القيادات العسكرية الجزائرية في العديد من الخطابات حيث تطرق رئيس الأركان الجيش الشعبي الوطني " سعيد شنقريحة " من خلال كلمته في افتتاح أشغال الملتقى الثاني " الأمن السيبيراني والدفاع السيبيراني "رهانات وتحديات على ضوء التحولات الجديدة المتعددة الأبعاد يومي 23 و24 ماي 2021 حيث صرح كما لا يفوتني أن أؤكد على ضرورة حماية وتأمين والدفاع في فضائنا السيبيراني هي مسؤولية جماعية، تضمن من خلال استراتيجية وطنية شاملة

[1] سلمى عبد النبي، مرجع سبق ذكره، ص 24.

[2] جمال بوازدية، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبيرانية " التحديات والآفاق المستقبلية"، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 01، فيفري 2019، ص 1284.

للأمن السيبيراني يتعين أن ينخرط فيها الجميع بداية من المواطن."[1] والمقصود هنا أن يكون مواطن على دراية شاملة بمخاطر الفضاء السيبيراني، وأن يفعل دور المختصين والمسؤولين في هذه الناحية لإنجاح الاستراتيجية الوطنية المكافحة للجرائم الإلكترونية والتي تهدف إلى تعزيز الأمن السيبيراني.

كما ساهمت الجامعات ومؤسسات البحث العلمي من تنظيم ملتقيات وأيام دراسية حول هذه الظاهرة والتي تخلص في غالب الأحيان بمجموعة من التوصيات المهمة التي يمكن أخذها بعين الاعتبار. بالإضافة إلى وزارة العدل التي تقوم بالعديد من البرامج التكوينية ،في هذا الإطار كالقيام بعمل إحصائيات سنوية حول الجرائم الإلكترونية وتأثيراتها بالاشتراك مع المصالح والهيئات الأمنية.

فعند تنظيم الطبعة السابعة للمؤتمر المرسوم ب: "الأمن السيبيراني: من سرقة المعلومات إلى التلاعب بالمعلومات" المنظم من طرف **"world Trade center algiers "** في 07 ديسمبر 2021 بالجزائر العاصمة، حيث أوصى على هامشه الخبراء المشاركين فيه بإنشاء مدرسة متخصصة في الأمن السيبيراني، وذلك لاكتساب الخبرات اللازمة من أجل التصدي بمختلف الهجمات الإلكترونية التي تهدد استقرار البلاد... وحماية الجزائر من خلال وضع استراتيجيات وطنية وأمنية في إطار ما تقترحه المدرسة.[2] وهذا ما تم تجسيده فعليا على أرض الواقع حيث أمر السيد رئيس الجمهورية بفتح مدرسة وطنية عليا للأمن السيبراني سنة 2023.

[1] عبد الله جعفري، "التهديدات السيبيرانية وتأثيرها على الأمن القومي الجزائري"، **المجلة الأفريقية للدراسات القانونية والسياسية**، المجلد 06، العدد 02، ديسمبر 2021، ص 253.

[2] وفاء مطروح وابتسام أونيس، مرجع سبق ذكره، 238.

خلاصة الفصل الثاني:

تبين في سياق الفصل الثاني من الدراسة أن الجريمة الإلكترونية واحدة من أبرز التحديات التي تواجه الأمن السيبراني في الجزائر، خصوصاً في ظل التوسع السريع في استخدام التكنولوجيا في مختلف المجالات والذي أدى إلى ارتفاع الجريمة وتعدد في أنواعها وتحولها إلى جريمة منظمة من قبل جماعات إجرامية، مما خلق تهديداً حقيقيا يؤثر على البنية التحتية الرقمية للوطن وتنعكس تأثيرات هذه الجرائم على العديد من الجوانب.

هذا ما خلق تحدي للجزائر وسلطاتها المختصة في سبيل مكافحة الجرائم الإلكترونية والحد منها بكافة الوسائل وتحقيق الأمن السيبراني، من خلال توجه المشرع الجزائري إلى إصدار قوانين متخصصة وإنشاء هيئات أمنية رقابية وهيئات إدارية في سبيل المكافحة وتعزيز الأمن السيبراني، بالإضافة إلى إطلاق حملات تحسيسية لكافة الشرائح الاجتماعية لتوعية المواطنين وتكوين الكوادر على مختلف التطورات الحديثة التي تساهم في تحقيق الأمن السيبراني وضمان فضاء سيبراني آمن ومستقر يخدم التنمية الوطنية.

الخاتمة

الخاتمة

في خضم التحول الرقمي العالمي وما يرافقه من انفجار معلوماتي وتوسع في استخدام الإنترنت برزت الجريمة الإلكترونية كواحدة من أخطر التحديات التي تهدد أمن الدول وسيادتها الرقمية، وبشكل خاص الأمن السيبراني، الذي أصبح أحد المرتكزات الأساسية لاستقرار المجتمعات الحديثة. وقد سعت هذه المذكرة إلى تسليط الضوء على مدى تأثير الجريمة الإلكترونية على الأمن السيبراني في الجزائر، من خلال تحليل المفاهيم المرتبطة بها وتقييم واقعها، ورصد مكامن الضعف والتحديات، إلى جانب استعراض الجهود المبذولة لمواجهتها.

قد بيّنت الدراسة أن الجزائر بالرغم من الخطوات التي قطعتها في سبيل تعزيز أمنها السيبراني، لا تزال تواجه تهديدات إلكترونية متصاعدة، بفعل الانتشار الواسع للتكنولوجيا من جهة وضعف الحماية القانونية والتقنية من جهة أخرى، كما تبيّن أن الجريمة الإلكترونية تطورت من أفعال معزولة إلى ظاهرة منظمة تتغذى من الثغرات التشريعية، ونقص الكفاءات، وغياب التنسيق بين الفاعلين المؤسساتيين.

النتائج :

أسفر البحث في موضوع "**تأثير الجريمة الإلكترونية على الأمن السيبراني في الجزائر**" عن جملة من النتائج المهمة، يمكن تلخيص أبرزها في ما يلي:

1. ارتفاع وتيرة الجرائم الإلكترونية في الجزائر خلال السنوات الأخيرة بشكل ملحوظ، حيث تحولت من حالات فردية متفرقة إلى عمليات منظمة تستخدم تقنيات متقدمة، مما أدى إلى تهديد متزايد للأمن السيبراني الوطني.
2. رغم الانتشار الواسع للإنترنت والتقنيات الرقمية في البلاد، إلا أن البنية التحتية للأمن السيبراني تعاني من ضعف واضح في الموارد التقنية والتنظيمية، مما يحد من قدرة المؤسسات على مواجهة التهديدات السيبرانية بكفاءة.
3. تشير المؤشرات الدولية إلى وجود فجوة كبيرة في جاهزية الجزائر لمواجهة التحديات السيبرانية مقارنة بالدول الأخرى، ما يعكس الحاجة إلى تعزيز الاستراتيجيات الوطنية ومواكبة التطورات التقنية.

4. يفتقر الإطار القانوني الجزائري إلى نصوص حديثة ومتكاملة تتناول الجرائم الإلكترونية، كما يعاني من غياب آليات فعالة للتحقيق والإثبات في القضايا الرقمية.
5. تعاني الأجهزة الأمنية والقضائية من نقص في الكفاءات التقنية المتخصصة في مجال التحقيق الجنائي الرقمي، مما يؤثر سلبًا على فاعلية مكافحة الجرائم الإلكترونية.
6. يلاحظ قصور في التنسيق بين الجهات المعنية بالأمن السيبراني على المستوى الوطني بالإضافة إلى محدودية التعاون الدولي، ما يعيق الجهود المبذولة لمواجهة الجرائم العابرة للحدود.
7. يعاني المجتمع الجزائري من ضعف في مستوى الوعي بالمخاطر السيبرانية وأساليب الحماية، الأمر الذي يزيد من تعرض الأفراد والمؤسسات للهجمات الرقمية.

التوصيات:

بعد التطرق لمختلف الجوانب المتعلقة موضوع الدراسة الجريمة الإلكترونية وأثارها على الأمن السيبراني في الجزائر، اتضح أن هذه الإشكالية تفرض تحديات جدية تتطلب استجابة شاملة وفعالة، وبناءً على ما توصل إليه هذا البحث من نتائج، يمكن اقتراح جملة من التوصيات التي قد تسهم في تعزيز المنظومة الوطنية للأمن السيبراني والحد من مخاطر الجريمة الإلكترونية، وتتمثل هذه التوصيات في ما يلي:

1. **تحديث الإطار التشريعي:** ضرورة مراجعة وتطوير التشريعات الوطنية لتشمل كافة صور الجرائم الإلكترونية الحديثة، مع وضع آليات قانونية واضحة ومرنة للتحقيق والإثبات تتناسب مع خصوصية الأدلة الرقمية.
2. **إنشاء هيئة وطنية مستقلة للأمن السيبراني:** تأسيس جهة مركزية متخصصة ذات صلاحيات واسعة لتنسيق السياسات الوطنية، ومتابعة تنفيذ الاستراتيجيات المتعلقة بمكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني.
3. **تعزيز القدرات الفنية والبشرية:** الاستثمار في تدريب وتأهيل الكوادر الأمنية والقضائية والفنية من خلال برامج متخصصة لتطوير مهارات التحقيق الجنائي الرقمي وإدارة الحوادث السيبرانية.

4. **تطوير البنية التحتية التقنية:** تعزيز وتحديث الموارد التقنية والأدوات المستخدمة في الحماية والمراقبة السيبرانية، خاصة في القطاعات الحيوية والمرافق الوطنية الأساسية.

5. **رفع مستوى الوعي المجتمعي:** إطلاق حملات توعوية مستمرة تستهدف مختلف شرائح المجتمع لتعزيز الثقافة الأمنية الرقمية، والوقاية من المخاطر المرتبطة باستخدام الفضاء الإلكتروني.

6. **تعزيز التعاون الوطني والدولي:** تفعيل آليات التنسيق بين مختلف الجهات الوطنية ذات الصلة، وتوسيع التعاون مع المؤسسات والمنظمات الدولية المختصة لمواجهة الجرائم السيبرانية العابرة للحدود بفعالية.

7. **تشجيع البحث والتطوير العلمي:** دعم وتمويل الأبحاث والدراسات المتخصصة في مجال الأمن السيبراني، وربط نتائجها بسياسات الدولة لتطوير حلول تقنية وقانونية مستدامة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر:

1- النصوص القانونية

- **الدستور:**

1) المادة 47 من الفصل الأول تحت عنوان الحقوق والحريات العامة، من دستور 2020، المؤرخ في 30 ديسمبر 2020، ج. ر، العدد 82، 2020.
2) المادة 55 من الفصل الأول تحت عنوان الحقوق والحريات العامة، من دستور2020، المؤرخ في 30 ديسمبر 2020، ج. ر، العدد 82، 2020.

- **الأوامر والقوانين:**

1) الأمر03-05، المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج. ر، عدد 44، 2003.
2) الأمر رقم 11/21 الذي يتمم الأمر 66-155، المؤرخ في 25 أوت 2021، المتضمن تعديل قانون الإجراءات الجزائية، ج .ر، عدد 65، 2021.
3) القانون رقم 04-15، المؤرخ في 10 نوفمبر2004، المتضمن قانون العقوبات، ج .ر، العدد 71، 2004.
4) القانون 05-10، المؤرخ في20 يونيو2005 ، المتعلق بالقانون المدني، ج. ر، عدد 44، 2005.
5) القانون رقم 09/01 المؤرخ في: 25 فيفري 2009، المتضمن قانون العقوبات الجزائري ، ج. ر، العدد 15، 2009.
6) القانون رقم 09-04، المؤرخ في 5 سبتمبر 2009 ، المتضمن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها**، ج. ر العدد 47، الصادر في 16 أوت 2009.
7) القانون رقم 175، المؤرخ في 14 أغسطس 2018، **المتعلق بمكافحة جرائم تقنية المعلومات**، ج. ر، العدد 32، 2018.
8) المادة 127 من القانون رقم 2000- 03، المؤرخ في 5 أوت 2000، المتعلق بالقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج. ر، العدد 48، 2000.

9) المادة 2 من المرسوم الرئاسي رقم 04-183، المؤرخ في 26 يونيو 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج. ر، العدد 41، 2004.

10) المادة 4 من المرسوم الرئاسي رقم 04-183، المؤرخ في 26 يونيو 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج. ر، العدد 41، 2004.

11) المادة 65 مكرر 5 من القانون رقم 06-22 ،المؤرخ في 20 ديسمبر 2006، الذي يعدل ويتمم الأمر 06-155، **المتضمن قانون الإجراءات الجزائية**، ج. ر، عدد 84، 2006.

12) المادة 14 من القانون رقم 09-04، المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر، العدد 47، 2009.

13) المادة 4 من المرسوم الرئاسي رقم 15- 265، المؤرخ في 8 أكتوبر 2015، المتعلق يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر، العدد 53، 2015.

14) المادة 22 من القانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج. ر، العدد 34، 2018.

15) المادة 25 من القانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج. ر، العدد 34، 2018.

16) المادة 3 من المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر، العدد 4، 2020.

17) المادة 4 من المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر، العدد 4، 2020

18) المادة 18 من المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر، العدد 4، 2020.

19) المادة 211 مكرر22 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

20) المادة 211 مكرر23 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

21) المادة211 مكرر 24 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

22) المادة 211 مكرر 25 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

23) المادة 211 مكرر 27 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

24) المادة 211 مكرر28 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

25) المادة 211 مكرر 29 من الأمر 21-11، المؤرخ في 25 أوت 2021، المتعلق باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر، العدد 65، 2021.

26) المادة 394 من القانون رقم 06-24، المؤرخ في 28 أبريل 2024، الذي يعدل ويتمم الأمر 66-155، المتعلق بقانون العقوبات، ج. ر، عدد 30، 2024.

2- النصوص التنظيمية

- **المراسيم:**

1) المرسوم الرئاسي من القانون رقم 09- 04، المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر، العدد 47، 2009.

2) المرسوم الرئاسي رقم 15- 265، المؤرخ في 8 أكتوبر 2015، المتعلق يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر، العدد 53، 2015.

3) قرار بقانون رقم 10 ، المؤرخ في 3 ماي 2018، المتعلق بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، ج. ر الفلسطينية، العدد 16، 2018.

ثانيا: المراجع

1- كتب باللغة العربية

1) بن مكي نجاة، **السياسة الجنائية لمكافحة جرائم المعلومات** ، د. ط، دار الخلدونية للنشر والتوزيع، الجزائر،2017.
2) حبابية محمد ميرفت، **مكافحة الجريمة الإلكترونية: دراسة مقارنة في التشريع الجزائري و الفلسطيني**، المجلد 01، ط الأولى، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2020.
3) خليفة إيهاب، **الحرب السيبرانية (الاستعداد لقيادة المعارك العسكرية في الميدان الخامس)**، العربي للنشر والتوزيع، الطبعة الأولى، القاهرة، 2020.
4) العمارات محمد فارس، **الأمن السيبراني مفهوم وتحديات العصر**، الطبعة 01، دار الخليج للنشر والتوزيع، الأردن، 2022.
5) العمارات فارس محمد، **جرائم العصر من الرقمية إلى السيبيرانية**، الطبعة 01، دار الخليج للنشر والتوزيع، الأردن، 2023.
6) نهلا عبد القادر المؤمني، **الجرائم المعلوماتية**، الطبعة 02، دار الثقافة للنشر والتوزيع، عمان، 2010.
7) ياكر الطاهر، **الجرائم للإلكترونية الأحكام الموضوعية والإجرائية**، د ط، دار بلقيس للنشر، الجزائر، 2024.
8) يحي الزعاترة فرح، **التهديدات السيبرانية على الأمن القومي الأمريكي(دراسة تحليلية)** ، القاهرة، العربي للنشر والتوزيع، 2023.

2- كتب باللغة الأجنبية

1) Pekka Neittaanmaki, Martti Lehto, " Cyber Security : Analytics, Technology and Automation" , Spnger international Publishing, volume 78, Inteellingent System, control and Automation Science and Enerineering, Switzerland, 2015.

ثالثا: الأطروحات والمذكرات

- **أطروحات دكتوراه**

1) بوحزمة نصيرة، **التحقيق الجنائي في الجرائم الالكترونية (دراسة مقارنة)**، أطروحة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2022.
2) باطلي غنية، **الجريمة الإلكترونية (دراسة مقارنة)**، أطروحة دكتوراه في القانون الخاص، كلية الحقوق، جامعة باجي مختار، عنابة،2011.
3) بن يحيى إسماعيل، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2021.
4) براهيمي جمال، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراه في العلوم تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.
5) ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016.
6) العوفي دليلة، **آليات محاربة الجريمة المعلوماتية (دراسة حالة الجزائر2009-2006)**، أطروحة دكتوراه علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة ابراهيم سلطان شيبوط، الجزائر، 2020.

- **رسائل ماجستير.**

1) صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.
2) عبد الكريم نعمان، **الجرائم الإلكترونية وموقف المشرع الجزائري منها**، مذكرة ماجستير، كلية الحقوق، الجزائر، 2017.
3) العجمي عبد الله دغش، **المشكلات العلمية والقانونية للجرائم الإلكترونية(دراسة مقارنة)**، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن.
4) العفيفي يوسف خليل يوسف ، **الجرائم الإلكترونية في التشريع الفلسطيني(دراسة تحليلية مقارنة)**، رسالة ماجستير قسم القانون العام ، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2013.

- **ثالثا: المقالات**

1) بن لعربي أسماء، مديحة الفحلة، "مكافحة الجريمة الإلكترونية في الجزائر: رؤية تشريعية واستراتيجيات عملية"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 09، العدد01، مارس 2025.

2) بن جدو بن علية، "تحديات الأمن السيبيراني لمواجهة الجريمة الإلكترونية"، **المجلة الجزائرية للأمن الإنساني**، المجلد 07، العدد 02، جويلية2022.

3) بوازدية جمال، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبيرانية " التحديات والآفاق المستقبلية"، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 01، فيفري 2019.

4) بوضياف اسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، ع11، ماي2018.

5) بارة سمير،" الأمن السيبراني"cyber Security" في الجزائر: السياسات والمؤسسات"، **المجلة الجزائرية للأمن الإنساني**، العدد 04، جويلية 2017.

6) بدرين سيد علي، "استراتيجية الجزائر لمواجهة التهديدات السيبرانية"، **مجلة الشرطة**، المديرية العامة للشرطة الجزائرية، العدد 156، أكتوبر 2023.

7) بعوني ليلى،" التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نمودجا"، **مجلة ستراتيجيا**، العدد 16، السداسي الثاني، 2021.

8) بلقاسم سميحة، حميد بوشوشه،" الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابهتها"، **مجلة العلوم الإنسانية**، مجلد 10، العدد 1، جوان2023.

9) بن عبو عفيف، "الآليات القانونية في الجزائر وتطورها في مكافحة الجريمة الإلكترونية"، **مجلة حقوق الإنسان والحريات العامة**، المجلد 09، العدد01، جوان2024.

10) بن عزوز حاتم، مناني حليمة، "الأمن السيبراني و الجريمة الإلكترونية في الدول ما بعد الحداثية: الولايات المتحدة الأمريكية(نموذجا)"، **مجلة الرسالة للدراسات الاعلامية**، المجلد 6، العدد 2، جوان 2022.

11) بوعون عفاف، نسيمة أولاد سالم، "الجريمة الإلكترونية (قراءة سوسيوتاريخية في النشأة والأثار)"، **مجلة القيس للدراسات النفسية والاجتماعية**، المجلد05، العدد 20، ديسمبر 2023.

12) بولحية شهرزاد و خلوفي رشيد، "تحديات الجريمة الإلكترونية في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية**، المجلد 04، العدد 02، جانفي 2020.

13) بغدادي، إيمان، "أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية"، **مجلة آفاق للبحوث والدراسات**، 2019.

14) تغريد صفاء مهدي، خميس مهدي لبنى، "أثر السيبرانية في تطور القوة"، **مجلة حمورابي للدراسات**، مركز حمورابي للبحوث والدراسات الاستراتيجية، العددان 33–34 السنة الثامنة (شتاء–ربيع)، 2020.

15) جعفر بن محمد بن ذيب بن شفلوت، "العوامل الاجتماعية المؤدية لارتكاب الجرائم الإلكترونية في المجتمع السعودي"، دراسة ميدانية على المحققين في النيابة العامة بمدينة الرياض، **مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية**، جامعة الفيوم، العدد 27، 2022.

16) جعفري عبد الله، "التهديدات السيبيرانية وتأثيرها على الأمن القومي الجزائري"، **المجلة الأفريقية للدراسات القانونية والسياسية**، المجلة 06، العدد02، ديسمبر 2021.

17) جيلالي شويرب، مراد فائزة، "مفهوم الحروب السيبيرانية والأمن السيبراني"، **مجلة الحقوق والحريات**، المجلد 11، العدد01، أفريل 2023.

18) جبريل رشاد مراعي إسراء، " الجرائم الإلكترونية: الأهداف– الأسباب– طرق الجريمة ومعالجتها"، **مجلة الدراسات الإعلامية، المركز الديموقراطي العربي**، العدد الأول، يناير 2018

19) حميدي حياة، طايلب نسيمة، "مدخل مفاهيمي حول الأمن السيبراني"، **مجلة مدار للدراسات الاتصالية الرقمية**، المجلد02 ، العدد 02، نوفمبر ، 2022.

20) حيمر فتيحة، "الجرائم المعلوماتية في الجزائر: المواجهة والتحدي"، **مجلة الحقوق والعلوم السياسية**، المجلد12، العدد 02، جانفي 2025.

21) حيمر فتيحة، "تأثير الجريمة الإلكترونية على الأمن في إفريقيا"، **مجلة أبحاث قانونية وسياسية**، المجلد 9، العدد 1، جوان 2024.

22) خلف فاروق، "الآليات القانونية لمكافحة الجريمة المعلوماتية"، **مجلة الحقوق والحريات**، العدد 2، سنة 2015.

23) دقايشية زهور، "الحماية الجنائية للطفل غلى ضوء قانون العقوبات الجزائري"، **مجلة الحقوق والعلوم السياسية**، العدد2، جوان2016.

24) رابح سعاد، "ضوابط مكافحة الجريمة المعلوماتية"، **مجلة القانون العام الجزائري والمقارن**، المجلد 07، العدد 01، جوان 2021.

25) رحموني محمد ، "خصائص الجريمة الإلكترونية ومجالات استخدامها"، **مجلة الحقيقة**، العدد41، جانفي2018.

26) زخمي الطاهر، "الجرائم المعلوماتية في التشريع الجزائري وتدابير الوقاية منها"، **مجلة التشريع الإعلامي**، المجلد 02، العدد 01، أكتوبر 2023.

27) زدام بريزة، بن سماعين سمية، "الجريمة الإلكترونية والآليات الدولية لمكافحتها"، **مجلة علمية دولية نصف سنوية**، المجلد08 ، العدد01، 2023.

28) زروقي عاسية، "جرائم الاعتداء على الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات الحماية"، **مجلة القانون والعلوم السياسية**، المجلد 8، العدد 2، جويلية 2022.

29) السبتي آسيا، بوقريط عمر، "الجرائم السيبيرانية: مفهومها وآليات مكافحتها"، **مجلة الحقوق والعلوم الإنسانية**، المجلد 18، العدد01، أفريل2025.

30) السحمان مني عبد الله، "متطلبات تحقيق الأمن السيبيراني لأنظمة المعلومات الإدارية"، بجامعة الملك سعود، مجلة كلية التربية جامعة المنصورة، العدد111 ، يوليو 2022.

31) سعيدي خليل ، مرزوق بن مهدي، "الذكاء الاصطناعي كتوجه حتمي في حماية الامن السيبيراني"، **مجلة الدراسات في حقوق الإنسان**، المجلد 06، العدد 01، جوان 2022.

32) سوماتي شريفة، "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص"، **مجلة الدراسات القانونية (صنف ج)**، المجلد 08، العدد 02، جوان 2022.

33) طالة لامية، كهينة سلام، الجريمة الإلكترونية : "بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعية"، **مجلة الرواق للدراسات الاجتماعية والإنسانية**، العدد 02، ديسمبر2020.

34) علي محمود سيناء، "التحديات الأمنية للدول في الفضاء السيبراني"، **مجلة قضايا سياسية**، كلية العلوم السياسية جامعة النهرين، العدد 80، مارس2025.

35) عادل الرواشدة صباح، "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة ميدانية في الأردن"، **المجلة الأردنية في إدارة الأعمال**، المجلد 21، العدد 01، ديسمبر2023.

36) عباس غنية، "الجريمة الإلكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية"، **المجلة الجزائرية للسياسات العامة**، المجلد 12، العدد 03، ديسمبر2024.

37) عبد القادر إيمان، "أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من2011 حتى 2023"، **مجلة الأكاديمية العسكرية للدراسات العليا والاستراتيجية**، العدد 03، يناير2024.

38) عبد النبي سلمى، "دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في مواجهة الاعتداءات الواقعة على المعطيات المعلوماتية"، **مجلة الحقوق والعلوم السياسية**، المجلد 11، العدد 02، جوان 2024.

39) عراب مريم، "جريمة التهديد والابتزاز الإلكتروني"، **مجلة الدراسات القانونية المقارنة**، المجلد 7، العدد 01، جوان 2021.

40) عطية إدريس، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، **مجلة مصداقية**، صادرة عن المدرسة العليا العسكرية للإعلام والاتصال، المجلد 01، العدد 01، سبتمبر 2019.

41) عمور راضية، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 06، العدد01، مارس 2022.

42) العيداني محمد، زروق يوسف، "حماية المعطيات في الجزائر في ضوء القانون رقم 18-07(المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)"، **مجلة معالم للدراسات القانونية والسياسية**، العدد 05، ديسمبر 2018.

43) عادل الرواشدة صباح، "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة ميدانية في الأردن"، **المجلة الأردنية في إدارة الأعمال**، المجلد 21، العدد 01، ديسمبر 2023.

44) على شرشر محمود محمد صفاء الدين ، "الجهود الدولية والتشريعية لمكافحة جرائم الأنترنت"، **مجلة البحوث القانونية والاقتصادية**، كلية الحقوق جامعة المنوفية، العدد 51، مايو 2020.

45) فاضل عائشة، "المسؤولية الجزائية في الجرائم الإلكترونية(الجزائر نموذجا)"، **مجلة الحقوق والحريات**، المجلد11، العدد 01، أفريل 2023.

46) قريني كمال، "**تحديات الأمن السيبراني في مكافحة الجرائم السيبرانية في المجتمع الجزائري**"، من مؤلف جماعي، بعنوان: الجرائم الإلكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبراني، مارس 2022.

47) قاسم مراد محمد غالب محمد ، "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية(دراسة مقارنة)"، **المجلة العصرية للدراسات القانونية**، جامعة تغر باليمن، المجلد 02، العدد 02، جوان 2024.

48) كزيز صباح، "أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية نموذجا"، **مجلة الناقد للدراسات القانونية**، العدد 03، أكتوبر 2018.

49) كلاع شريفة، "الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"، **مجلة الحقوق والعلوم الإنسانية** ، مجلد 15، العدد 01، 2022.

50) لطرش فيروز، عزوز حاتم، "الجريمة الإلكترونية في الجزائر: من جريمة فردية إلى منظمة"، **مجلة آفاق العلوم**، المجلد 01، العدد 01، جانفي 2016.

51) المري راشد محمد ، "الأمن السيبراني وحماية الأنظمة الإلكترونية (دراسة تحليلية تأصيلية)"، **مجلة الدراسات القانونية والاقتصادية**، المجلد 09، العدد 01، مارس 2023.

52) مسكين حنان، "واقع مكافحة الجريمة المعلوماتية واتجاهاتها التشريعية في الجزائر"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 4، العدد01، مارس 2020.

53) مطروح وفاء، أونيس ابتسام،" تداعيات جائحة كوفيد-19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر"، **المجلة الدولية للاتصال الاجتماعي**، المجلد 09، العدد، 02، جوان 2022.

54) معتوق أم الخير، "كسب رهان الأمن السيبراني ضمان تعزيز الأمن والدفاع الوطني في الجزائر"، **مجلة البحوث في الحقوق والعلوم السياسية**، المجلد 09، العدد 02، مارس 2014.

55) ناشف فريد، "آليات التعاون الدولي في مكافحة الجرائم الإلكترونية "، **مجلة البحوث في الحقوق والعلوم السياسية**، المجلد رقم 08، العدد01، جوان2022.

56) المطيري خالد ظاهر عبد الله جابر السهيل ، "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، **مجلة البحوث الفقهية والقانونية**، العدد 38، يوليو2022.

57) ياقوت زينب، "واقع الجريمة عير الفيسبوك و سبل الحد من انتشارها دراسة حالة الجزائر"، **مجلة الدراسات والبحوث القانونية**، المجلد 07، العدد 02، جوان 2022.

رابعا: المداخلات العلمية.

1) البداينة ذياب موسى، "**الجرائم الإلكترونية- المفهوم والأسباب**"، ورقة بحث مقدمة في الملتقى العلمي: **الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية**، عمان- الأردن، 2 و 4 سبتمبر 2014.

2) خلوف حفيظة،" **تطور الجريمة الإلكترونية في ظل التغيرات الحاصلة**"، الملتقى العلمي الوطني بعنوان: **الجرائم المستحدثة أنواعها ومخاطرها. وآليات مواجهتها**، جامعة مولود معمري تيزي وزو، المنعقد يومي 27 و28 ديسمبر 2022.

3) سويسي فتيحة، **التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها**"، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية، مركز البحوث القانونية والقضائية، المنعقد 18جانفي 2020.

4) نوي أحمد، قداوري فاطمة الزهرة، مداخلة: **بعنوان رؤية قانونية للجريمة الإلكترونية وضوابط التصدي لها في القانون الجزائري**، في الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات

الجنائي، ط الأولى، الولايات المتحدة الأمريكية: المركز المغاربي شرق أدنى للدراسات الاستراتيجية، جانفي 2024.

- **المحاضرات.**

1) بن دراج علي إبراهيم، **محاضرات في الجرائم المعلوماتية**، موجهة لطلبة السنة الثانية ماستر، المركز الجامعي آفلو، 2021.
2) بوزيادية جمال، **الأمن السيبراني**، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص استراتيجية ودولية، جامعة الجزائر 3، كلية العلوم السياسية والعلاقات الدولية،2021.

خامسا: المواقع الإلكترونية.

1) بارة سمير، **الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Security Cyber) في الجزائر: الدور والتحديات** https://dspace.univ-ouargla.dz/jspui/bitstream/123456789/14049/1/%D8%AF-%D8%A8%D8%A7%D8%B1%D8%A9_%D8%B3%D9%85%D9%8A%D8%B1.pdf أطلع عليه بتاريخ 01 ماي 2025 ، الساعة 17:30
2) **استخدام الإنترنت لأغراض إرهابية**، مكتب الأمم المتحدة المعني بالمخدرات والجريمة **(UNDC)**، الأمم المتحدة، نيويورك، 2012، https://www.unodc.org/documents/congress/background-information/Terrorism/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf ، أطلع عليه بتاريخ 01 ماي 2025 ، الساعة 17:50.
3) الجزيرة، "**مجموعة الثماني**"، الجزيرة نت، الرابط : https://www.aljazeera.net/news/2008/7/6/%D9%85%D8%AC%D9%85%D9%88%D8%B9%D8%A9-%D8%A7%D9%84%D8%AB%D9%85%D8%A7%D9%86%D9%8A ، اطلع عليه بتاريخ 16 ماي 2025.
4) باشوش نوارة ، "**14 ألف جريمة سيبرانية في 2023 والتسوق الإلكتروني في الصدارة** "، الشروق أونلاين، 18 فبراير 2024، الرابط: https://www.echoroukonline.com/14-%D8%A3%D9%84%D9%81-%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%81%D9%8A-2023-%D9%88%D8%A7%D9%84%D8%AA%D8%B3%D9%88%D9%82-

%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA ، اطلع عليه 13 مايو 2025، الساعة 10:00.

5) باشوش نوارة ، "**توقيف 1410 شخص ينشطون في 'تيك توك' ومواقع أخرى** "، الشروق أونلاين، 14 مارس 2025، الرابط :
https://www.echoroukonline.com/%D8%AA%D9%88%D9%82%D9%8A%D9%81-1410-%D8%B4%D8%AE%D8%B5-%D9%8A%D9%86%D8%B4%D8%B7%D9%88%D9%86-%D9%81%D9%8A-%D8%AA%D9%8A%D9%83-%D8%AA%D9%88%D9%83-%D9%88%D9%85%D9%88%D8%A7%D9%82%D8%B9-%D8%A3%D8%AE ، اطلع عليه في 01 ماي 2025، الساعة 10:00 .

6) باشوش نوارة ، "**14 ألف جريمة سيبرانية في 2023 والتسوق الإلكتروني في الصدارة** "، الشروق أونلاين، 18 فبراير 2024، الرابط:https://www.echoroukonline.com/14-%D8%A3%D9%84%D9%81-%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%81%D9%8A-2023-%D9%88%D8%A7%D9%84%D8%AA%D8%B3%D9%88%D9%82-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA ، اطلع عليه 13 مايو 2025، الساعة 10:00.

7) باشوش نوارة ، "**توقيف 1410 شخص ينشطون في 'تيك توك' ومواقع أخرى** "، الشروق أونلاين، 14 مارس 2025، الرابط :
https://www.echoroukonline.com/%D8%AA%D9%88%D9%82%D9%8A%D9%81-1410-%D8%B4%D8%AE%D8%B5-%D9%8A%D9%86%D8%B4%D8%B7%D9%88%D9%86-%D9%81%D9%8A-%D8%AA%D9%8A%D9%83-%D8%AA%D9%88%D9%83-%D9%88%D9%85%D9%88%D8%A7%D9%82%D8%B9-%D8%A3%D8%AE ، اطلع عليه في 01 ماي 2025، الساعة 10:00 .

8) "**الأمن السيبراني مفهومة وتاريخه**"، الجزيرة نت، الرابط:
https://www.aljazeera.net/encyclopedia/2024/9/19/%D8%A7%D9%84%D8%A3%D9%85%D9%86-

%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%85%D9%81%D9%87%D9%88%D9%85%D9%87-%D9%88%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE%D9%87.

اطلع عليه بتاريخ 21 أفريل 2025، الساعة 00:30.

9) **تاريخ الأمن السيبراني**، موضوع، الرابط:

https://mawdoo3.com/%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE_%D8%A7%D9%84%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A#google_vignette ، أطلع عليه بتاريخ 23 أفريل 2025، الساعة 00:50.

10) **الحرب السيبرانية تتصاعد ضد الجزائر، جريدة الإخبارية ، 15 فيفري 2023**، الرابط: https://elikhbaria.dz/الحرب-السيبرانية-تتصاعد-ضد-الجزائر/، اطلع عليه بتاريخ 13 ماي 2025، الساعة 14:40.

11) مسلم محمد ، **"تحذيرات من الاختراق والتجسس على هواتف الجزائريين"**، الشروق أونلاين، 24 جانفي 2022، الرابط :

https://www.echoroukonline.com/%D8%AA%D8%AD%D8%B0%D9%8A%D8%B1%D8%A7%D8%AA-%D9%85%D9%86-%D8%A7%D9%84%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D9%88%D8%A7%D9%84%D8%AA%D8%AC%D8%B3%D8%B3-%D8%B9%D9%84%D9%89-%D9%87%D9%88%D8%A7%D8%AA%D9%81#google_vignette ، اطلع عليه بتاريخ: 16 ماي 2025، الساعة 14:54.

12) **حماية المستهلك تحذّر مستخدمي "بريدي موب" من الاحتيال، جريدة الإخبارية الجزائرية** ، الرابط:

https://elikhbaria.dz/%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B3%D8%AA%D9%87%D9%84%D9%83-%D8%AA%D8%AD%D8%B0%D8%B1-%D9%85%D8%B3%D8%AA%D8%AE%D8%AF%D9%85%D9%8A-%D8%A8%D8%B1%D9%8A%D8%AF%D9%8A-%D9%85%D9%88/

،اطلع عليه بتاريخ 13ماي 2025 ،الساعة 10:00.

13) **موسى عمر، عادل عبد الفتاح**، "قياس تأثير الإفصاح عن مخاطر الإنترنت على تكاليف رأس المال المقترض والمال المملوك: دراسة تطبيقي"، **مجلة الدراسات المالية والإدارية،**

المجلد 16، العدد 04 ، ديسمبر 2024، ص 424، الرابط :
https://masf.journals.ekb.eg/article_396234_4d460fe7842005bfb947b81b9758dec1.pdf، تم الاطلاع عليه في **13ماي 2025، الساعة 12:00.**

1) Anurag Lal, **"The Evolution Of Cybersecurity And How Businesses Can Prepare For The Future"**, Forbes, Idonet, 14 Aug 2023, available at: https://www.forbes.com/councils/forbesbusinesscouncil/2023/08/14/the-evolution-of-cybersecurity-and-how-businesses-can-prepare-for-the-future/, accessed in: 21 Apr 2025, at: 00:15.
2) BENDOUKHA Mohammed Reda, BOUFELDJA Kalloum, " **Strengthening Cybersecurity of Public Accounting Data in Algeria: A Comparative Analysic of Gaps and Challenges with Developed Countries**", Revue des Arts, Linguistique, Littérature & Civilisations, vol 2, no 11 September 2024, Université Peleforo Gon Coulibaly – Korhogo, p20 , available at: file:///C:/Users/user/OneDrive/Documents/%D8%A7%D9%83%D8%B3%D9%84/01-Art.-Bendou-1.pdf , accessed in: 13 May 2025.
3) **Christopher Hill**, "**What are the motives behind cybercrimes ?**", Chill Cyber Security, Idonet, 20 May 2024,availablei at : https://www.chillcybersecurity.co.uk/what-are-the-motives-behind-cybercrimes/ Accesed :18 Apr 2025 ,at : 23:31.
4) Courtny Goodman, **"AI in Cybersecurity: Transforming Threat Detection and Prevention"**, Balbix, Idonet, 16 Jan 2025, available in : https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ , accessed: 23 Apr 2025, at: 01:00.
5) FBI, **"The FBI Released Its Internet Crime Report 2024**", Federal Bureau of Investigation, April 16, 2024 available at: https://www.fbi.gov/contact-us/field-offices/atlanta/news/the-fbi-released-its-internet-crime-report-2024, Accessed in : May 12 2025, at 13 :02
6) **Kaspersky ICS CERT, "Statistics"** Published by **AO Kaspersky Lab** in **2025**, available in: https://ics-cert.kaspersky.com/statistics/ ,accessed in : **May 13 2025, at 22 :00.**
7) Kepios, Digital 2025: Algeria, Data Reportal, 2025, available at: https://datareportal.com/reports/digital-2025-algeria, accessed in: 10 May 2025, at: 00:00.

8) Mix Mode, **"Global Cyber crime Report 2024: Which Countries Face the Highest Risk?"** Mix Mode Blog, April 112024, available at:https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/ Accessed in: May 12 2025, at 13 :20

9) **NETSCOUT Systems Inc**, **"Algeria - Latest Cyber Threat Intelligence Report",** NETSCOUT DDoS Threat Intelligence Report, published for **July–December 2024,** available at: https://www.netscout.com/threatreport/emea/algeria/, accessed : May 13 2025, at 15 :00.

10) United Nations Department of Economic and Social Affairs," **E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development**", New York: United Nations, 2024, available at:https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf ، accessed in: 13 May 2025, at: 10:00.

11) **United Nations , "E-Government Survey 2024",** Department of Economic and Social Affairs, United Nations. Published in 2024, available in: https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf ,accessed in : May 13 2025, at 14 :2