

جامعة عمار ثليجي الأغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق



عنوان

الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية

مذكرة في اطار مقتضيات نيل شهادة الماستر في القانون

تخصص: قانون دولي عام

اشراف الأستاذ:

رابحي لخضر

اعداد الطالبة:

_ رابحي مسعودة

لجنة المناقشة

الصفة	
رئيسا	الدكتور بن عطية لخضر
مناقشا	الدكتور شويرب جيلالي
مشرفا	الدكتور رابحي لخضر

السنة الجامعية: 2025-2026



شكر وعرفان

بسم الله الرحمن الرحيم، والحمد لله رب العالمين

الذي منحني القوة وساعدني على إنهاء هذا البحث والخروج به بهذه الصورة
الممتازة، فبالأمس القريب بدأت مسيرتي التعليمية وانا انظر إلى يوم التخرج كأنه
يوم بعيد، وإن هذا البحث الذي اقدمه لكم يحمل في طياته معلومات هامة بذلت
مجهودًا عظيمًا لدراستها وجمعها ليظهر لكم بهذا الشكل،

وإيمانًا بمبدأ أنه لا يشكر الله من لا يشكر الناس، فأني اتوجه بالشكر الجزيل
للأستاذ الدكتور "رابحي لخضر" الذي ساعدني كثيرًا في مسيرتي لإنجاز وكتابة هذا
البحث وكان له دورًا عظيمًا من خلال تعليماته ونقده البناء ودعمه الأكاديمي،
وأخيرًا أتوجه بشكر خاص للأستاذة الذين درسونا طيلة مسيرتنا الجامعية



اهداء

أهدي ثمرة جهدي المتواضع إلى سبب وجودي في
الحياة، وقرة عيني، ورمز العطاء والمحبة؛ أُمي
الغالية وأبي العزيز، حفظهما الله وأطال في عمرهما
جزاء ما قدماه لي من دعم لا ينضب
إلى سندي وعزوتي، إخوتي وأخواتي الأوفياء، الذين
شاركوني الدرب وكانوا لي خير معين
إلى الروح الطاهرة التي ترفرف في سماء ذاكرتي، إلى
ابنتي الغالية جيهان، أسكنها الله فسيح جناته
وجعلها شفيعة لنا
إلى منارة العلم وفخر جامعة عمارثليجي بالأغواط،
أستاذنا الفاضل زازة لخضر، فقيه القانون الدولي
الذي ألهمنا بعلمه وترك بصمة علمية لا تمحى في
نفوس طلابه
إلى كل الأساتذة الأفاضل الذين لم يبخلوا علينا
بعطائهم وتوجيهاتهم طوال مسيرتنا الدراسية، لكم
مني كل التقدير والامتنان

رابحي مسعودة

مقدمة

مقدمة:

يشهد عالمنا المعاصر ثورة تكنولوجية هائلة، غيرت مسار الحياة البشرية فأصبحت الأنظمة الرقمية والمعلومات شريان القطاعات الحيوية للدول، وفي ظل هذا التطور التقني المتسارع ظهر جانب مظلم لهذا الفضاء الرقمي يتمثل في الجريمة السيبرانية التي أصبحت في العصر الراهن تشكل تحدياً قانونياً وأمنياً غير مسبوق نتيجة للتحويل الرقمي الشامل وانتشار استخدام تقنيات المعلومات والاتصالات التي تغلغلت في كافة مجالات الحياة فلم تعد هذه الجرائم مجرد أفعال محدودة و استثنائية بل أوجدت عالماً افتراضياً موازياً للعالم الواقعي بات مجالاً خصباً لارتكاب أنماط إجرامية مستحدثة تمس حقوق الأفراد وخصوصياتهم وأمن الدول مما أصبحت تشكل خطر بات يهدد الأمن القومي للدول، واستقرارها الاقتصادي والاجتماعي وحتى السياسي. و بالنظر للخصوصية الفريدة لهذه الجرائم وقدرتها على عبور الحدود الجغرافية والحدود الرقمية بكبسة زر وجدت المنظومات التشريعية التقليدية نفسها أمام تحدي كبير فلم تعد القوانين الكلاسيكية قادرة على استعاب هذا النوع من الإجرام السيبراني وهنا تحول الاهتمام الدولي و الوطني باتجاه البحث عن آليات قانونية و مؤسساتية قادرة على ضبط هذا الفضاء وحمايته من الأخطار دون المساس بالحريات الفردية و مبدأ سيادة الدول الجغرافية والرقمية.

تنبثق أهمية دراسة آليات مكافحة الجريمة السيبرانية من خطورتها المتزايدة وتأثيراتها الاقتصادية والاجتماعية العميقة، حيث لم يعد هناك قطاع إداري أو مالي كالبنوك والمؤسسات الحكومية إلا و بات يعتمد بشكل رئيسي على أنظمة المعلومات، مما يجعلها عرضة للتهديدات المستمرة.

كما تبرز الأهمية في حجم الخسائر الاقتصادية حيث تشير التقديرات الدولية إلى أن هذه الجرائم تكبد الاقتصاد العالمي مليارات الدولارات سنوياً من خلال عمليات الاحتيال وسرقة الهوية.

كذلك طبيعتها العابرة للحدود حيث تتسم هذه الجرائم بتجاوزها للحدود الجغرافية، والرقمية مما يجعل التشريعات الوطنية قاصرة وحدها و غير كافية لمواجهتها، ويستوجب وجود تعاون دولي فعال امام قصور القواعد التقليدية و عجز النصوص الجنائية الكلاسيكية عن استيعاب الطبيعة التقنية والمعنوية لهذه الجرائم، مما يفرض ضرورة إيجاد أطر قانونية متطورة تركز مبدأ الشرعية الجنائية.

يسعى هذا البحث إلى دراسة وتحليل الآليات القانونية والمؤسساتية والتقنية المتبعة لمواجهة الظاهرة الإجرامية السيبرانية، وذلك من خلال تحقيق الأهداف التالية:

- توضيح ماهية الجريمة السيبرانية وخصائصها الفريدة التي تميزها عن الجريمة التقليدية

-رصد وتحليل الآليات الدولية والاتفاقيات الإقليمية مثل اتفاقية بودابست 2001 اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية 2024 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تهدف إلى توحيد الجهود العالمية.

- تسليط الضوء على الآليات الوطنية والتشريعات المقارنة، وبيان مدى ملاءمتها للتطورات التقنية المتسارعة مثل الذكاء الاصطناعي .

-استعراض التحديات الإجرائية والموضوعية التي تواجه سلطات إنفاذ القانون في عمليات تتبع وضبط مرتكبي هذه الجرائم.

- تقديم رؤية تحليلية نقدية تهدف إلى تعزيز فاعلية المواجهة القانونية لهذه الجرائم على المستويين الوطني والدولي.

تعددت الدوافع التي أدت إلى اختيار موضوع الجرائم السيبرانية، وتتمثل أبرزها في:

- الرغبة في إثراء البحث القانوني والمكتبة الجامعية بدراسات متخصصة حول الجريمة الإلكترونية، باعتبارها ظاهرة مستحدثة ومعقدة.

- الشغف للتعلم في ظاهرة الجريمة السيبرانية كونها تلامس الحياة اليومية

-حدثة الموضوع وأهميته المتزايدة نظراً للاعتماد الواسع والمتزايد على التكنولوجيا في مختلف مجالات الحياة، مما جعل من الضروري دراسة المخاطر القانونية المرتبطة بها

- التحول الرقمي العالمي مواكبة التحول الجذري الذي فرضه العصر الرقمي، وما نتج عنه من أنماط إجرامية عابرة للحدود تختلف عن الجرائم التقليدية.

ومن ابرز الدراسات السابقة التي اعتمدت عليها فقد استندت إلى أبحاث أكاديمية ومقالات حديثة متخصصة، منها مهداوي حنان في دراستها "التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري" 2022 و خلدون عيشة في مقال "الجريمة المعلوماتية في القانون الدولي والجزائري" 2023 مهدي رضا في بحثه "الجرائم السيبرانية وآلية مكافحتها في التشريع الجزائري" 2021 مشة نسرین وونام بغیانی في دراستهما حول "الجرائم المستحدثة وآليات التصدي لها في التشريع الجزائري" اما بالنسبة الدراسات المتخصصة في التشريع المصري والمقارن لإثراء الجانب المقارن من الدراسة، استعنت بمراجع مصرية وعربية حديثة: الدكتور رامي متولي القاضي في دراسته العميقة

"المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري و بوبصلة أمانة في بحثها حول الإستراتيجية المصرية في مكافحة التهديدات والجرائم السيبرانية" وفريد ناشف في بحثه حول "آليات التعاون الدولي في مكافحة الجرائم الإلكترونية"

اما الصعوبات التي واجهتني خلال الدراسة:

- قلة المراجع المتخصصة و ندرة الدراسات والمصادر الأكاديمية المكتوبة باللغة العربية التي تتناول هذا الموضوع بشكل معمق بسبب حداثة.

- تغير الأطر القانونية صعوبة الإحاطة الشاملة بجميع القوانين والاتفاقيات الدولية، كونها تتسم بالتغير المستمر والتطور السريع لملاحقة التقنيات الجديدة

- الطبيعة التقنية المعقدة يتطلب الموضوع فهماً لجوانب معلوماتية وأمنية وتقنية دقيقة تتجاوز النطاق القانوني الصرف، مما يزيد من تعقيد البحث.

الاشكالية :

ما مدي فعالية الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية ؟

الاسئلة الفرعية:

1- ماهي الجريمة السيبرانية وماهي اهم خصائصها وصورها واثارها ؟

2- كيف نظم المجتمع الدولي آليات لمواجهة هذه الجريمة؟

3- كيف واجه المشرع الجزائري والمصري الجريمة السيبرانية؟

اما بالنسبة لمنهج الدراسة المعتمد من قبلي فهو المنهج الوصفي التحليلي ، من خلال وصف هذه الجريمة وابرار خصائصها و استعراض وتحليل النصوص القانونية المتعلقة بالجريمة السيبرانية بالإضافة الى المنهج المقارن عند دراسة جهود الدول والمنظمات الدولية في التصدي لهذه الجريمة والمقارنة بينها وتخصيص دراسة مقارنة بين التشريع الجزائري والتشريع المصري في مكافحة الجريمة السيبرانية

اما عن الخطة المتبعة فهي كالتالي :

تطرقنا في الفصل الاول و المعنون بالاطار المفاهيمي والقانوني للجريمة السيبرانية فقسمناه الى مبحثين المبحث الاول مدلول الجريمة السيبرانية الذي قسمناه الى ثلاثة مطالب المطلب الاول مفهوم الجريمة السيبرانية فقها وتشريعا المطلب الثاني خصائص الجريمة السيبرانية المطلب الثالث اركان الجريمة السيبرانية اما المبحث الثاني فهو بعنوان صور الجريمة السيبرانية واثارها فتناولنا في المطلب الاول انواع الجريمة السيبرانية المطلب الثاني اثار الجريمة السيبرانية .

الفصل الثاني والمعنون بالآليات القانونية والمؤسسية على المستويين الدولي والوطني لمكافحة الجرائم السيبرانية وقد قسمناه الى مبحثين تناولنا في المبحث الاول اليات مواجهة الجريمة السيبرانية على المستوى الدولي فقسمناه الى ثلاثة مطالب المطلب الاول الآليات القانونية الدولية في مكافحة الجريمة السيبرانية المطلب الثاني الآليات المؤسسية الدولية لمكافحة الجريمة السيبرانية اما المطلب الثالث فهو اليات التعاون الدولي في مكافحة الجريمة السيبرانية ، اما المبحث الثاني فعنوانه اليات مواجهة الجريمة السيبرانية على المستوى الوطني (دراسة مقارنة بين التشريع الجزائري والمصري) فقسمناه الى ثلاثة مطالب المطلب الاول الآليات القانونية الوطنية في مكافحة الجريمة السيبرانية المطلب الثاني الآليات المؤسسية الوطنية في مكافحة الجريمة اما المطلب الثالث فهو مدى انسجام وفعالية التشريعين الجزائري والمصري مع المعايير الدولية .

الفصل الأول

الإطار المفاهيمي والقانوني للجرائم
السيبرانية

يعد ضبط الإطار المفاهيمي لأي بحث علمي من المراحل الأساسية التي تساعد على الإحاطة بموضوع البحث وفهم أبعاده المختلفة خاصة إذا تعلق الأمر بموضوع حديث ومتجدد كالجريمة السيبرانية التي تطورت بتطور تكنولوجيا المعلوماتية، إذ أصبحت تشكل تهديدا للأمن على كافة الأصعدة على المستويين الدولي والوطني.

ومن هذا المنطلق نسعى في هذا الفصل إلى تحديد الأسس النظرية و المفاهيمية المهمة لدراسة هذه الجريمة المستحدثة من خلال تبيان مفهوم هذه الجريمة وتوضيح خصائصها والتعريف على أركانها وصورها، كذلك ما يترتب عليها من آثار تنعكس على الجانب والاقتصادي والاجتماعي والقانوني والسياسي، وعلى هذا الأساس تم تقسيم هذا الفصل الى مبحثين كمايلي :

المبحث الاول: دراسة مدلول الجرائم السيبرانية من حيث مفهومها وخصائصها واركائها
اما المبحث الثاني: فهو يعالج صور الجرائم السيبرانية واثارها.

المبحث الأول: مدلول جرائم السيبرانية

تعد الجريمة السيبرانية من الجرائم المستحدثة التي دوخت العالم نظرا للغموض الذي يشوبها منذ ظهورها مما اثار فضول الفقهاء والمشرعين والباحثين الأكاديميين على حد سواء للتمحس فيها من اجل ضبط مفهومها وتحديد عناصرها وكشف خصائصها ، وبدورنا حاولنا في هذا المبحث ابراز المفاهيم التي لها علاقة بالجرائم السيبرانية من خلال توضيح مفهومها وخصائصها واركائها مما يتيح لنا فهم جوهرها وتمييزها عن غيرها من الجرائم.

المطلب الأول: مفهوم الجرائم السيبرانية

أدى التطور التكنولوجي المتسارع الى ظهور نمط جديد من الجرائم يعرف بالجرائم السيبرانية التي يعتبر الحاسوب وشبكة الانترنت أدواتها، فهي تختلف عن الجرائم التقليدية بالنظر الى خصوصيتها وطبيعتها، فأخذت عدة تسميات للدلالة عليها فتعددت تسميتها، وتعددت التعارف الفقهية منها بالأخص، كما تناولتها التشريعات الوطنية بمسميات مختلفة .

الفرع الاول :تطور مصطلح الجريمة السيبرانية بتطورها

لم تستقر الجريمة السيبرانية على هذه التسمية إلا بعد تطور تدريجي ارتبط ارتباطا وثيقا بتطور الوسائل التكنولوجية ذاتها "إن تطور مفهوم الجريمة السيبرانية كان يتطور بتطور هذه التقنية واستخدماتها ففي الستينيات والسبعينيات أي بداية ظهورها ظهر أولى معالجات ما يسمى الكمبيوتر فظهرت جرائم الكمبيوتر في الستينيات ، واقتصرت في بدايتها على مواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير الأنظمة والتجسس المعلوماتي أين ثار الجدل حول ما إذا كانت هذه الأفعال جرائم قانونية أم مجرد سلوكيات غير أخلاقية في مهنة الحوسبة ، ومع منتصف السبعينات وانتشار الحواسيب الشخصية أكثر بدأت النظرة تتغير فبدأت الدراسات على أنها ظاهرة إجرامية مستجدة ¹.

اما في الثمانينات برز مفهوم جديد ارتبط بعمليات اقتحام الأنظمة عن بعد وانتشرت الفيروسات الالكترونية المدمرة فشاع مصطلح "الهاكرز" للتعبير عن مقتحمي الأنظمة ، وكانت حينها دوافعها محصورة في الجانب السياسي والعسكري أو بسبب رغبات شخصية أين تسببت في خسائر مالية حينها

¹ سعيدي سليمة،حجازي بلال، جرائم المعلومات والشبكات في العصر الرقمي ،ط 1، دار الفكر الجامعي الإسكندرية مصر2017 ، ص 57،

حيث سجلت وزارة العدل الأمريكية سنة 1986 خسائر للبنوك بسبب الاحتيال وكان عام 1988 نقطة تحول هامة بعد حادثة "دودة موريس" التي هاجمت آلاف الحواسيب مما لفت الأنظار الى أهمية أمن الشبكات¹.

وفي مرحلة التسعينيات عندما انتشرت الانترنت انتشارا هائلا شهدت هذه العشرية تغيرا جذريا في نطاق ومفهوم الجريمة الالكترونية بفعل ظهور شبكة الإنترنت التي سهلت اختراق الأنظمة أين ظهرت صور إجرامية جديدة لم تعرف من قبل مثل "أنشطة إنكار الخدمة" التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد مما سبب خسائر بالملايين وانتشرت جرائم نشر الفيروسات عبر مواقع الانترنت.

ثم تطورت هذه الجريمة من 2016 الى 2020 فتطورت الأساليب الإجرامية لتشمل اختراق أنظمة السيارات المتصلة بالإنترنت ثم انتقلت الهجمات لاستهداف المؤسسات من خلال النظم المنزلية للموظفين لكونها اقل أمانا او الاستيلاء على البيانات البنكية والرواتب ، وزاد خطر برامج الفدية والاختراقات وتخزين وبيع البيانات المسروقة²

فهناك تباين كبير فيما يخص المصطلحات المستخدمة للدلالة على هذه الجريمة رافقتها منذ نشأتها و تطورت بتطور هذه الظاهرة المتصلة بتقنية المعلومات منها: إساءة استخدام الكمبيوتر ثم احتيال الكمبيوتر ، الجريمة الالكترونية ، جرائم الكمبيوتر والانترنت، جرائم التقنية العالية ، جرائم المعلوماتية ، والجرائم الرقمية، والسيبر كرايم ، جريمة أصحاب ألياقات البيضاء ، والجرائم الناعمة والجرائم النظيفية ، ان هذا التعدد في التسميات والمصطلحات تعددا يحمل صورة التنوع والثراء لا التنازع والتضاد ، فهي كلها جرائم تطل المعلومات والمعرفة في أثواب متعددة³

¹ سعيدي سليمة، حجازي بلال المرجع السابق، ص 58،

² سعيدي سليمة ، حجازي بلال المرجع نفسه، ص 59،

³ سعيدي سليمة، حجازي بلال ، المرجع نفسه، ص 55

"وأيا كانت التسمية لا بد لها وبشكل مجرد من أن تكون دالة على المسمى ، وذلك بشمولها الجوانب المتعددة له ، بحيث يكون المصطلح دالا دلالة قاطعة على الموصوف"¹

وقد استقر الفقه القانوني المعاصر على استعمال مصطلح الجرائم السيبرانية Cyber Crimes، وهو إحدى المصطلحات الحديثة والمستخدمة للدلالة على جرائم الانترنت ، نظرا لكونه الأكثر شمولاً بحيث يغطي كل الجرائم المرتبطة بالفضاء الرقمي والأنظمة المعلوماتية والشبكات الالكترونية ، سواء كانت متصلة بالانترنت أم لا "وقد صيغ مصطلح الجريمة السيبرانية لأول مرة من قبل وليام جيبسون في عام 1982"²

الفرع الثاني : تعريف الجرائم السيبرانية فقها

أولى الفقه القانوني عناية بالجرائم السيبرانية في محاولة منه لمواكبة التطور الكبير لهذه الجريمة من اجل الإلمام بجميع عناصرها الأمر الذي أدى إلى تعدد التعاريف الفقهية لهذا النوع من الجرائم نتيجة لإختلاف الزوايا التي تناولها منها فقهاء القانون فمنهم من تناولها من منظور أداة ارتكابها ومنهم من تناولها من حيث محل الجريمة ومنهم من عرفها بالنظر الى طبيعة النشاط الإجرامي أو الدافع من وراء ارتكابها فمنهم من ضيق من مفهومها ومنهم من حاول التوسيع في مفهومها .

1-الاتجاه المضيق في تعريف الجريمة السيبرانية:

فقد عرفت بأنها: " جرائم المعلوماتية والانترنت هي تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر والانترنت في أعمال وأنشطة إجرامية عادة ما ترتكب بهدف أن تحقق عوائد مالية ضخمة جراء أعمال غير شرعية يعاد ضحها في الاقتصاد الدولي عبر شبكة الانترنت باستخدام النقود الالكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الانترنت أو تداول

¹ اسامة احمد المناعسة، جلال محمد الزغبى ، جرائم تقنية نظم المعلومات الالكترونية دراسة مقارنة ، ط2 ، دار الثقافة للنشر والتوزيع ، عمان ، 2014 ، ص67

² مانيو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة ،مجلة القانون والتنمية ، جامعة طاهري محمد بشار ، الجزائر - المجلد 4/ العدد 1 سنة 2022 ص53

الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة.¹

والجدير بالذكر أن هذا التعريف يركز على وسيلة ارتكاب هذه الجرائم وهي الحاسوب والإنترنت باعتبارها أداة التكنولوجيا الحديثة كما يشير هذا التعريف الى الدافع الربحي لهذه الجرائم، كما أن هذا التعريف يميز بين الجرائم السيبرانية والجرائم التقليدية من خلال الأداة المستعملة ألا وهي الكمبيوتر والإنترنت مبرزاً خصوصيتها التقنية، غير انه تعريف ضيق فقد اغفل بعض الجوانب كالأثر الاجتماعي والسياسي لهذه الجرائم كما انه يعاب عليه استبعاد دوافع أخرى لارتكاب هذه الجريمة بجانب الدافع المالي فهناك جرائم تكون ذات دوافع غير ربحية مثل التجسس أو التخريب، غير انه بشكل عام تعريف تناول العناصر الأساسية لهذه الجريمة ويمكن تطويره حيث يصبح أكثر توازناً وشمولية.

كما عرفت بأنها "سلوك غير مشروع معاقب عليه قانوناً صادر عن إرادة جرميه محله معطيات الكمبيوتر"²

ونقول بان هذا التعريف دقيق من حيث تحديد العناصر الأساسية للجريمة وهي وجود إرادة جرميه محلها معطيات الحاسوب أي التكنولوجيا الرقمية ، غير انه اهمل الدافع من وراء ارتكاب هذه الجريمة كالربح المالي ، والتجسس وغيره.

وهناك من عرف الجريمة المعلوماتية بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب والتي تتعلق بالمعالجة الآلية للبيانات"³

والملاحظ أن هذا التعريف ضيق ركز على الأفعال غير مشروعة فحصرها في النسخ أو تغيير أو الحذف أو الوصول غير مصرح بيه الى المعلومات كما حدد الأداة وهي الحاسوب والمعالجة الآلية للبيانات.

1 عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت الجرائم الالكترونية دراسة مقارنة في النظم القانونية لمكافحة جرائم المعلوماتية والانترنت مع الاشارة الى جهود مكافحتها محليا وعربيا ودوليا ط1 ، منشورات الحلبي الحقوقية، بيروت، 2007 ، ص 15

2 امير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، ط1 ، مكتبة الوفاء القانونية ، الاسكندرية 2011 ، ص 75.

3 عبد الاله النوايسة ، جرائم تكنولوجيا المعلومات، شرح الاحكام الموضوعية في قانون الجرائم الالكترونية، ط1، دار وائل للنشر والتوزيع الاردن - عمان ، 2017 ، ص 41

ومن التعريفات : "إساءة استخدام تكنولوجيا المعلومات والاتصالات بين المجرمين بالتبادل أو إساءة استخدام الكمبيوتر"¹

المتمعن في هذا التعريف يلاحظ أن مصطلح إساءة استخدام تكنولوجيا المعلومات لا تشمل كل أنواع الجرائم السيبرانية بل ان إساءة الاستخدام هي جزء من الإجرام المعلوماتي فهي تقع على النظام والبيانات مثل الاختراق وذلك عن طريق الدخول غير المصرح به لقاعدة البيانات او عن طرق الاتلاف بإرسال فيروسات لتدمير الملفات فإساءة استخدام تكنولوجيا المعلومات تعني الانحراف في استعمال الوسيلة والوسيلة هنا وسيلة تقنية متاحة لشخص ما وبالتالي فإساءة استخدام تكنولوجيا المعلومات هي احد صور الجريمة السيبرانية.

واتجه جانب من الفقه الفرنسي حيث يرى الاستاذ "Massa" ان المقصود بها "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية لغرض تحقيق الربح"² ، ووجدنا تعريف للجريمة التقنية للأستاذ "ماسا" في كتاب جرائم تقنية نظم المعلومات الالكترونية دراسة مقارنة للقاضي اسامة احمد المناعسة وجمال محمد الزغبى هي: "الاعتداء القانوني الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الجريمة"³

ونقول بان هذا التضارب في نقل تعريف الفقيه " ماسا" يرجع في تصورنا الى ترجمة النص الاصلي من اللغة الفرنسية الى العربية ، بين الباحثين العرب فيظهر هنا الاختلاف في المصطلحات في النصين ، ادى الى اختلاف كبير في المعنى بين النصين ،النص الاول « لغرض تحقيق الربح» يضيق من نطاق الجريمة السيبرانية فجعل الهدف منها ربحي، اما النص الثاني «بغرض تحقيق الجريمة هو نص اشم من سابقه فكلمة جريمة تشمل اي نتيجة اجرامية فقد تكون مساس بأمن الدولة او مساس بالحياة الخاصة او المساس بحقوق ، التشهير ، الحاق الضرر، الاهداف السياسية ، او مجرد التسلية الى غيرها من الدوافع، ونرى نحن بأن النص الثاني هو الأرجح بالنظر الى توافقه مع طبيعة الجريمة الالكترونية واتساقه معها.

1شويرب جيلالي و مراد فايزة ، الاليات الدولية والوطنية لمكافحة الجريمة السيبرانية، مجلة الدراسات القانونية والسياسية جامعة عمار ثلجي الاغواط الجزائر المجلد 09 العدد 2/ 2023 ، ص 156

2 غانم مرضى الشمري، الجرائم المعلوماتية ماهيتها. خصائصها. كيفية التصدي لها قانونا، ط1، دار الثقافة، عمان 2016، ص25

3 اسامة احمد المناعسة وجمال محمد الزغبى المرجع السابق، ص70

من جهة أخرى الجريمة فعل غير مشروع أو اعتداء غير قانوني وإذ امعنا النظر في هذا التعريف لـ "ماسا" نجد انه وصف الجريمة بأنها اعتداءات قانونية أو اعتداء قانوني وهذا وصف خطأ فكيف يمكن تصور ان تكون الاعتداءات قانونية فكان الأجدر به القول اعتداءات غير قانونية أو فعل غير مشروع، ولا يخرج هذا التعريف من النظرة المضيقفة للجريمة الالكترونية.

وهناك تعريف اخر للفقهاء "دول" وهو: "كل فعل إجرامي يستخدم الحاسب الآلي لإتمامه" وهذا التعريف يركز بالدرجة الاولى على اداة الجريمة الى وهي الحاسب الآلي فهو بدوره تعريف ضيق.

وفي نفس الاتجاه سار الفقيه "لميتو" بتعريفها " الفعل غير المشروع الذي يستخدم فيه الحاسب الآلي كأداة رئيسية" ¹ فكان تعريفه مرتكزا على الأداة وهي الحاسب الآلي، إن هذا الاتجاه من الفقه يربط بين الجريمة من حيث الصفة والأداة الرئيسية فحسبهم أنهم جعلوا من الجريمة جريمة تقنية أو جريمة انترنت كلما كان الحاسب الآلي ذاته أدواتها الرئيسية مما يكون قد اغفل جانبا كبيرا من الجرائم التقنية وهي التي يكون محلها مفردات الحاسب الآلي ذاته المعنوية منها بالأخص.

ومن التعريفات المضيقفة هي الاتجاه الذي يربط بين قوة ارتكاب الجريمة وبين وجود قدر كافي من المعرفة لدى الفاعل الى حد الإتيان إيماننا منهم ان جرائم التقنية جرائم ذات صلة بتقنية الحاسب الآلي فلا يرون وقوع الجريمة إلا من شخص لديه ذلك الإلمام بتقنية الحاسب ، كما يرى بأنه لا يجب الاندماج الكبير بين وقوع الجريمة ومدى براعة الفاعل او اتقانه لتقنية الحاسب الآلي فلا يتطلب ذلك البراعة الفائقة بل تكفي كبسة زر واحدة يجيدها أيا كان يملك جهاز حاسب آلي او شبكة المعلوماتية ²

ونقول انه بل يكفي فقط ان يمتلك مراهق جهاز هاتف ذكي لكي يرتكب هذه الجريمة او يشارك في ارتكابها على ان يكون له الحد الأدنى من المعرفة بتقنية الحاسوب لكي يرتكب الجاني هذه جريمة او يشارك فيها . فنحن مع هذا الري .

¹ اسامة احمد المناعسة وجلال محمد الزغبى، المرجع السابق، ص 69

² اسامة احمد المناعسة وجلال محمد الزغبى، المرجع نفسه ص 72

اما تعريف مكتب تقييم التقنية الامريكي بانها: "الجرائم التي تلعب بها البيانات والبرامج المعلوماتية دورا اساسيا"¹ وهو من التعريفات التي تستند الى وسيلة ارتكاب الجريمة .

2- الاتجاه الموسع في تعريف الجريمة السيبرانية :

ومن جهة اخرى اتجه جانب من الفقه الى محاولة التوسيع في تعريف الجريمة السيبرانية او الالكترونية غير انهم لم ينجحوا في الاحاطة بكل جوانبها ومن هذه التعريفات : " كل فعل او امتناع عمدي ،ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف الى الاعتداء على الاموال المادية او المعنوية "²

ويرى الاستاذ "تردمن" بأن : " الجريمة المعلوماتية تشمل اي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات "³

وهو تعريف اوسع بالمقارنة بتعريف الفقيه "ماسا" الا انه يعاب عليه انه ركز على الجانب المالي يفهم منه الجرائم الواقعة على المال مثل السرقة الالكترونية كما ربطها بالمعالجة الآلية للبيانات ، وما يمكن قوله هنا انه ليست كل الجرائم الالكترونية مالية فهناك الجرائم الالكترونية التي تقع على الاشخاص وهناك الجرائم الالكترونية التي تمس بأمن الدولة وهناك الجرائم الالكترونية الاخلاقية وهناك التي تتعلق بالملكية الفكرية بالإضافة الى الجرائم التي تقع على البيانات والأنظمة التقنية البحتة.

اما الفقيه الالمانى " ناريمان " فيعرفها بأنها : "كل اشكال السلوك غير المشروع او الضار بالمجتمع الذي يرتكب باستخدام الحاسب الالى"⁴ ، ويعتبر هذا التعريف اوسع من التعريفين السابقين - تعريف ماسا وتردمن - بحيث جأت فيه عبارة كل اشكال السلوك مما يوحي بشموله لكل صور الجرائم سواء اكانت مالية او سياسية او اخلاقية او واقعة على الاشخاص اوغيرها، كما انه يذكره لعبارة السلوك غير المشروع أي انه سلوك مخالف للقانون كما انه لا يهمل الدافع المحتمل - الضار بالمجتمع - وقد يختلف

¹ اسامة احمد المناعسة، جلال محمد الزغبى، المرجع السابق ، ص70

² نهلاء عبد القادر المومني، الجرائم المعلوماتية ، ط2، دار الثقافة للنشر والتوزيع ، 2010، ص 49

³ نهلاء عبد القادر المومني، المرجع نفسه ، ص 48

4 غانم مرضي الشمري، المرجع السابق ، ص 25

هذا الضرر من جريمة لأخرى وقد يتغير هذا الضرر فالأضرار، التي قد تمس بالمجتمع في المستقبل لا تكون معروفة في الوقت الراهن فتظهر اشكال اخرى للضرر كون الجرائم الالكترونية تتطور باستمرار.

وهناك تعريف موسع قام به الفقهاء **micel-credo** : "وهو سوء استخدام الحاسب الآلي او جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة الى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه او بياناته كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء كان هذا الارتداء على جهاز الحاسب ذاته ام المعدات المتصلة به وكذلك الاستخدام غير المشروع لبطاقات الائتمان وانتهاك كيانات الحاسب الالية بما تتضمنه من شيكات تمويل الحسابات المالية بطريقه الكترونيه وتزيف المكونات المادية والمعنوية للحاسب بل وسرقة جهاز الحاسب في صفاته او احد مكوناته"¹

وتم تعريفها: "كل نشاط ايجابي او سلبي من شأنه الاتصال دون وجه حق بالكيان المعنوي للحاسب الالي او بنظام المعلومات او الانترنت او التأثير عليه بتعطيله او اضعاف قدرته على اداء وظائفه بالنسخ او التعديل بالإضافة او الحذف الكلية او الجزئي او المناقلة للخصائص الأساسية للبرامج او مجرد النسخ او الوصول الى البرامج او المعلومات المخزنة او الوصول اليها اثناء نقلها او ارسالها او الاتصال بها من غير وجه حق باي وسيله كانت"²

ولعل هذا التعريف واسع و اكثر دقه وشمولية، اذ تناول كل اشكال النشاط غير المشروع سواء بالنسخ او تعديل او الحذف او الوصول غير المصرح به والمتعلق بالكمبيوتر وانظمة المعلومات او الانترنت كما تناول الجوانب التقنية و القانونية في تعريفها.

وذهب البعض الى القول بأن هذه الجرائم "هي كل عمل او امتناع عن عمل يأتيه الإنسان إضراراً بمكونات الحاسب المادية والمعنوية وشكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي يحميها القانون"³

1 غانم مرضي الشمري ، المرجع السابق، ص 25، 26

2 عبد الإله النوايسة ، المرجع السابق ، ص 41 ، 42 ، 43

3 مهدي رضا، الجرائم السيبرانية والية مكافحتها في التشريع الجزائري،مجلة ابلير للبحوث والدراسات الجامعية محمد بوضياف المسيلة الجزائر المجلد 06 العدد. 2021/12/13 ص 113

اما تعريف منظمه التعاون الاقتصادي والتنمية OECD 1983 فهي " كل سلوك غير مشروع او غير اخلاقي او غير مصرح به يتعلق بالمعالجة الاليه للبيانات او نقلها " ¹

وهناك تعريف بلجيكي من طرف خبراء متخصصون في معرض ردهم على استبيان منظمة التعاون والتنمية بأنها " كل فعل او امتناع عن فعل من شأنه الاعتداء على الامواج المادية او المعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية " ²

الفرع الثالث :تعريف الجرائم السيبرانية تشريعا

اذا كان فقهاء القانون قد واجهوا صعوبة في وضع تعريف جامع مانع للجريمة السيبرانية ولعل هذا يعود الى حداثة هذه الجريمة وتطورها التقني المتسارع وتداخلها مع عدة فروع قانونيه فإن المشرع لا يلام عن ذلك كون وظيفته الاساسية ليست التنظير المفاهيمي، بل وضع قواعد التجريم والعقاب لذلك نجد أن أغلب التشريعات الوطنية قد حددت الأفعال المجرمة عوض عن تقديم تعريف لهذا النوع من الجرائم وهذا لا يعاب على المشرع نقاديا للقصور التشريعي امام تطور هذه الجرائم و لعله اختيار مقصود من المشرع تماشيا مع تحقيق المرونة والفعالية في مكافحه هذا النوع من الجرائم لمواجهة طبيعتها المستحدثة.

اولا : تعريف الجريمة السيبرانية في التشريعات العربية

ومع ذلك فقط عرفها المشرع السعودي في المادة 1/8 بأنها "اي فعل يرتكب متضمنا استخدام الحاسب الآلي او الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" بهذا التعريف تبني المنظم السعودي المعيار الضيق في مجال الجريمة المعلوماتية. ³

¹ علوي علي، احمد الشارفي، الوجيز في جرائم تقنية المعلومات ، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية الاقتصادية و السياسية برلين المانيا، 2024، ص 34

² محمود احمد القرعان، الجرائم الإلكترونية، ط1، دار وائل للنشر والتوزيع عمان سنة 2017 ، ص 24

³ عبد الإله النوايسة ، المرجع السابق ،ص40

"اما المشرع المصري فلم يقدم تعريفا في مادة مستقلة بل اتى على تعريف بعض المصطلحات الفنية التي تبني عليها الجريمة في المادة 01 منه ،وقام بحصر وتوصيف الجرائم في المواد 13،14،15 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 بتاريخ 14 اغسطس 2018¹

اما في القانون الأردني " لم يعرف المشرع الأردني في قانون الجرائم الالكترونية رقم 27 لسنة 2015 الجريمة الالكترونية وانما جرم بعض الأفعال التي تقع على الأنظمة المعلوماتية والمواقع والشبكات الالكترونية ، وكذلك استخدم الوسائل الالكترونية في ارتكاب بعض الجرائم في المواد 3- 12"² حتى في قانون الجرائم الالكترونية الجديد لعام 2023 قانون الجرائم الإلكترونية رقم 17 لسنة 2023 لم يضع المشرع تعريفا للجريمة الالكترونية بل اكتفى بتحديد الوسائل والتعاريف التقنية في المادة الثانية منه مثل الشبكة المعلوماتية ، نظام المعلومات وسيلة تقنية المعلومات³

وبهذا انتهج المشرع الأردني الطريق نفسه بعدم اتيانه بجديد فيما يخص تعريف الجرائم المعلوماتية. وعلى نفس النهج سار المشرع الليبي اذ انه لم يضع تعريفا شاملا جامعاً مانعاً للجريمة السيبرانية حيث نص في مادته الأولى على: (.... اي فعل يرتكب باستخدام أنظمة الجريمة الالكترونية الكمبيوتر او شبكة المعلومات الدولية او اي وسيلة أخرى من وسائل تكنولوجيا المعلومات بما يخالف احكام هذا القانون....)⁴.

"وعرف المشرع القطري الجريمة الالكترونية في المادة الأولى من قانون مكافحة الجرائم الالكترونية رقم 14 لسنة 2014 بانها اي فعل ينطوي على استخدام وسيلة تقنية المعلومات، او شبكة المعلوماتية

¹الجريدة الرسمية المصرية العدد 32 مكرر ج 14 اغسطس 2018 متاح على موقع منشورات قانونيه ارشيف رقمي الموقع الالكتروني <https://manshrat.or/nod/3148> تاريخ الاطلاع : بتاريخ 2026 /2/14 على الساعة 13:20

²عبد الإله النوايسة ، المرجع السابق ، ص 41

³متاح على الموقع الالكتروني <https://w.w.w.lob.gov.jo> تاريخ الاطلاع : 2026/02/14 الساعة 13:00

⁴ المجمع القانوني الليبي، قانون الجرائم الالكترونية الليبي رقم 5 لسنة 2022 بشأن مكافحة جريمة الالكترونية الصادر عن مجلس النواب الليبي الربط الالكتروني <https://lawsociety.ly/législation> تاريخ الاطلاع: 2026/04/26 12:10

بطريقة غير مشروعة بما يخالف احكام القانون، وبهذا التعريف اخذ المشرع القطري بالمعيار الموسع للجريمة الالكترونية بحيث تشمل كل جريمة ارتكبت بوسيلة الكترونية¹

ويبدو ان المشرع الإماراتي الذي اتى بمرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الالكترونية² ، كان اكثر جراءة وحاول تعريف مصطلحات وذلك في المادة الاولى منه ، مثل مصطلح تقنية المعلومات وعرف كلمة السيبراني بقوله "كل ما يتعلق بالشبكات المعلوماتية الحاسوبية ، وشبكة الانترنت ، والبرامج المعلوماتية المختلفة وكل الخدمات التي تقوم بتنفيذها كذلك عرف مصطلح الهجمات الالكترونية في نفس المادة"³.

"وبالرجوع الى التشريع الجزائري نجده لم يستقر على استخدام مصطلح واحد للدلالة على هذه الجرائم حيث سماها بموجب القانون 04-15 المتضمن قانون العقوبات بجرائم المساس بأنظمة المعالجة الالية للمعطيات ثم بموجب القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها استخدم مصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال للدلالة على هذه الجرائم"⁴ ، فقد عرفها بموجب احكام الماده 2 الفقرة أ من قانون رقم 04-09 على انها "جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات اوي جريمة اخرى ترتكب او يسهل ارتكابها عن طريق المنظومة المعلوماتية او نظام للاتصالات الإلكترونية⁵ وفي الفقرات (ب ، ج ، د، و) عرف مصطلحات ذات علاقة بالوسائل والادوات مثل منظومة معلوماتية، معطيات معلوماتية ، مقدمو الخدمات ومن خلال هذا التعريف نستنتج ان المشرع الجزائري اعطى تعريفا موسعا للجريمة السيبرانية ربما هذا من اجل استيعاب كل صور الجرائم التي من الممكن ان تظهر مستقبلا كونها جريمة متطورة بالنظر الى ما

¹ عبد الإله النوايسة ، المرجع السابق ، ص 40

² الجريدة الرسمية عدد 712 بتاريخ 26 سبتمبر 2021 <https://share.google/KEQXhhTSacIvWRaqb2021> تاريخ النشر اخر تحديث 04 افريل 2024 تاريخ الاطلاع : 2026/04/26

³ انظر المادة 1 من القانون رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الالكترونية بتاريخ : 20 سبتمبر 2021 الجريدة الرسمية عدد 712

⁴ مهدي رضا ، المقال ، السابق ص 113

⁵ انظر الجريدة الرسمية الجزائرية قانون رقم 09-04 الصادر في 05 اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47 الموقع الالكتروني SGG Algerie [https:// sharegoogle/XKare8uSeJRyI7aSaN5](https://sharegoogle/XKare8uSeJRyI7aSaN5) تاريخ الاطلاع : 2026/04/26

شهدته من تسارع في التطور وبروز في كل مرة صورة جديدة أدت الى انه من الصعوبة على التشريعات استيعابها في كل مرة.

اما المشرع التونسي فقد تناول هذه الجريمة في المرسوم عدد 54 لسنة 2022 يتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال فلم يعرفها بل جرم بعض الافعال التي اعتبرها جرائم سيبرانية وحدد العقوبات فقط .

ثانيا : تعريف الجريمة السيبرانية في التشريعات الاجنبية :

فبعيدا عن التشريعات العربية ، كانت التشريعات الاجنبية لها الاسبقية في تجريم هذه الجرائم ومنها التشريع الفرنسي في مجال الجريمة السيبرانية " عالج المشرع الفرنسي الجريمة الالكترونية منذ صدور القانون المتعلق بتكنولوجيا المعلومات والحريات رقم 78/17 الصادر في 6 جانفي 1978 ، بعد ذلك جاء قانون godfrin المتعلق بالاحتيال عبر الكمبيوتر رقم 19/88 الى غاية اخر تعديل من قانون العقوبات الفرنسي 29 جويلية 2023 ، نجده لم يتطرق الى مفهوم الجريمة الالكترونية وانما استعمل مصطلح " المساس بأنظمة المعالجة الالية للمعطيات " في المواد من 1- 313 الى 7- 323 من قانون العقوبات ¹ .

وعرفه المشرع الامريكي " واذا نظرنا الى التشريع الامريكي نجد ان إدارة العدل الامريكية قد توسعت في ربط جهاز الحاسب الالي بتقنيته فذهبت الى تعريف جرائم جهاز الحاسب الالي بأنها هي : كل عدوان بالارتكاب على اي قانون يتضمن في محتواه تقنية جهاز الحاسب الالي ويكون عرضة للتحقيق والاثام كان ذلك بالطبع بتأثير من اتجاهات المشرع الامريكي في تعديل 1996 لقانون البنية الوطنية للمعلومات الذي استوحى التجريم من الربط بين جهاز الحاسب الالي وتقنيته ككل" ²

¹ رزاق بارة كريمة ، مقال الجريمة الالكترونية المتعلقة بالأشخاص وفقا للتشريع الفرنسي والتشريع الجزائري ، المركز الجامعي عبد الحفيظ بوالصوف ميلة الجزائر ، المجلة الجزائرية للحقوق والعلوم السياسية - المجلد 08، العدد 02 سنة 2024 ص4

² نايف شافي المظافره الهاجري ، مقال، جرائم تقنية المعلومات في التشريع الامريكي مقارنة بالتشريعات العربية ، العدد 38 مارس 2023 ص 339

المطلب الثاني: خصائص الجريمة السيبرانية .

مما لا شك فيه ان الجريمة السيبرانية جريمة مستحدثة تختلف عن الجرائم التقليدية بشكل او باخر تتميز بالسرعة في التطور نتيجة للثورة التكنولوجية الهائلة، التي أحدثت بدورها ثورة معلوماتية مست كل ميادين الحياة الاجتماعية والثقافية والعلمية خاصة مع استعمال الرقمنة على مستوى كل مؤسسات الحكومية و الخاصة فهي جرائم لها من الخصوصية ما يجعلها تختلف عن الجرائم التقليدية اختلافا جذريا ومن جملتها هذه الخصائص ما يلي:

الفرع الاول: جرائم عابرة للحدود الجغرافية وخطيرة:

لأنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الأنترنت وسهولة حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكابها عن طريق حاسب ألي موجود في دولة محددة بتوقيت معين ويتحقق الفعل الإجرامي في دولة او دول أخرى بتوقيت مختلف¹.

ولعل هذا ما يجعلها من الجرائم الخطيرة التي تمس أمن الدول وسيادتها فيمكن لشخص موجود في روسيا أن يرتكب جريمة قرصنة مواقع او حسابات بنكية في بريطانيا، مثلا عن ذلك هجمات اغراق خوادم الساحة الزرقاء الالكترونية من طرف قرصنة روس بإرسال رسائل الكترونية إلى قسم خدمة الرسائل طلب منهم فدية 20,000 دولار أمريكي مقابل إيقاف الهجمات والتهديد بتكبيد الشركة خسائر مالية فادحة في حالة الرفض²

فبسبب الاستعمال العالمي للأنترنت جعل منها جريمة عالمية عابرة للحدود الجغرافية اذ ان "المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع مفتوح عبر شبكات تخترق الزمان والمكان دون ان تخضع لحرس الحدود"³، فهي تتسم بالخطورة البالغة نظرا للخسائر المادية التي تسببها على المستوى الوطني والدولي والتي يصعب تقديرها بسبب الاحجام عن التبليغ من طرف المؤسسات وهي تمس الاشخاص الطبيعيين والمعنويين ومن أخطرها نشر الفيروسات المدمرة ، اضافة الى المساس

¹ علوي علي، احمد الشارفي ، المرجع السابق ،ص 39

² الجزيرة الوثائقية، برنامج وثائقي علوم الإجرام الجرائم الالكترونية منشور على موقع يوتيوب تاريخ النشر 31 اغسطس

2024 تاريخ الاطلاع: 1 ابريل 2026 الساعة 15:45

³ نهلاء عبد القادر المومني ، المرجع السابق ،ص 50

بالحياة الخاصة للإنسان والأمن القومي ومما زاد من خطورتها انها سهلة لا تتطلب مجهود ولا فترة زمنية طويلة مما اغرى الجناة لارتكابها وبخاصة الوقعة على الاموال¹

ان خطورة هذه الجريمة مست كل النواحي الاقتصادية والاجتماعية والسياسية مما ارق الدول في محاربتها بالإضافة الى ذلك فإن المجرم المعلوماتي يتميز بخصائص تميزه عن المجرم الذي يرتكب الجريمة التقليدية الذي لا يتطلب ان يكون ذات مستوى علمي ومعرفي عالي لكي يرتكبها ، فان الامر مختلف بالنسبة للمجرم المعلوماتي كونها جرائم تقنية فتتطلب ان يكون المجرم من ذوي الاختصاص في مجال المعلوماتية او على الاقل لديه حد ادنى من المعرفة والقدرة على استخدام الحاسوب بالأخص في جرائم التحويل الالكتروني للأموال، كذلك بواعث ارتكاب الجريمة تختلف لدى المجرم المعلوماتي عن المجرم التقليدي²

الفرع الثاني : جريمة ترتكب في بيئة تقنية رقمية:

اي انها ترتكب في البيئة المعلوماتية الرقمية وتعرف البيئة الرقمية بأنها: " هي ذلك الفضاء الافتراضي المعتمد على المواقع الالكترونية وشبكات التواصل الاجتماعي والبرمجيات التي تستخدم في إدارة نشاطات مستخدمي وسائل الاتصال والانترنت والاجهزة الالكترونية سواء كان شخص او مؤسسة بمختلف انواعها وفي جميع المجالات من اجل تنظيمها وتلبية رغباتهم وتوجيهها من خلال ملفات الارتباط وسجلات النشاط"³ ويرى "تيلي" ان المكونات الأساسية التي يجب توفر في البيئة الرقمية هي:- المعلومة على الشكل الرقمي- تكنولوجيا الحديثة لنقل المعلومات والاتصال-الوسائل التقنية المستعملة من قبل المستخدم للوصول الى المعلومة"⁴

¹ عبد الإله النوايسة , المرجع السابق ، ص 80

² نهلاء عبد القادر المومني ، المرجع السابق، ص 59

³ دراجي بوطي و عبد الرحيم بن بوزيان، مقال التكيف المدرسي في ظل البيئة الرقمية مجله الاعلام والمجتمع المجلد

08 العدد 1 جوان، 2024 ص 48

⁴ دراجي بوطي ومن معه، المقال نفسه ، ص 49

الفرع الثالث: صعوبة الإثبات والتتبع :

تعتبر هذه الخاصية هي نتيجة منطقية للخاصيتين السابقتين كونها تقنية رقمية، مما يجعل من الصعوبة إثباتها وتتبع مرتكبيها وتزيد الصعوبة في الجرائم التي ترتكب في دول أخرى ، فلا يترك مرتكبها أثرا ماديا يدل عليه كما هو الحال في الجرائم التقليدية ، إضافة الى خطوات تنفيذ الجريمة معروفة مسبقا فلجاني فيها لا يخشى المفاجآت اثناء التنفيذ كما هو الحال في الجرائم التقليدية التي من السهولة ترك الجاني اثرا يمكن اكتشافه كاداه اثبات ضده ، بينما الجاني في الجريمة السيبرانية يكاد يكون الدليل رقمي وسيلة الإثبات الوحيدة التي يمكن من خلالها تعقب اثر الجاني وهذه الوسيلة من السهولة طمسها وإخفاء معالمها نهائيا¹.

ونرى بأن هذه الخاصة ساهم فيها نقص التكوين في مجال الإثبات في الجريمة السيبرانية فيما يخص الدليل الرقمي والتفتيش الرقمي .

الفرع الرابع : جريمة ناعمة وجذابة :

كما توصف بأنها من الجرائم الناعمة والجذابة" فتتميز بأنها ناعمة من حيث تنفيذها ، فلا يستوجب على مرتكبها استعمال العنف بل تعتمد على المجهود الذهني لا البدني ونتيجة لذلك يستطيع ارتكاب هذه الجرائم الشخص المقعد والضرير وايضا النساء بمختلف اعمارهن واي شخص اذا توافرت لديه الخبرة والدراية اللازمين للتعامل مع قواعد البيانات والاجهزة الالكترونية"²

وعلى العموم فان الجريمة السيبرانية تتميز بخصائص أخرى تجعلها تختلف عن جرائم التقليدية تنتم بالطابع الخفي بحيث يصعب اكتشافها في غالب الأحيان فالكثير من الجرائم لن تكتشف وأخرى لم يتم اكتشافها إلا بعد أمد طويل من حدوثها كما تمتاز بسرعة ارتكابها وانتشار تأثيراتها في وقت وجيز إضافة الى صعوبة تحديد حجم الأضرار المترتبة عنها خاصة عندما يتعلق الأمر بالاعتداء على البيانات او الانظمة المعلوماتية وهذا ما يجعلها من الجرائم الخطيرة نظرا لما لها من انعكاسات على مختلف

¹ عبد الإله النوايسة ، المرجع السابق ص 80

² علوي علي، احمد الشارفي ، المرجع السابق ،ص41

المجالات الامنية والاقتصادية والاجتماعية فضلا عن تعدد دوافع ارتكابها وتعدد صورها واساليبها. ويضاف الى ذلك بانها تتطور بوتيرة سريعة تفوق سرعة مواكبة التشريعات الجنائية لها.

المطلب الثالث: اركان جريمة السيبرانية

من المستقر فقها وقضاء ان كل الجريم التقليدية تقوم على اركان أساسية هي الركن الشرعي والركن المادي والركن المعنوي والتي لا تتحقق المسؤولية الجزائية الا بتوافرها مجتمعه وفي الجريمة السيبرانية لا يختلف الامر اذ تخضع بدورها لهاته الأركان العامة مع مراعاة خصوصيتها المرتبطة بالبيئة الرقمية التي ترتكب فيها وتتمثل في

الفرع اولا: الركن الشرعي:

ويقصد به وجود نص يجرم الفعل ويوضح الجزاء المترتب على مخالفته وهو اساس التجريم او ما يسمى بمبدأ شرعية الجريمة و العقوبة" فلا جريمة ولا عقوبة الا بناء على نص" وقد اصدت غالبية الدول قوانين عرفت جرائم تقنيه المعلومات وحددت العقوبات المقررة¹

ان الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني يقوم على عنصرين اساسيين: مطابقه الفعل لنص التجريم وان لا يقع الفعل المرتكب لسبب من أسباب الإباحة

وينطبق هذا التصور كذلك على الجريمة السيبرانية ، اذ تخضع بدورها لمبدأ الشرعية الجنائية فلا تقوم الا بوجود نص خاص يجرب السلوك المرتكب عبر الوسائط الالكترونية مع انتفاء اسباب الإباحة، يرى الاستاذ المناعسة وجلال الزغبى من خلال شرحه مفهوم "مبدأ الشرعية" لا يمكن معاقبة الشخص بدون وجود نص قانوني ساري المفعول يحدد مضمونها من خلال تبيان النمط السلوكي المحظور الذي تم الإقدام عليه او القيام به وبيان العقوبة.² ويرى في مبدأ الشرعية في مواجهة الجريمة المستحدثة انه لا مبرر لغياب الجهد الفاعل في رصد السلوكيات المستحدثة والعمل على اظهار عناصر كل سلوك تمهيدا لإقرار قاعدة العقاب اللازمة التي تتسجم مع الطبيعة الخاصة لهذا السلوك او ذاك.³

¹ علوي علي، احمد الشارفي المرجع السابق ، ص 48

² اسامة احمد المناعسة، جلال محمد الزغبى ، المرجع السابق، ص 45

³ اسامة احمد المناعسة ، جلال محمد الزغبى المرجع نفسه ، ص 47

اما بالنسبة للعنصر الثاني: ان لا يخضع الفعل لسبب من أسباب الاباحة يقصد بها تلك الأفعال التي تكون في ظاهرها أفعال مجرمة تستوجب العقاب لكن اتيانها لعل المصلحة العامة تصبح افعالا مباحة وهي جزء من مبدأ الشرعية وتعد اسباب الاباحة أسباب موضوعية تنصب على الفعل ذاته فتتفي عنه صفة الجرم وهي تختلف عن موانع المسؤولية والعقاب التي تنصب على شخص الفاعل ، ويمتد اثر الاباحة ليشمل كل من شارك في الفعل سواء كان فاعلا أصليا او شريكا وتشمل أسباب الاباحة بالمفهوم الواسع للقانون سواء كان تشريعا او مراسيم صادرة عن السلطة التنفيذية طالما ان الغرض منها هو الاباحة وليس التجريم ، وتشمل أسباب الاباحة

1- ما امر به القانون: يقصد به الحالات التي يتوجب فيها القانون على الشخص القيام بفعل معين بحيث يصبح هذا الفعل مباحا بل ويعتبر الامتناع عنه جريمة يعاقب عليها القانون ، مثل الزام مقدمي خدمات الانترنت بتقديم بحفظ المعطيات التي تسمح بالتعرف على المستخدمين وتفاصيل اتصالاتهم وتقديمها للسلطات القضائية عند الطلب المساعدة للسلطات القضائية مما، يتيح لهم تقييد خصوصية المراسلات التي يحميها القانون اصلا.

2- ما اذن به القانون: وهي رخصة تجيز للشخص القيام بالفعل او تركه مثل معالجة المعطيات الشخصية والتفتيش الالكتروني حق التأديب الذي يقوم به الأولياء في اطار تأديب أبنائهم أثناء استعمال الاجهزة الالكترونية وذلك بمراقبة معطياتهم الشخصية التي يتداولونها في البيئة الالكترونية والانترنت¹

3-الدفاع الشرعي: ويشمل رد الاعتداء الذي يهدد النفس او المال وقد توسع ليشمل الدفاع الشرعي الالكتروني الوقائي أو الإستباقي لحماية امن الدولة لمنظومتها المعلوماتية من الحروب السيبرانية²

الفرع الثاني : الركن المادي:

" لتتكون الجريمة لا بد من ارتكاب فعل مادي محسوس (أو امتناع عن اتيان فعل) يعاقب عليه القانون فالجريمة ليست مجرد وجود نية جرمية ، اذ لا بد لهذه النية من ان تتجسد في كيان مادي محسوس ، هذا

¹ نور الدين موفق، مقال اسباب الاباحة الالكترونية ، جامعة محمد لمين دباغين سطيف 2 مجله المحامي ، العدد 2025/01 ص 166، 169، 170

² نور الدين موفق، مقال نفسه ص 176

السلوك المادي المحسوس الذي ينص عليه القانون هو ما يعرف بالركن المادي للجريمة ، والذي يشكل شرطا اساسيا للبدء في عملية البحث عن توافر الجريمة من عدمه¹ ، ولإتمام الركن المادي لابد من توافر ثلاثة عناصر وهي السلوك الاجرامي النتيجة الإجرامية والعلاقة السببية بينهما

فالسلك الإجرامي : فالبحث عن الجريمة يكون بإظهار النوايا الى الواقع المادي بإتيان سلوك يعد خرقا لأمر المشرع ، سلوك تتعدد صوره بتحريك الجاني لعضو من اعضاء جسده بشكل ارادي بغية احداث نتيجة معينة مثل القتل بطعنة سكين او سرقة بيت ، اما في الجريمة المستحدثة لا يخفى الاختلاف الكبير في محتوى ومضمون وطبيعة هذا السلوك الجرمي الذي تطور بتطور وسائل متاحة جديدة وجدت بين ايدي الفاعل الذكي اين خرج السلوك من سلوك تقليدي الى مساحات معقدة كثيرا نتج عنها صعوبات جمة من ناحية تحديد ماهية وعناصر واركان هذا السلوك ، اومن ناحية متابعة وجمع ادلة اثباته او نسبه الى فاعل معين وهي امور ادت الى ظهور نمط مستحدث من الاجرام ادى الى انقلاب في النظرية العامة للجريمة .²

ومن امثلة السلوك الإجرامي الخارجي يتمثل في الاستخدام غير مشروع للأنظمة الالكترونية ويشمل ذلك افعالا ملموسة مثل اختراق الانظمة او تدمير المعلومات او سرقة بيانات بطاقات الائتمان او التلاعب بالبيانات وتزويرها.

اما العنصر الثاني الذي يرتبط به الركن المادي هي النتيجة الجرمية:التي تحدث اثرا ضارا يمس بمصلحة يحميها القانون في الواقع مثال ذلك التلاعب بالبيانات البنكية الالكترونية ، بما يؤدي الى تحويل اموال الغير دون وجه حق والنتيجة هنا هي الحاق ضرر مالي بالمجني عليه صاحب الحساب البنكي ومن الامثلة ايضا التلاعب ببيانات الضرائب بقصد تحقيق منفعة غير مشروعته واذا كانت النتيجة الاجرامية هي الأثر الواقعي الملموس الذي يثبت اكتمال ركن المادي للجريمة فان هذا الاكتمال لا يكون الا متى ثبت ان هناك علاقة سببية بين السلوك الاجرامي والضرر الناتج عنه.³

¹ اسامة احمد المناعسة، جلال محمد الزغبى ، المرجع السابق ،ص 53

² اسامة احمد المناعسة، جلال محمد الزغبى ، المرجع نفسه ،ص 53 و 54

³ اسامة احمد المناعسة، جلال محمد الزغبى ، المرجع نفسه ص 55

فالعلاقة السببية: هي الرابطة المادية بين السلوك المادي والنتيجة الاجرامية فمثلا يجب لتحقيق جريمة انتهاك الحق في الخصوصية عبر الانترنت ان يكون هناك دخول على الانترنت باستخدام حاسوب عامل والقيام باختراق الخوادم المختلفة في مسارها ثم بعد ذلك التعدي على الخصوصية في موقع ما".¹

ففي جريمة التهديد عبر مواقع التواصل الاجتماعي التي تعد من الجرائم السيبرانية عندما تتم برسائل تكنولوجيا الاعلام والاتصال وفقا لقانون عقوبات الجزائي واحكام القانون رقم 09- 04 المؤرخ في 05 اوت 2009 فان إرسال رسالة تهديد عبر مواقع التواصل مثل الفيسبوك او نشر منشور يتضمن تهديد موجه لشخص ما او صورة او تسجيل صوتي او عبر التطبيقات مثل وتساب او البريد الالكتروني لشخص ما بقصد ادخال الرعب والخوف في نفس المجني عليه او المساس بحريته وأمنه فهذه الجريمة مكتملة الأركان جرمة قانون العقوبات الجزائري.

الفرع الثالث :الركن المعنوي

يعرف بأنه العلم بعناصر الجريمة واردة ارتكابها وبالتالي يتكون من عنصرين هم العلم والارادة.²
-العلم : يعد العلم العنصر الأول من عناصر القصد الجنائي في الركن المعنوي للجريمة ويقصد به أن يكون الجاني على دراية بجميع عناصر الجريمة اي ماديات الجريمة الواردة في النص القانوني ويشمل العلم ماييلي:³

- 1- علم مفترض: وهو العلم بالقاعدة القانونية حيث لا يعتد بالجهل بالقانون.
- 2-العلم بالوقائع: ويشمل العلم بموضوع الجريمة مثل علم الجاني ان فعله يقع على نظام معلوماتي وبيانات مملوكة لغيره وليست ملكا له او مالا مباحا.
- 3-العلم بماهية الفعل وخطورته: يجب ان يدرك الجاني ان النشاط الذي يقوم به مثل الاختراق او تعطيل هو فعل غير مشروع من شأنه الحاق الضرر بالشبكة المعلوماتية او المعتدى عليه ، وعلى الرغم من ذلك فانه في بعض الحالات ان الفاعل لا يقصد الحاق ضرر مباشر الا ان الجريمة تعتبر مقصودة ما دام ان عنصر العلم متوفر حيث يدرك الفاعل ان الفعل غير مشروع ويستهدف نظام الغير وعنصر الارادة كذلك متوفر، ولا يكفي العلم وحده بل يجب تكامل العلم مع الارادة لقيام القصد في الجريمة التقنية.

¹ محمود القرعان ،المرجع سابق، ص 35

² محمود القرعان ،المرجع نفسه، ص 35

³ اسامة احمد المناعسة، جلال محمد الزغبى ، المرجع السابق ،ص61

فالإرادة: وهي العنصر الثاني للقصد الجرمي وهي القوة النفسية التي توجه أعضاء الجسم أو النشاط الذهني أو التقني نحو تحقيق النتيجة الجرمية فيجب ان تتجه إرادة الفاعل الى اتيان الفعل مثل إدخال أوامر برمجية معينة او تحقيق النتيجة مثل اختراق النظام او الاستيلاء على البيانات.¹

فمثلا "يتخذ الركن المعنوي في جريمة التهديد برسائل الاتصالات صورة القصد الجرمي العام يلزم ان يكون الفاعل مريدا لفعل التهديد غير مكره على ذلك وعالما بعناصر الجريمة وان من شأن فعله ترويع المجني عليه يتوافر القصد الجرمي أيا كانت غاية الجاني منه وما يرمي له من أهداف فالغرض الذي يتوخاه الجاني من فعل التهديد ليس عنصرا من عناصر الجريمة ولا يشترط لقيام قصد التهديد عزم الجان تنفيذ الأمر الذي هدد به ذلك ان نية التنفيذ أمر خارج عن تكوين الجريمة."²

" فالقصد الجنائي متوفر في جميع الجرائم الالكترونية دون استثناء ولكن هذا لا يمنع أن هناك بعض الجرائم الالكترونية تتطلب أن تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الانترنت..... والمشرع في جميع الحالات هو المختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص".³

ففي جريمة التهديد برسائل الاتصال يتخذ الركن المعنوي صورة القصد الجرمي العام فيلزم أن يكون الفاعل مريدا لفعل التهديد غير مكره على ذلك وعالما بعناصر الجريمة وانا من شان فعله ترويع المجني عليه ، ويتوافر القصد الجرمي أيا كانت غاية الجان منه وما يرمي له من اهداف فالغرض الذي يتوخاه الجاني من فعل تهديد ليس عنصرا من عناصر الجريمة ولا يشترط لقيام قصد التهديد عزم الجاني تنفيذ الأمر الذي هدد به ذلك ان نية التنفيذ أمر خارج عن تكوين الجريمة.⁴

فالقصد الجنائي متوفر في جميع الجرائم الالكترونية دون استثناء ولكن هذا لا يمنع أن هناك بعض الجرائم الالكترونية التي تتطلب أن تتوفر فيها القصد الجنائي الخاص مثل الجرائم تشويه السمعة عبر الانترنت.⁵

¹ اسامة احمد المناعسة وجلال محمد الزغبى المرجع السابق ،ص 62

² عبد الاله النويصة ، المرجع السابق ، ص115

³ محمود احمد القرعان ، المرجع السابق، ص 36

⁴ عبد الاله النويصة ، المرجع السابق ، ص 115

⁵ محمود احمد القرعان ، مرجع نفسه ، ص 36

المبحث الثاني: صور الجرائم السيبرانية و أثارها

شهد العالم في الآونة الاخيرة تطورا متسارعا في مجال تكنولوجيا المعلومات والاتصال ترتب عنه بالمقابل تطورا في الجرائم السيبرانية ويتجلى ذلك في ظهور صور جديدة لهذه الجريمة تنوعت أساليب ارتكابها مما أدى الى اجتهاد فقهاء القانون في تصنيفها وفق معايير مختلفة ونظرا لتعدد صورها ، فقد تعددت اثارها والاقتصادية والاجتماعية والسياسية والقانونية .

المطلب الاول: انواع الجرائم السيبرانية

نتناول في هذا المطلب انواع الجرائم السيبرانية التي تعددت صورها بتنوع الوسائل التقنية المستخدمة في ارتكابها والأهداف التي يسعى المجرم المعلوماتي الى تحقيقها فالفقه القانوني لم يقتصر على معيار واحد في تصنيف الجرائم السيبرانية وانما ثمة عدة معايير فمنهم من اعتمد معيار الهدف ومنهم من اعتمد معيار الوسيلة ومنهم من اعتمد معيار محل الاعتداء ومعيار صفة الجاني ومعيار النطاق الجغرافي ولعل اهم معيار والأكثر استخدام هو معيار محل الاعتداء والسلوك الاجرامي.

وفي دراستينا هذه تطرقنا الى الجرائم السيبرانية في فرعين جرائم تناولتها اتفاقية "بودابست" كفرع اول وفي الفرع الثاني تطرقنا الى الجرائم المستحدثة التي لم تتناولها اتفاقية بودابست او غير المنصوص عليها صراحة بها.

الفرع الاول : الجرائم السيبرانية المنصوص عليها في اتفاقية بودابست

تعددت التصنيفات التي اعتمدها فقهاء القانون في تصنيف الجرائم السيبرانية ، ولقد اوجدت اتفاقية بودابست تقسيما حديثا نسبيا للجريمة السيبرانية حيث قسمتها الى اربعة محاور رئيسية منها جرائم تمس سرية البيانات والانظمة المعلوماتية وسلامتها ، وجرائم مرتبطة بالكمبيوتر، وجرائم مرتبطة بالمحتوى ، والجرائم المرتبطة بانتهاك الملكية الفكرية.

اولا :الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر:وتشمل جريمة الدخول غير القانوني او غير المشروع نصت عليه المادة 2 من الاتفاقية والاعتراض غير القانوني الذي نصت عليه

المادة 3 من الاتفاقية والتدخل في المعطيات المادة 4 بينما نصت المادة 5 على التدخل في نظم الحاسوب وإساءة استخدام الأجهزة نصت عليه المادة 6.¹

1-جريمة الدخول غير القانوني: وذلك بالدخول المتعمد الى نظام كمبيوتر او جزء منه دون حق او اذان سواء كان بنية انتهاك وسائل الأمن او بنية الحصول على معطيات الكمبيوتر او لأي نية غير مشروعة المادة 2.²

2-جريمة الاعتراض غير المشروع: او الاعتراض غير القانوني المتعمد ودون حق بواسطة وسائل تكنولوجية للبيانات المرسله غير العامة الى أو من نظام كمبيوتر وكذلك اعتراض الاشعاعات الكهرومغناطيسية المنبعثة من نظام الكمبيوتر تحمل مثل هذه المعطيات المادة 3³

3-جريمة التدخل المتعمد في البيانات: بإتلاف بيانات حاسوبية حذفها افسادها تعديلها او تدميرها

4-جريمة التدخل عمدا في النظام: وبغير حق وكذلك بالإعاقة الخطيرة اشتغال نظام الكمبيوتر عن طريق ادخال بيانات حاسوبية ارسالها اتلافها حذفها افسادها تغييرها او تدميرها المادة 4⁵

5-إساءه استخدام الأجهزة: وقد كانت عنوان هذه الجريمة في مستهل الاتفاقية السابقة الادوات غير القانونية في حين ان العنوان الجديد اكثر دقة من الناحية الوصفية و الموضوعية وتشمل هذه الجريمة طائفتين من الافعال الاولى المنصوص عليها في الفقرة الاولى من المادة السادسة وتشمل الانتاج المتعمد او البيع او شراء او الاستخدام او استيراد او توزيع او غير ذلك من الاجهزة والادوات بما فيها برامج الكمبيوتر بهدف ارتكاب الافعال المنصوص عليها في المواد 2 و 5 المشار اليها اعلاه.⁵

كذلك كلمات، السر ورموز الدخول او ايه معطيات مشابهة بحيث تتيح اختراق نظام الكمبيوتر او الدخول اليه او الى جزء منه بنية ارتكاب اي فعل من الافعال المنصوص عليها في المواد 2 و 5 كما

¹ عبد الكريم عبد الله المرجع السابق ، صفحة 131

² عبد الله عبد الكريم ، المرجع نفسه ، صفحة 132

³ عبد الله عبد الكريم ، المرجع نفسه ، صفحة 132

⁴ عبد الله عبد الكريم ، المرجع نفسه ، صفحة 132

⁵ عبد الكريم عبد الله المرجع نفسه ، صفحة 132

تشمل هذه الجريمة وفقا للفقرة الثانية من المادة الثالثة حيازة وتملك اي عنصر او اداء مما ورد ذكره في الفقرة الاولى اعلاه بنيه ارتكاب اي من الافعال المشار اليها في المواد الثانية والخامسة من الاتفاقية.¹

ثانيا: الجرائم المعلوماتية:

1-التزوير المرتبط بالكمبيوتر: اذا ما ارتكب عمدا وبغير حق ادخال تغيير او اتلاف بياناتك كمبيوتر بشكل يجعل بيانات غير اصلية تبدو بقصد اعتبارها او استخدامها لأغراض قانونية بغض النظر اذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر ام لا المادة 7 الجزء 2

2-الاحتيال المرتبط بالكمبيوتر اذا ما ارتكب عمدا او تسبب في الحاق خساره بملكية شخص اخر عن طريق ادخال او حذف او تعديل او كتم بيانات الكمبيوتر , ومن خلال تدخل بعمليات نظام الكمبيوتر او برامجه بنيه الحصول على منفعة اقتصادية لنفسه او لغيره.²

ثالثا : جرائم متصلة بالمحتوى: الجرائم المرتبطة بدعارة الاطفال وبالرغم من ان هذه الجريمة مصنفة تحت عنوان جرائم المحتوى ليست هي الصورة الجرمية الوحيدة للأفعال الجرمية المتصلة بمحتوى مواقع المعلوماتية.³

منها السلوكيات التالية انتاج عرض توزيع مواد اباحية عن الاطفال بغرض توزيعها واتاحتها او نقلها عبر نظام كمبيوتر الحصول على هذه المواد الاباحية عن الاطفال عبر نظام كمبيوتر لصالح شخص ذاته او لفائدة الغير حيازة مواد اباحية عن الاطفال داخل نظام كمبيوتر او على دعامة التخزين بيانات الكمبيوتر المادة 9 من الاتفاقية.⁴

رابعا: الجرائم المتصلة بالاعتداء على الملكية الفكرية: الجرائم المتعلقة بانتهاك حقوق النشر والتأليف والحقوق ذات الصلة نصت عليها المادة 10 من الاتفاقية , في فقرتين الاولى خاصة بحق المؤلف والثانية بالحقوق المجاورة اذا ما ارتكبت عمد وبغرض تجاري باستخدام نظام معلوماتي.⁵

¹ عبد الكريم عبد الله المرجع السابق ، صفحة 133

² عبد الكريم عبد الله، المرجع السابق ، صفحة 133

³ عبد الله عبد الكريم ، المرجع نفسه ، صفحة 134

⁴ عبد الكريم عبد الله المرجع نفسه ، صفحة 134

⁵ عبد الله عبد الكريم ، المرجع نفسه ، ص 135

الفرع الثاني: الجرائم المستحدثة التي لم تتناولها اتفاقيه بودابست

اولا: الجرائم الواقعة على الاشخاص والمتصلة بالمحتوى

1- **القذف والتشهير**: ويكون بتوجيه الفاظ الى شخص تمس شرفه او كرامته او اتهم شخص بواقعة توجب العقاب قانونا وتعرضه لبغض الناس واحتقارهم له ويكون عبر خطوط الاتصال المباشر او يكون كتابيا عبر الوسائل الالكترونية ، بريد الكتروني، صفحات ويب، غرف المحادثات.¹، فالقذف يتضمن تصرفا صادرا عن شخص ما بمواجهه شخص محدد يتضمن الاعتداء عليه والمساس بسمعته بصورة تلحق الضرر به.

2- **مواقع الاباحية والدعارة**: وذلك عن طريق المواقع الاباحية التي تحرض على ممارسة الجنس وذلك بنشر صور وافلام ورسائل جنسية وممارسات مخلة بالحياء من اجل التداول في اوساط الشباب والقصر عبر الاف المواقع الاباحية باستعمال الشبكة المعلوماتية لتسهيل الدعارة²

3- **العاب القمار والالعب غير مشروع عبر الانترنت**: ادارة مشروع مقامرة على الانترنت وتسهيل ادارة مشاريع القمار على الانترنت وتشجيع المقامرة عبر الانترنت³
اصبح لاعب القمار اسهل عبر تجمع اللاعبين على صفحة واحدة من صفحات الانترنت على مستوى العالم ومن اماكن متفرقة⁴

4- **التحريض على العنصرية والتعرض للأديان**: فالكثير من المواقع والصفحات على شبكة الانترنت يستعملها اشخاص من اجل التحريض العلني والمباشر على التمييز والتفوق العنصري او الكراهية او الدعوة للعنف ضد افراد وجماعات بناءا على العرق او الاصل، فالقانون الجزائري يعاقب على ذلك بموجب الامر 05-20 مؤرخ في 28 ابريل 2020 بالحبس والغرامة وتشدّد العقوبة اذا ما تم التحريض عبر وسائل التواصل الاجتماعي في المادة 30 ويقصد بالتعرض للأديان او ازدياء الاديان في القانون

1 علوي علي احمد الشارفي المرجع السابق ص 62

2 علوي علي احمد الشارفي المرجع نفسه ص 63

3 غاني مرضي الشمري ، المرجع السابق ، ص 61

4. علوي علي احمد الشارفي المرجع نفسه ، ص 63

الجزائري كل فعل المادي او معنوي يتضمن الإساءة، التحقير، السخرية، او المساس بالذات الالهية او الانبياء او الكتب السماوية او الشعائر او المقدسات الدينية المعترف بها.¹

ثانيا : الجرائم الواقعة على الاموال:

1-السرقه الالكترونية: " وتعتبر السرقه الإلكترونية والمعطيات المعلوماتية من الجرائم الواقعة على الاموال فهي من الجرائم مستحدثة التي لها علاقة وثيقة بتكنولوجيا المعلومات ف جريمة السرقه المعلوماتية تختلف في ادواتها عن جرائم السرقه التقليدية مع بروز المفهوم الجديد للمال المعلومات المعنوي...."² وحسب الاستاذ عبد الكريم النعمان ان السرقه المعلوماتية تتميز عن السرقه التقليدية في انها ترد على محل معنوي يتمثل في المعلومات والبرامج وعناصر اخرى يصعب تصنيفها اذا كانت من العناصر المادية للمعلوماتية ام انها من عناصرها المعنوية كالدوائر المتكاملة مثلا التي يمكن ان تكون محلا لجريمه السرقه والمعلومات التي تحويها يصعب فصلها عنها فقد تكون السرقه بسرقة الوسيط الذي يتضمنها وقد تكون السرقه بمجرد قراءتها على شاشة الحاسب الالكتروني او نسخها على قرص مضغوط

2-جريمة الارهاب الالكتروني: تعد من صور الجريمة السيبرانية بحيث تعد جريمة الارهاب الالكتروني مفهوما مستحدثا يعتمد على تقنية انظمة المعلومات كوسيلة لارتكاب الفعل حيث تطل نتائج امن المعلومات وتتسبب في اضرار واسعة النطاق وعظيمة الاثر على المجتمع بحيث تعرض سلامة المجتمع وامنه للخطر كما تظهر تأثيراته على سياسة الدولة واجبارها على عمل او امتناع عن عمل او ايقاع الرعب بين الناس ،ولا يعتد التشريع بالدوافع في هذه الجريمة مثل الشهرة او اثبات الذكاء بل يركز على اثار الفعل التي تمتد للمجتمع محليا ودوليا ومدى تسببه في ايقاع الرعب واحتمال وقوعه ،اما اركانها فالركن المادي (السلوك الاجرامي) يتكون من عدة عناصر تتمثل في:³

- استخدام قدر كافي من العنف و التهديد ذو البعد المعنوي الالكتروني.-ان يؤدي هذا السلوك الى ايقاع الرعب بين الناس او تعريض حياتهم للخطر- ان يكون العمل فرديا او جماعيا وتتجلى صور واشكال الارهاب الالكتروني في تخريب البنية التحتية مثل التلاعب بأنظمة الاشارات الضوئية او انظمة ضغط

¹ علوي علي احمد الشارفي المرجع السابق ص 64

² عبد الكريم نعمان، مقال جريمة السرقه المعلوماتية في التشريع الجزائري المجلة الأكاديمية للبحث القانوني المجلد 15

العدد 2024/02، ص، 102-122

³ اسامة احمد المناعسة، جلال محمد الزغبى المرجع السابق، ص 323

الغاز والمياه والكهرباء ، الاضرار بالموارد الوطنية وتعريضها للخطر او تعطيل احكام الدستور والقوانين كذلك العمليات المالية كالقيام بتحويلات او عمليات مصرفية الكترونية مرتبطة بعمل ارهابي الاعتداءات التقنية بتعطيل الاتصالات واختراق شبكات المعلومات او التشويش عليها اما التهديد السياسي كالقيام باي عمل الكتروني يعرض نظام الحكم في الدولة للخطر او يهدف لتغيير كيان الدولة الاقتصادي او الاجتماعي¹

وقد جرمه المشرع الاردني في المادة 10 من قانون جرائم انظمة المعلومات رقم 30 لسنة 2010 " كل من استخدم نظام معلومات او الشبكة المعلوماتية او انشا موقعا الكترونيا لتسهيل القيام بأعمال ارهابية او دعم لجماعة او تنظيم او جمعية تقوم بأعمال ارهابية او الترويج لاتباع افكارها او تمثيلها يعاقب بالأشغال الشاقة المؤقتة"²

المطلب الثاني: اثار الجرائم السيبرانية:

رغم تطور التكنولوجيا والاتصالات والمعلومات ورغم ما حققته من تنمية في مختلف المجالات الثقافية والاجتماعية والاقتصادية من سهولة الوصول الى المعلومات والمعرفة والمساهمة في نشر الثقافة والتعرف على الحضارات المختلفة وتطوير التعليم من جهة وتعزيز التواصل الاجتماعي وتسهيل حياة الفرد وتحقيق الرفاهية وحتى تحسين الحياة الصحية اما من الناحية الاقتصادية فهي ساهمت في تطوير التجارة وزيادة النمو الاقتصادي ناهيك عن اختصار المسافات ، الا ان تكنولوجيا الاتصالات والمعلوماتية تبين انها سلاح ذو حدين رغم كل هذه المزايا الا ان هذا التطور السريع يقابله من جهة ثانية تطور اسرع في مجال الجريمة السيبرانية التي اصبحت تؤرق العالم ككل فكانت لها تأثيرات جد خطيرة على اقتصاد الدول وعلى الحياة الاجتماعية وحى السياسية والامن القومي ، كما رتبت اثار على الجانب القانوني وهذا ما سنتطرق اليه فيمايلي .

¹ اسامة احمد المناعسة ، جلال محمد الزغبى المرجع السابق ، ص 323-324

² اسامة احمد المناعسة، جلال محمد الزغبى ، المرجع نفسه ، ص 325

الفرع الاول: الاثار الاقتصادية للجريمة السيبرانية:

لقد ترتب على الجريمة السيبرانية اثار اقتصادية ومالية عميقة ، اثرت بشكل كبير على استقرار المؤسسات العامة والخاصة على حد سواء وبخاصة القطاع المصرفي والمالي وهذا ما أكدته الاحصائيات العالمية التي وضحت حجم الخسائر المالية الفادحة التي تتكبدها الشركات وكانت الولايات المتحدة الامريكية من اكثر الدول استهدافا للهجمات الرقمية مما ادى الى نهب المال وتسبب في فقدان ثقة العملاء وتكاليف انظمة الحماية التقنية وفيما يلي اهم الاضرار على المستوى الاقتصادي .

الخسائر المالية الناتجة عن الجريمة السيبرانية: تُعد الخسائر المالية الناتجة عن الجريمة السيبرانية

أو الإلكترونية من أبرز التحديات التي تواجه المؤسسات الاقتصادية المعاصرة، حيث تتنوع هذه الخسائر بين تكاليف مباشرة ناتجة عن الهجمات وتكاليف غير مباشرة تتعلق بالحماية، ويمكن تفصيل هذه الخسائر كما يلي :

شهدت التكلفة العالمية للجريمة الإلكترونية زيادة مستمرة، حيث بلغت ذروتها في عام 2017 لتصل إلى 11.7 مليون دولار كمتوسط تكلفة عالمية للمؤسسة الواحدة، مسجلةً زيادة قدرها 27.4% مقارنة بالعام الذي سبقه، في التكلفة العالمية تنصدر الولايات المتحدة الأمريكية قائمة الدول الأكثر تضرراً من حيث حجم الخسائر، حيث قفزت التكاليف فيها من 11.56 مليون دولار في 2013 إلى 21.22 مليون دولار يعتبر قطاع الخدمات المالية هو الأكثر تكلفة وتضرراً، حيث بلغت خسائره 18.28 مليون دولار في عام 2017 ، يليه قطاع المرافق والطاقة بخسائر قدرت بـ 17.2 مليون دولار تُعد المؤسسات المصرفية هدفاً رئيسياً لأن "النقد" هي السلعة الأساسية التي تتعامل بها، مما يجعلها عرضة لخسائر مالية فادحة سنوياً¹

يرتفع متوسط تكلفة الجريمة في الشركات التي تتبنى أجهزة أمنية منخفضة إلى 11.1 مليون دولار، بينما ينخفض إلى 7.9 مليون دولار² . ، إن الجريمة السيبرانية لا تكتفي بسلب الأموال مباشرة، بل

¹ وهيبه عبد الرحيم، ومن معها ،الجرائم الالكترونية من خلال مؤشرات عالمية واثارها على المؤسسات ،مجلة دراسات الصادرة عن جامعة الأغواط، المجلد 16، العدد 01، في شهر جانفي من عام 2019 ص 42، 43، 44

² وهيبه عبد الرحيم، . أمين بن سعيد، نادية عبد الرحيم ،المرجع نفسه ص 44

تُنهك ميزانيات الشركات من خلال رفع تكاليف التشغيل، وتعطيل الإنتاج، وفرض استثمارات إجبارية في أنظمة الحماية للوقاية من التهديدات المتزايدة.¹

ومن المتوقع أن تكلف الجرائم الإلكترونية الاقتصاد العالمي 10.5 تريليون دولار في عام 2026، وقد تصل إلى 15 تريليون دولار بحلول عام 2029.

يشعر 43% من المديرين التنفيذيين أن الجهات الفاعلة في التهديدات أكثر تقدماً من فرق الأمن الداخلية لديهم سيؤدي الخطأ البشري وسوء التكوين إلى 95% من الثغرات الأمنية السحابية في عام 2026.

من المتوقع أن يصل التأثير الاقتصادي طويل الأجل لبرامج الفدية إلى 265 مليار دولار سنوياً بحلول عام 2031، مما يعكس كلاً من تزايد حجم الهجمات وزيادة الطلب على خدماتها. ستستغل الجرائم الإلكترونية بشكل متزايد هويات المستخدمين وثقة العملاء والسلوك البشري بدلاً من الاعتماد فقط على نقاط الضعف.²

سيكون التشفير هو أكثر طرق الوصول الأولية استخداماً في عام 2026 في الوقت الذي استغرقته لفتح هذه المقالة، ربما تكون إحدى المؤسسات قد تعرضت لسرقة كلمة مرور، أو رسالة بريد إلكتروني للتصيد الاحتيالي تم إنشاؤها بواسطة الذكاء الاصطناعي، أو نقطة نهاية API لم يتم أحد بفحصها. هذه هي الحقيقة المزعجة حول الإنترنت في عام 2026.³

¹ د. وهبة عبد الرحيم ، أمين بن سعيد ، نادية عبد الرحيم ، المرجع السابق ص 52

² أكثر من 90 احصائية عن الجرائم الإلكترونية عام 2026 انظر الرابط الإلكتروني www.getastra.com . تاريخ تحديث

النشر 26 مارس 2026 تاريخ الاطلاع 02 افريل 2026

2 انظر الرابط الإلكتروني www.getastra.com المرجع نفسه .

الفرع الثاني : الآثار الاجتماعية للجريمة السيبرانية

تؤدي الجريمة السيبرانية إلى آثار اجتماعية عميقة وخطيرة تتجاوز مجرد الخسائر المادية، لتتأثر استقرار الأفراد والمجتمعات وبنيتها الأساسية. وتتلخص أبرز هذه الآثار استناداً إلى المصادر فيما يلي:

1- تآكل الثقة بين الأفراد والمؤسسات: تعد من أخطر الآثار الاجتماعية، حيث يولد تكرار الهجمات الإلكترونية شعوراً لدى المواطنين بعدم قدرة المؤسسات الحكومية والخاصة على حماية بياناتهم ، هذا التشكيك يدفع الأفراد إلى الحذر الشديد أو العزوف عن التعامل مع الخدمات الرقمية الحكومية والبنكية، مما يضعف كفاءة الدولة في التحول الرقمي .

تعزيز الفجوة الرقمية والاجتماعية: تساهم الجريمة السيبرانية في توسيع الفجوة بين من يمتلكون المهارات التقنية القادرة على توفير الحماية لأنفسهم ومن يفتقرون إليها من الفئات الأقل معرفة تقنياً مثل بعض الطلاب تصبح أكثر عرضة للاختراق والتهميش الاجتماعي والاقتصادي، مما يزيد من معدلات الفقر بينهم نتيجة تعرضهم للاحتيال .

بالإضافة الى تفكك الروابط الأسرية و زيادة معدلات الجرائم التقليدية والعنف لوحظ أن بعض ضحايا الجرائم الإلكترونية قد يلجؤون إلى الانتقام بطرق غير قانونية للقبض على المحتالين أو استرداد حقوقهم، مما يساهم في تفشي العنف الجسدي في المجتمع وحالة من الانفلات الاجتماعي¹.

العزلة الاجتماعية والقلق المستمر: تسبب الجرائم السيبرانية حالة من الخوف الدائم وفقدان الخصوصية، مما يدفع بعض الضحايا إلى تجنب استخدام وسائل التواصل الاجتماعي أو الإنترنت بشكل كامل، وهذا ما يؤدي إلى فقدان الروابط الاجتماعية الضرورية في العصر الرقمي الحديث.

الآثار النفسية الجماعية: يعاني نحو 40% من الضحايا من اضطرابات نفسية مثل القلق والاكتئاب والأرق الشديد ، هذه الحالة النفسية لا تؤثر على الفرد فحسب، بل تمتد لتؤثر على جودة حياته وعلاقاته

الاجتماعية والمهنية داخل المجتمع .¹

¹ عبد الحميد بوديار، رشيد طبال ، مقال الجريمة السيبرانية وتأثيراتها على الفرد والمجتمع في عصر التكنولوجيا ، مجلة الباحث في العلوم الانسانية والاجتماعية ، المجلد 16/العدد 01- السنة 2025. ص 21 ، 22

الفرع الثالث : الآثار على المستوى السياسي والامن القومي تتمثل الآثار والمخاطر المترتبة على الجريمة الإلكترونية على المستوى السياسي في تحولها إلى أداة صراع جديدة ومكشوفة بين الدول، ولم تعد مجرد جرائم فردية بل تجاوزت الحدود المعتادة، ويمكن تلخيص أبرز هذه الآثار السياسية في:

1- الجريمة السيبرانية أداة في الصراع السياسي الدولي: أصبحت جرائم المعلومات وسيلة تُستخدم في النزاعات السياسية والاقتصادية بين الدول، حيث شهد عام 2011 جولات صراع علنية عبر الفضاء الإلكتروني.

2- التجسس وجمع المعلومات الاستخباراتية: بحيث تُصمم بعض الفيروسات المتطورة، مثل فيروس "دوكو" لغرض أساسي هو جمع معلومات استخباراتية ومعلومات عن الأصول من منظمات معينة، مثل الشركات المصنعة لمكونات بيئات التحكم الصناعي. ويهدف هذا النوع من التجسس إلى الحصول على وثائق التصميم التي قد تُستخدم لاحقاً لشن هجمات على منشآت حيوية.²

3- تخريب البرامج والمنشآت الوطنية: يُعد فيروس "ستكسنت" نموذجاً لاستخدام الأسلحة السيبرانية في إحداث فوضى داخل برامج دول أخرى، كما أشارت التقارير إلى استخدامه ضد البرنامج النووي الإيراني. ظهور جماعات القرصنة ذات الأهداف السياسية: برزت جماعات متخصصة من القرصنة الإلكترونية ، مثل جماعة "انونيموس Anonymous " وجماعة "لؤلؤسيك LulzSec "

التي تستهدف الشركات والأفراد لتحقيق مآرب وأجندات سياسية مختلفة، وتتميز هذه الجماعات بقدرة متزايدة على اختراق الشبكات والإفلات من الرصد والمقاضاة القانونية.³

4- ترويج الفكر المتطرف: استغلت الجماعات المتطرفة والتيارات الفكرية المختلفة فضاء الإنترنت المفتوح لنشر ثقافة العنف والكراهية والترويج لأفكارها، خاصة في ظل استغلال الواقع المتردي في بعض المجتمعات .

¹ عبد الحميد بوديار، رشيد طبال ، مرجع نفسه، ص 21، 22،

² سعيدي سليمة، حجازي بلال ، جرائم المعلومات والشبكات في العصر الرقمي ، الطبعة الاولى ، دار الفكر الجامعي ، 2018 ص 65

³ سعيدي سليمة، حجازي بلال ، المرجع نفسه، ص 66،

خلاصة الفصل

الجريمة السيبرانية جريمة مستحدثة وقد استقر الفقه المعاصر على تسميتها بمصطلح الجريمة السيبرانية كونه الأكثر شمولاً لتغطية كافة الجرائم المرتبطة بالفضاء الرقمي ، ولقد تعددت التعاريف الفقهية لهذه الجريمة بين الاتجاه المضيق لمفهومها والاتجاه الموسع ، أما التشريعات المقارنة فقد فضلت أغلب القوانين عدم تعريف الجريمة الالكترونية .

من جهة اخرى تتميز الجريمة السيبرانية بخصائص فريدة، أبرزها أنها عابرة للحدود الجغرافية، مما يمس بسيادة الدول وتنفذ في بيئة رقمية افتراضية، كما تتسم بصعوبة الإثبات والتتبع نظراً لطبيعة الدليل الرقمي القابل للمحو السريع، وتوصف بأنها جريمة ناعمة تعتمد على الجهد الذهني والخبرة التقنية بدلاً من العنف المادي.

تقوم الجريمة السيبرانية على ثلاثة أركان أساسية الركن الشرعي المستند لمبدأ لا جريمة ولا عقوبة إلا بنص، والركن المادي الذي يتكون من السلوك الإجرامي مثل الاختراق والنتيجة الجرمية والعلاقة السببية بينهما والركن المعنوي المتمثل في العلم بعناصر الجريمة وإرادة تحقيق النتيجة الإجرامية تتنوع صور هذه الجرائم لتشمل الاعتداء على سلامة البيانات، والجرائم المرتبطة بالمحتوى كإلحاق الضرر والقذف والاعتداء على الملكية الفكرية، وصولاً إلى الإرهاب الإلكتروني ،

وتخلف هذه الجرائم آثاراً اقتصادية فادحة تتمثل في خسائر بمليارات الدولارات وآثاراً اجتماعية بالغة الخطورة بالإضافة إلى تهديد الأمن القومي والسياسي من خلال التجسس وتخريب المنشآت الحيوية .

الفصل الثاني

الأليات القانونية والمؤسسية على المستويين الدولي
والوطني لمكافحة الجريمة السيبرانية

بعد ان تطرقنا في الفصل الاول الى الاطار المفاهيمي للجريمة السيبرانية من خلال تحديد مفهومها وخصائصها واركائها وابرز اهم صورها وانتهينا الى الاثار الخطيرة التي ترتبت عنها على الصعيد الاقتصادي والاجتماعي والسياسي ، مما اصبح يهدد الامن القومي للدول فكان لابد من ايجاد اليات لمواجهةها والتصدي لها ، واستكمالا لدراستنا استوجب علينا الامر الانتقال الى معالجه الآليات القانونية والمؤسسية المعتمدة في مكافحتها في ظل وجود قوانين تقليدية لا تستوعب هذا النوع المستحدث من الجرائم.

فاصبح الامر يتطلب منظومة متكاملة من الاجراءات والتدابير على المستويين الدولي والوطني وتزداد الحاجة الملحة الى هذه الآليات بالنظر الى طبيعتها العابرة للحدود، الامر الذي يتطلب تعاون الجهود الدولية من خلال أطر قانونية اتفاقية وهيئات دولية مختصة الى جانب تطوير اطر تشريعية ومؤسسية وطنية في مواجهتها لعلها تواكب التطور المستمر لهذه الجريمة وتتصدى لها، وعليه نهدف في هذا الفصل الى ابراز اهم اليات مواجهة هذه الجريمة فدرسنا كل هذا في مبحثين

المبحث الاول: اليات مواجهة الجريمة السيبرانية على المستوى الدولي.

المبحث الثاني: اليات مواجهة الجريمة السيبرانية على المستوى الوطني.

المبحث الاول: آليات مواجهة الجريمة السيبرانية على المستوى الدولي

لمواجهة هذه الجريمة المستحدثة العابرة للحدود استدعى الامر ضرورة تكاتف الجهود الدولية وتعزيز التعاون بين كافة الدول من اجل وضع اطار قانوني دولي مشترك يهدف الى مكافحة هذه الجريمة بفعالية و يتجلى ذلك من خلال اتفاقيات دولية واقليمية واليات مؤسسية وأليات تعاون دولية.

ولدراسة كل هذا قسمنا هذا المبحث إلى ثلاثة مطالب ، ك مطلب أول سيتم التطرق إلى الآليات القانونية الدولية لمكافحة الجريمة السيبرانية ، بينما خصصنا المطلب الثاني للآليات المؤسسية الدولية لمكافحة الجريمة السيبرانية و المطلب الثالث لآليات التعاون الدولي في مكافحة الجريمة السيبرانية .

المطلب الاول: الآليات القانونية الدولية لمكافحة الجريمة السيبرانية

في ظل ظهور جريمة تقنية رقمية مستحدثة وخطيرة لم تعد القوانين التقليدية قادرة على استيعابها ومواجهتها بفعالية، فكان لزاماً على رجال القانون السعي إلى وضع أطر قانونية دولية جديدة للتصدي لهذه الجريمة الخطيرة العابرة للحدود التي أرقّت الدول ، فتم إبرام عدة اتفاقيات دولية وتنظيمات قانونية تتناسب وتواكب التطور المتسارع لهذه الجريمة ، فكان لابد من الحد من هذه الجرائم السيبرانية ومكافحتها وتعزيز التعاون الدولي بشأنها، اين اسفر العمل الدولي في هذا الشأن على عدت اتفاقيات دولية واقليمية .

الفرع الاول: اتفاقية بودابست 2001

اولا- تعريف اتفاقية بودابست :

"تُعرف اتفاقية بودابست لعام 2001 رسمياً بالاتفاقية الأوروبية لمكافحة جرائم المعلوماتية أو الجرائم الإلكترونية وهي نتاج جهد دولي وإقليمي واسع قادته اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية على مدار أكثر من عشرة أعوام ، وقد تم إقرار مسودتها النهائية في بودابست عام 2001 لتصبح أول معاهدة دولية تتناول الجرائم التي تُرتكب عبر الإنترنت والشبكات الحاسوبية"¹

ثانيا : الملامح الرئيسية للاتفاقية: تتكون الاتفاقية من مقدمة وأربعة فصول أساسية موزعة كالاتي:

الفصل الأول: يغطي المصطلحات والمفاهيم الأساسية مثل معطيات الكمبيوتر ومزود الخدمة،

¹ عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية والانترنت الجرائم الالكترونية دراسة مقارنة في النظم القانونية لمكافحة جرائم المعلوماتية والانترنت مع الاشارة الى جهود مكافحتها محليا وعربيا ودوليا ، ط1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007 ص 124.

الفصل الثاني يتعلق بالتدابير الواجب اتخاذها وطنياً، ويشمل القانون الموضوعي (التجريم)، والقانون الإجرائي (التحقيق والضبط)، وقواعد الاختصاص القضائي، أما الفصل الثالث ينظم آليات التعاون الدولي والمبادئ العامة والمساعدة القانونية المتبادلة، الفصل الرابع يتضمن الأحكام الختامية للاتفاقية¹

ثالثاً: الأهداف الاستراتيجية للاتفاقية:

تستهدف الاتفاقية تحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة إليها من خارج أوروبا، لتكون بمثابة دليل إرشادي ومرجعية وطنية لمكافحة الأنشطة التي تمس سرية وسلامة وتوفر المعلومات، كما تسعى لبناء شبكة تعاون عالمية لملاحقة الجرائم العابرة للحدود.²

لا سيما مواجهة المخاطر المدمرة لجرائم الكمبيوتر حيث أكدت مقدمة الاتفاقية الحاجة الماسة لاتخاذ تدابير تشريعية لمكافحة هذه الجرائم، خاصة في ظل الانتشار الواسع لشبكات المعلومات والنماء الكبير لأنظمة الحوسبة المفتوحة وتدفق المعلومات عبر الحدود، ومن أهداف الاتفاقية أيضاً حماية أمن المعلومات حيث استهدفت الاتفاقية مكافحة الأنشطة التي تمس العناصر الثلاثة الأساسية لأمن المعلومات وهي السرية، وسلامة المحتوى، وتوفر المعلومات والنظم كذلك سد الثغرات الإجرائية، حيث سعت الاتفاقية إلى توفير قواعد قانونية ملائمة لعمليات التحري والتحقيق والضبط والتفتيش والمحاكمة، بما يتناسب مع الطبيعة التقنية المعقدة للجرائم الإلكترونية التي قد لا تترك أثراً مادياً.³

أما فيما يخص تعزيز التعاون الدولي والإقليمي ونظراً للطابع العابر للحدود لهذه الجرائم، برزت ضرورة ملحة لخلق إطار للتعاون الدولي يضمن ملاحقة مرتكبي الجرائم وكشفهم وتنسيق الجهود بين الدول لتبادل المعلومات الاستخباراتية والقانونية، كما سعت إلى توحيد السياسات التشريعية حيث استهدفت الاتفاقية تحقيق وحدة في التدابير التشريعية بين الدول الأوروبية والدول المنضمة إليها من خارج أوروبا، لتكون بمثابة دليل إرشادي ومرجعية وطنية عند سن قوانين مكافحة جرائم التقنية.⁴

علاوة على ذلك ركزت الاتفاقية على ضرورة إيجاد توازن دقيق بين متطلبات تنفيذ القانون كالتفتيش والضبط وبين احترام الحقوق الأساسية للإنسان⁵

¹ اتفاقية بودابست مجلس أوروبا 2026 تاريخ الاطلاع: 25 افريل 2026: <https://www.coe.int>

² عبد الله عبد الكريم عبد الله، المرجع سابق ص 127

³ اتفاقية بودابست مجلس أوروبا المرجع السابق

⁴ اتفاقية بودابست مجلس أوروبا المرجع السابق

⁵ عبد الله عبد الكريم عبد الله، المرجع سابق ص 128،

رابعاً : الطوائف الإجرامية التي شملتها: أوجدت الاتفاقية تقسيماً جديداً نسبياً شاملاً لجرائم الكمبيوتر واحكامها القواعد الموضوعية شمل أربع طوائف رئيسة وطائفة خامسة تتعلق بأحكام المساهمة والعقوبات لهذه الطوائف الاربعة ، وتم التقسيم كما يلي :

1-جرائم تستهدف أمن المعلومات: مثل الدخول غير القانوني (الاختراق)، والاعتراض غير القانوني للبيانات، والتدخل في المعطيات أو الأنظمة، وإساءة استخدام الأجهزة

2-الجرائم المرتبطة بالكمبيوتر: مثل التزوير المعلوماتي والاحتيايل المعلوماتي¹

3-الجرائم المرتبطة بالمحتوى: وركزت بشكل أساسي على مكافحة دعارة الأطفال عبر الأنظمة المعلوماتية

4-الجرائم المرتبطة بحق المؤلف: التي تستهدف المصنفات الرقمية والحقوق المجاور

5- الطائفة الخامسة : المساهمة الجرمية والعقوبة ويعالج الشروع والمساعدة والتحريض ومسؤولية الاشخاص المعنية ومعايير العقاب في المواد 11،12،13²

خامساً :أبرز الإجراءات الجنائية الجديدة التي نصت عليها الاتفاقية:

1- الحفظ السريع للمعطيات المخزنة و يهدف هذا الإجراء إلى ضمان الاحتفاظ بالمعلومات الرقمية وحمايتها من التلف أو فقدان، نظراً لكون الأدلة الرقمية مؤقتة وسريعة التغير، وتسمح الاتفاقية للسلطات الوطنية بإصدار أوامر قضائية أو إدارية للحفظ الفوري للبيانات لضمان عدم فقدان الأدلة الضرورية لكشف الجريمة.³

2- تجميع المعلومات الخاصة بالمشتكرين يشمل ذلك جمع بيانات مثل أرقام الهواتف، وعناوين، البريد الإلكتروني، وعناوين المواقع، وتُعد هذه المعلومات أدوات حاسمة لتحديد هوية الجناة، مع التأكيد على ضرورة أن يتم ذلك وفق إجراءات رسمية وبإذن قضائي لحماية الخصوصية الرقمية.

3- التفتيش المعلوماتي و يتطلب هذا الإجراء إذناً رسمياً للوصول إلى البيانات في مواقع محددة بهدف جمع الأدلة الرقمية دون المساس بالحقوق الأساسية للأفراد ، و يرتبط هذا أيضاً بالتنصت الرقمي اعتراض البيانات وهو أداة تسمح باعتراض المراسلات أو تسجيل المكالمات أو النقاط الصور في الفضاء

¹ عبد الله عبد الكريم عبد الله، المرجع نفسه ص 130،131

² عبد الله عبد الكريم عبد الله، المرجع سابق ص 131،130

³ سعيد مسعود الكثيري، المرجع نفسه ، الصفحة ، 959

الفصل الثاني: الآليات القانونية والمؤسسية على المستويين الدولي والوطني لمكافحة الجريمة السيبرانية

الرقمي، ويشترط هذا الإجراء الحصول على موافقة السلطات القضائية لضمان استخدامه بطريقة قانونية و محدودة¹.

4- ويعتبر التعاون الدولي المنصوص عليه في المادة 23 وما بعدها الركيزة الأساسية لتفعيل الإجراءات السابقة، حيث تنص الاتفاقية على تبادل المعلومات والأدلة بسرعة وفعالية بين الدول، و وضع آليات لتسليم المجرمين والتنسيق في التحقيقات عبر الحدود.

ومن الإجراءات أيضا تحديد المصطلحات القانونية جديدة اين ركزت الاتفاقية على صياغة تعريفات دقيقة لمصطلحات مثل "التفتيش الرقمي" و "الحفظ السريع للبيانات"، مما يعالج غموض القوانين التقليدية ويضمن توحيد الإجراءات القضائية بين الدول الأعضاء.

وتسعى هذه الإجراءات بمجملها إلى تحقيق توازن دقيق بين فعالية التحقيق الجنائي وبين حماية حقوق الأفراد وخصوصيتهم في العالم الرقمي كما وفرت الاتفاقية سياقاً تشريعياً يسهل ملاحقة الجناة الذين غالباً ما يرتكبون جرائمهم من دول تختلف عن دول ضحاياهم.²

سادسا : آليات التعاون التي اقترتها اتفاقية بودابست

أقرت اتفاقية بودابست آليات شاملة للتعاون الدولي والإقليمي في الفصل الثالث منها، والذي خُصص بالكامل لتنظيم هذا التعاون عبر مستويين أساسيين، المبادئ العامة المواد 23-28 والنصوص الخاصة المواد 29-35 وتتمثل أبرز هذه الآليات والأسس فيما يلي:

1- بناء شبكة تعاون عالمية تهدف الاتفاقية إلى إيجاد قاعدة معلومات فاعلة تتيح للدول ملاحقة مرتكبي الجرائم الإلكترونية وكشفهم وتنسيق الجهود الدولية في هذا الإطار

2- تنسيق الإجراءات القضائية والأمنية حيث ركزت الاتفاقية على تسهيل عمليات التحري والتحقيق والضبط والتفتيش والمحاكمة على المستوى الدولي، بما يضمن ملاحقة الجرائم العابرة للحدود بفعالية.

3- توحيد التدابير التشريعية اين سعت الاتفاقية لتحقيق وحدة وانسجام في القوانين بين الدول الأعضاء والدول المنضمة إليها من خارج أوروبا، ليكون التعاون القانوني مبنياً على مرجعية ودليل إرشادي موحد الاستناد إلى الاتفاقيات الثنائية والجماعية بحيث تعتمد آليات التعاون في الاتفاقية على ما

¹ سعيد مسعود الكثيري، الجريمة الإلكترونية في ضوء اتفاقية بودابست الاطار المفاهيمي والتصنيفي، مجلة البحوث القانونية والاقتصادية ، جامعة ظفار عمان ، المجلد 9 العدد 1 2026 ، ص ، 959

² سعيد مسعود الكثيري، المرجع نفسه ، ص ، 959

هو مبرم من اتفاقيات قضائية وأمنية بين الدول، لتعزيز فاعلية أنشطة التحقيق والمقاضاة للجرائم التي تتجاوز النطاق الجغرافي للدولة الواحدة.¹

4-التوازن بين التعاون والحقوق حيث شددت الاتفاقية على أن آليات التعاون الدولي يجب أن تقيم توازناً دقيقاً بين متطلبات تنفيذ القانون لمكافحة الجريمة وبين احترام السيادة الوطنية والحقوق الأساسية للإنسان، مثل حق الخصوصية وحرية الرأي.

5- تفعيل المساعدة القانونية المتبادلة ، فقد تضمنت الاتفاقية نصوصاً خاصة تنظم كيفية تقديم المساعدة القانونية بين الدول في مجال الجرائم التقنية، لضمان تبادل الأدلة والمعلومات المتعلقة بالتحقيقات الجنائية

سابعاً: الصعوبات التي تواجه الاتفاقية:

على الرغم من الأهمية البالغة لهذه الاتفاقية وما حقته من إنجازات ملموسة لكنها تواجه جملة من الصعوبات يتمثل في:

1-عدم انضمام جميع الدول إلى الاتفاقية: يُعد غياب دول كبرى ذات ثقل سياسي وتكنولوجي، مثل الصين وروسيا، عن نطاق الاتفاقية من أبرز التحديات؛ حيث يؤدي ذلك إلى إضعاف فعاليتها نظراً للطبيعة العابرة للحدود لهذه الجرائم. ويخلق هذا الغياب ما يُسمى "مناطق قانونية آمنة" يستغلها المجرمون للإفلات من الملاحقة، خاصة عندما تُرتكب الجريمة في دولة غير طرف بينما يقع الضرر في دولة موقعة.

2- التطور التكنولوجي المتسارع: منذ اعتماد الاتفاقية عام 2001، طرأت تحولات جذرية في البيئة الرقمية شملت انتشار الهواتف الذكية، والحوسبة السحابية، والذكاء الاصطناعي، والعملات المشفرة. وقد أدى هذا التطور إلى ظهور أنماط إجرامية مستحدثة لم تكن مطروحة وقت صياغة الاتفاقية، مما جعل بعض نصوصها غير كافية لمواجهة التهديدات الحديثة أو بحاجة إلى تفسيرات موسعة قد تنثير خلافات قانونية بين الدول

3- تفاوت مستويات التنفيذ والتطبيق العملي: تختلف قدرة الدول الموقعة على ترجمة التزامات الاتفاقية إلى تشريعات وطنية وإجراءات عملية تبعاً لاختلاف إمكاناتها القانونية والتقنية، فبعض الدول تعاني من نقص الخبرات الفنية المتخصصة، أو ضعف البنية التحتية الرقمية، أو بطء الإجراءات القضائية، مما يؤدي إلى تباين في مستوى الحماية والأمن السيبراني ويضعف التعاون الدولي المنشود

¹ اتفاقية بودابست مجلس اوربا، تاريخ الاطلاع: 01 ماي 2026 <https://www.coe.int>

أن مواجهة هذه التحديات تتطلب مراجعة مستمرة لبنود الاتفاقية، وتعزيز شموليتها الدولية، وتقديم الدعم الفني والتشريعي للدول النامية لمواكبة التطورات المتسارعة في هذا المجال¹.

الفرع الثاني: اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية 2024

مما لا شك فيه ان القوانين التي هي من وضع البشر تأتي دائماً ناقصة تستوجب التغيير والتعديل فاذا كانت اتفاقية مجلس واربا اول محاولة لتأطير الجريمة الالكترونية ،الا انها تركت بعض الثغرات القانونية ولم يرحب بها في كل دول العالم فكان لابد من اتفاقية جديدة فكانت اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية 2024.

اولا :تعريف الاتفاقية :

تُعد اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية معاهدة عالمية اعتمدها الجمعية العامة للأمم المتحدة في 24 ديسمبر 2024 تهدف هذه الاتفاقية بشكل أساسي إلى مكافحة الجرائم الإلكترونية وتعزيز التعاون الدولي بين الدول الأطراف، وحماية المجتمعات من التهديدات الرقمية، وتوفير منصة لتبادل الأدلة وحماية الضحايا.²

ثانيا :التأسيس :

فُتح باب التوقيع على الاتفاقية العالمية لمنع الجريمة السيبرانية في 25 أكتوبر/تشرين الأول 2025، وذلك في العاصمة الفيتنامية هانوي ، قامت 65 دولة بالتوقيع على الاتفاقية. يتعين على الدول التي وقعت على الاتفاقية أن تقوم بالمصادقة عليها وفقاً لإجراءاتها الوطنية الخاصة لكل دولة، اما فيما يخص دخول الاتفاقية حيز التنفيذ لا تدخل الاتفاقية حيز التنفيذ فور التوقيع، الا بعد مرور 90 يوماً من تاريخ تصديق الدولة الأربعين عليها لتصبح نافذة³. تعتبر هذه الاتفاقية "صكاً قوياً وملزماً قانوناً" بمجرد إتمام إجراءات المصادقة ودخولها حيز التنفيذ، وتهدف إلى توحيد الدفاعات الجماعية ضد التهديدات الرقمية. كما تُلزم المادة 17 من الاتفاقية الدول

¹ إسلام عبد ربه رمضان عبد ربه هديب، "مكافحة الجريمة السيبرانية في ضوء القانون الدولي"، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية، بدون عدد بدون سنة ، الصفحة 302،303

² اتفاقية الامم المتحدة الامم المتحدة مكتب المعنى بالمخدرات والجريمة تاريخ الاطلاع : 01 ماي 2026 <https://www.unodc.org/unodc/ar/cybercrime /convention/text / convention-full-text.html>

³ اتفاقية الامم المتحدة مرجع سابق تاريخ الاطلاع : 03 ماي 2026

الفصل الثاني: الآليات القانونية والمؤسسية على المستويين الدولي والوطني لمكافحة الجريمة السيبرانية

الأطراف بإبلاغ الأمين العام للأمم المتحدة بقوانينها الوطنية المتعلقة بتنفيذ بعض بنود الاتفاقية، مثل مكافحة غسل العائدات الإجرامية¹.

وكان دورا الجزائر القيادي في الرئاسة والمسار التفاوضي حيث ترأست الجزائر اللجنة المتخصصة المكلفة بإعداد الاتفاقية، وهو ما منحها دوراً محورياً في قيادة المسارات التفاوضية منذ ماي 2021، وساهمت الدبلوماسية الجزائرية في تقريب وجهات النظر بين الدول الأعضاء، مما أدى إلى اعتماد نص الاتفاقية بالإجماع خلال الدورة 79 للجمعية العامة للأمم المتحدة في ديسمبر 2024²، غير انه حتى يومنا هذا لم تدخل اتفاقية الامم المتحدة لسنة 2024 حيز التنفيذ بشكل رسمي رغم اعتماد نصها النهائي وفتح باب التوقيع عليها .

ثالثا: الملامح الرئيسية للاتفاقية :

تتكون اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية من 9 فصول رئيسية، وتضم في مجموعها 68 مادة ، وتنظم هذه الفصول والمواد الأطر القانونية والإجرائية لمكافحة الجرائم الرقمية، ومن أبرز ما تتناوله:

- الفصل الاول : الأحكام العامة ونطاق التطبيق: حيث تحدد المادة 3 سريان الاتفاقية على منع الأفعال المجرمة والتحقيق فيها وجمع الأدلة الإلكترونية وفي المادة 5 صون السيادة وفي المادة 6 احترام حقوق الانسان الفصل الثاني بعنوان التجريم المواد من 7 إلى 17 وتغطي جرائم الوصول والاعتراض غير المشروعين، التدخل في البيانات والأنظمة، إساءة استخدام الأجهزة، التزوير والسرقة المتعلقين بنظام تكنولوجيا المعلومات والاتصالات والجرائم المتعلقة بالاعتداء الجنسي على الأطفال واستدراجهم، بالإضافة إلى النشر غير الرضائي للصور حميمية و غسل العائدات الإجرامية وفي المادة 18 تناولت مسؤولية الاشخاص الاعتباريين والمادة 19 المشاركة و الشروع، الإجراءات الجنائية والعقوبات المواد 21 و 22 وتتناول فرض عقوبات رادعة.³ الفصل الثالث بعنوان الولاية القضائية وتحديد الولاية القضائية للدول على الجرائم المرتكبة في إقليمها أو ضد مواطنيها المادة 22 منها الفصل الرابع : التدابير الاجرائية ونفاذ القانون المواد من 23، 34 الفصل الخامس بعنوان التعاون الدولي من 35 الى المادة 52

¹ اتفاقية الامم المتحدة مرجع سابق تاريخ الاطلاع : 03 ماي 2026

² معاهدة مكافحة الجريمة السيبرانية ثمرة 5 سنوات من المفاوضات الدولية بقيادة الجزائر تاريخ النشر : 2025/10/26
تاريخ الاطلاع : 05 ماي 2026 <https://www.youtube.com/watch?v=@AL24newschannel>

³ اتفاقية الامم المتحدة، المرجع سابق تاريخ الاطلاع : 05 ماي 2026

الفصل السادس: التدابير الوقائية المواد: 53 الفصل السابع المساعدة التقنية وبناء القدرات المواد، 54، 55،
، 56 الفصل الثامن: آلية التنفيذ المواد 57، 58 الفصل التاسع احكام ختامية المواد من 59 الى 68
رابعا :اهداف الاتفاقية :

تسعى الاتفاقية الدولية الدولية لمكافحة الجريمة السيبرانية الى تحقيق مجموعة من الاهداف الجوهرية الت تعكس ادراك المجتمع الدولي لخطورتها تتمثل اهم اهدافها -تعزيز التعاون الدولي: تهدف بشكل أساسي إلى زيادة فعالية جهود منع ومكافحة الجرائم السيبرانية من خلال تيسير التعاون وتنسيق التحقيقات وتبادل المعلومات الأدلة الإلكترونية بين الدول. - بناء القدرات والدعم الفني: تركز على توفير الدعم الفني والتقني وبناء القدرات القانونية والفنية، ولا سيما لصالح الدول النامية لمساعدتها على مواكبة التطور التكنولوجي السريع. - حماية الحقوق والمجال الرقمي: تسعى لتعزيز آليات مكافحة الجريمة وحماية البنى التحتية الحيوية مع ضمان تحقيق التوازن وحماية الأشخاص وحقوقهم وحررياتهم الأساسية في الفضاء الرقمي¹

خامسا : أهم الجرائم التي تجرمها الاتفاقية

تُلزم الاتفاقية الدول الأطراف باتخاذ تدابير قانونية لتجريم مجموعة من الأفعال منها:

- 1- الوصول غير المشروع: الدخول غير المصرح به إلى أنظمة تكنولوجيا المعلومات والاتصالات.
- 3- الاعتراض غير المشروع: اعتراض البيانات الإلكترونية بوسائل تقنية أثناء إرسالها
- 2- التدخل في البيانات والأنظمة: إتلاف أو حذف أو تحويل البيانات الإلكترونية، أو إعاقة عمل الأنظمة عمداً.
- 4- إساءة استخدام الأجهزة: إنتاج أو بيع أو حيازة برامج أو أجهزة مصممة لارتكاب جرائم سيبرانية
- 5- الجرائم ضد الأطفال: إنتاج أو توزيع مواد تتعلق بالاعتداء الجنسي على الأطفال، أو استدراجهم عبر الإنترنت لغرض جنسي.

6- غسل العائدات الإجرامية: تحويل أو إخفاء الأموال والأصول الناتجة عن الجرائم السيبرانية²

سادسا :آليات التعاون الدولي :

تضع الاتفاقية إطاراً شاملاً للتعاون بين الدول لضمان استجابة سريعة للجرائم العابرة للحدود، و تشمل هذه الآليات:

¹ إسلام عبد ربه رمضان عبد ربه هديب، "المرجع السابق، ص 304

² انظر اتفاقية الامم المتحدة، المرجع سابق تاريخ الاطلاع : 01 ماي 2026

الفصل الثاني: الآليات القانونية والمؤسسية على المستويين الدولي والوطني لمكافحة الجريمة السيبرانية

- 1- شبكة اتصال تعمل على مدار الساعة (7/24): تعيين جهة اتصال لتقديم مساعدة فورية في التحقيقات، وتبادل المعلومات التقنية، وتحديد أماكن المشتبه فيهم.
- 2- تبادل الأدلة الإلكترونية و ذلك لتسهيل الحصول على الأدلة الرقمية والاحتفاظ بها ومشاركتها لأغراض الملاحقة القضائية.
- 3- المساعدة القانونية المتبادلة وتشمل تسليم المطلوبين، ودعم التحقيقات، واسترداد عائدات الجريمة.
- 4- تجميد ومصادرة الأصول و ذلك بتمكين السلطات من تتبع وتجميد ومصادرة الممتلكات أو الأدوات المستخدمة في الجرائم.¹

سابعا : التحديات التي تواجه الاتفاقية

تواجه اتفاقية الأمم المتحدة الجديدة لمكافحة الجريمة السيبرانية لعام 2024 مجموعة من التحديات التي قد تحد من فعاليتها، وتصنف هذه التحديات في المصادر إلى جانبين رئيسيين: تحديات التنفيذ والتعاون الدولي، وتحديات فنية تكنولوجية. تتمثل أبرز هذه التحديات فيما يلي:

- 1- **تحديات التنفيذ والتعاون الدولي:** يعتمد نجاح الاتفاقية بشكل أساسي على مدى التزام الدول الموقعة بتطبيق بنودها وتبرز الخلافات السياسية واختلاف المصالح الاستراتيجية بين الدول كعائق يعرقل التعاون الفعلي في ملاحقة المجرمي. إلا أنه حصل تباين الاستجابة لطلبات التعاون أين ظهر التحديات في الواقع العملي من خلال تفاوت مستويات الاستجابة لطلبات المساعدة القانونية المتبادلة، أو التأخير في تبادل المعلومات والأدلة الرقمية، مما يضعف التحقيقات الجنائية العابرة للحدود² اختلاف الأنظمة القانونية يؤدي اختلاف النظم القانونية والإجرائية، خاصة في مجالات حماية البيانات والخصوصية، إلى إشكاليات قانونية وتفسيرات متباينة لنصوص الاتفاقية.
- مخاوف السيادة تشكل مخاوف الدول من المساس بسيادتها الوطنية تحدياً مستمراً يحول دون تحقيق التعاون الدولي الأمثل³.

- 2- **التحديات الفنية ومواكبة التطور التكنولوجي:** التسارع التقني وظهور أنماط مستحدثة: تتطور الجرائم السيبرانية بوتيرة تفوق قدرة الأطر القانونية التقليدية على المواكبة. وقد أفرزت تقنيات مثل الذكاء

¹ اتفاقية الامم المتحدة مرجع نفسه ، تاريخ الاطلاع : 02 ماي 2026

² إسلام عبد ربه رمضان عبد ربه هديب، "المرجع السابق" ، ص 309

³ إسلام عبد ربه رمضان عبد ربه هديب، "المرجع السابق" ، ص 309

الاصطناعي، وسلاسل الكتل (Blockchain) ، والعملات المشفرة أنماطاً إجرامية لم تكن في الحسبان وقت وضع نصوص الاتفاقية.

- الحاجة للمراجعة الدورية نظراً للتطور السريع، قد تصبح بعض أحكام الاتفاقية غير كافية، مما يفرض ضرورة إجراء مراجعات دورية وتحديثات مستمرة للنصوص لتتلاءم مع المستجدات التقنية.

- فجوة القدرات في الدول النامية حيث تواجه الاتفاقية تحدي نقص الخبرات الفنية والكوادر المتخصصة والبنية التحتية التقنية اللازمة في العديد من الدول، ولا سيما النامية منها، مما يعيق قدرتها على تطبيق أحكام الاتفاقية بفعالي أن مواجهة هذه التحديات تتطلب إرادة سياسية قوية، وتوحيد الأطر التشريعية الدولية، وتقديم دعم فني وتدريب مستمر للدول لضمان تحقيق توازن بين الأمن السيبراني وحماية الحقوق والحريات¹.

الفرع الثالث: المقارنة بين الاتفاقيتين

إذا ما حولنا المقارنة بين الاتفاقيتين نجد ان اتفاقية الأمم المتحدة تُعتبر أول صك دولي عالمي وشامل يتم اعتماده من قبل الجمعية العامة للأمم المتحدة، مما يمنحها صبغة متعددة الأطراف تشمل جميع الدول الأعضاء؛ كما أنها تهدف لضمان عدم ترك أي دولة دون حماية بغض النظر عن مستوى تطورها منها بعض دول نامية ، اما اتفاقية بودابست نعلم بانها معاهدة إقليمية في الأصل مجلس أوروبا انضمت إليها دول من خارج أوروبا لاحقاً، تسعى لبناء سياسة جنائية موحدة.

*اما من حيث النطاق و الشمولية فنجد بان اتفاقية بودابست نصت على جرائم محددة وواضحة ، لكن اتفاقية الأمم المتحدة توسعت في جوانب معينة فشملت الجرائم التقليدية المرتكبة بواسطة الانترنت على الرغم من انهما تشتركان في بعض الجرائم مثل هي تجريم الوصول غير المشروع لأنظمة المعلومات، الاعتراض غير المشروع للبيانات، والتدخل في الأنظمة والبيانات.

لكن ما يميز اتفاقية الأمم المتحدة انها تُعد الأولى عالمياً التي تتناول بشكل مفصل وشامل العنف الجنسي ضد الأطفال عبر الإنترنت، بما في ذلك "الاستدراج أو الاستمالة" لغرض جنسي ، كما تشمل بنوداً صريحة حول غسل العائدات الإجرامية الناتجة عن الجرائم السيبرانية

اما من حيث آليات التعاون الدولي نجد بان الاتفاقيتان تتشابهان بشكل كبير في الأدوات الإجرائية لضمان الملاحقة العابرة للحدود من خلال شبكة الـ 7/24 تلزم الاتفاقية الأممية الدول بإنشاء

¹ إسلام عبد ربه رمضان عبد ربه هديب، "المرجع السابق، ص 309-310

الفصل الثاني: الآليات القانونية والمؤسسية على المستويين الدولي والوطني لمكافحة الجريمة السيبرانية

جهة اتصال تعمل على مدار الساعة لتقديم مساعدة فورية في التحقيقات وجمع الأدلة الإلكترونية وتحديد أماكن المشتبه فيهم الأدلة الإلكترونية توفر الاتفاقيتان إطاراً لجمع الأدلة الرقمية، وتفتيش الأنظمة الحاسوبية، والأمر بتقديم معلومات المشتركين من مزودي الخدمة، ورغم ذلك قدمت اتفاقية بودابست فعالية وسرعة اليات ذات سرعة وفعالية غير ان اتفاقية الامم 2024 تتسم ببطء الاجراءات بالنظر الى الاجراءات التي تفرضها في اليات التعاون مراعاة لسيادة الدول .

وفضلا عن ذلك تعتبر مسألة السيادة وحقوق الإنسان من اهم النقاط فاذا كانت اتفاقية الأمم المتحدة تركز بشكل مكثف على مبدأ المساواة في السيادة وعدم التدخل في الشؤون الداخلية للدول، كما تؤكد على الحفاظ على حقوق الإنسان على الإنترنت وضمان المحاكمة العادلة للمتهمين و هذا بشكل عام دون ضمانات .

فان اتفاقية بودابست، تضع إطاراً يمنح السلطات صلاحيات لجمع الأدلة مع ضمان حماية الخصوصية ، خضوع الإجراءات لمبدأ التناسب، رقابة قضائية على جمع الأدلة احترام حقوق الإنسان والحريات الأساسية وهي مرتبطة بمعايير حقوق الانسان الاوربية .

اما من حيث حماية ودعم الضحايا أن اتفاقية الأمم المتحدة أولت اهتماماً خاصاً بدعم الضحايا، بما يشمل خدمات التعويض، استرداد الحقوق، وإزالة المحتوى غير القانوني، مع تقديم دعم نفسي وجسدي متخصص للأطفال ضحايا الاعتداء الجنسي.

واستخلاصا لما سبق نستطيع ان نقول ان الاتفاقيتين تشكلان إطارين قانونيين دوليين لمكافحة الجريمة السيبرانية ، غير أنهما تختلفان من حيث النطاق واليات التطبيق، فبينما تركز اتفاقية بودابست على توحيد التجريم ووضع قواعد دقيقة للجريمة السيبرانية مع اعتماد آليات سريعة وفعالة للتعاون لمكافحة هذه الجريمة ، مع ضمانات واضحة لاحترام حقوق الانسان ، تتميز اتفاقية الامم المتحدة 2024 وهي لا تزال في طور التبنّي بطابعها العالمي والسعي الى اشراك اكبر عدد من الدول ودعم الدول النامية والتزامها بمبدأ السيادة الوطنية في حين تعتمد اتفاقية الامم رؤية فضفاضة تثير اشكاليات تفسيرية ، خاصة في مجال حقوق الانسان في ظل عدم وجود ضمانات .

المطلب الثاني : الآليات المؤسسية الدولية لمكافحة الجريمة السيبرانية

الفرع الاول : جهود الأمم المتحدة :

بذلت الامم المتحدة جهوداً قيمة لمواجهة تحديات الجريمة السيبرانية من خلال دورها كإطار مرجعي دولي يهدف إلى تعزيز العمل المشترك والوعي بخطورة هذه الجرائم العابرة للحدود، وقد تجلت هذه الجهود في عقد سلسلة من المؤتمرات الدولية لمنع الجريمة وقد تعددت المؤتمرات التي نظمتها الأمم المتحدة لمكافحة الجريمة السيبرانية، حيث انبثقت عنها عدة مؤتمرات من أهمها:

1-المؤتمر السابع (ميلانو، 1985): كلف لجنة من الخبراء بدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الحاسب الآلي ، واعداد تقرير قصد عرضه على المؤتمر الثامن .

2- المؤتمر الثامن (هافانا، 1990): أقر معاهدات نموذجية لتسليم المجرمين وتبادل المساعدة الجنائية، وأكد على ضرورة تحديث القوانين الوطنية، ومصادرة الأصول غير المشروعة، ورفع الوعي لدى القضاة والأجهزة المعنية وقامت الجمعية الدولية بعقد المؤتمر الخامس عشر لقانون العقوبات في ريو دي جانيرو، البرازيلية سنة 1994¹

ولقد اقر العديد من التوصيات بشأن جرائم الكمبيوتر سواءا في الشق الموضوعي او في الشق الاجرائي حيث وضع قائمة بالحد الأدنى للأفعال التي يجب تجريمها، مثل الاحتيال المرتبط بالكمبيوتر، التزوير المعلوماتي، الإضرار بالبيانات، والدخول غير المصرح به وفي الشق الجزائي اصدر المؤتمر الكثير من الاجراءات.

3-المؤتمر التاسع (القاهرة، 1995): أوصى بوجوب حماية الإنسان في حياته الخاصة وملكيته الفكرية من مخاطر التكنولوجيا، وضرورة التنسيق الدولي لاتخاذ الإجراءات المناسبة

4-المؤتمر الثاني عشر (سلفادور، 2010): ناقش تطورات مكافحة الجريمة وأكد على بناء قدرات السلطات الوطنية لمنع وكشف الملاحقة الجنائية بكافة أشكالها.

5-المؤتمر الثالث عشر (الدوحة، 2015): ركز على استحداث أدوات وبرامج لتسهيل المكافحة، وبناء قدرات أجهزة إنفاذ القانون في التحري الرقمي، كما أوصى بدراسة إمكانية وضع اتفاقية دولية شاملة بشأن الجريمة السيبرانية.²

¹ عبد الله عبد الكريم عبد الله ، المرجع السابق، ص 107 الى 114

² عبد الله عبد الكريم عبد الله ، المرجع السابق ، ص من 107 الى 114

الفرع الثاني: جهود المنظمات الإقليمية

أخذت العديد من المنظمات الإقليمية على عاتقها مكافحة الجريمة السيبرانية ومنها منظمة التعاون الاقتصادي، مؤسسة الإنترنت للأسماء والأرقام المخصصة والمنظمة الدولية لتوحيد المقاييس، الإنترنت واليوروبول، وسنتناول في دراستنا منظمين جامعة الدول العربية والاتحاد الإفريقي.

أولاً : الجهود العربية لمكافحة الجريمة السيبرانية

تتمثل الجهود العربية في مواجهة الجرائم الإلكترونية ، في عدة مسارات تشريعية وتنظيمية تقودها جامعة الدول العربية والهيئات التابعة لها، ويمكن تلخيصها فيما يلي:

1-الاتفاقيات العربية الإقليمية:

حيث نجحت منظمة جامعة الدول العربية في إبرام عدد من الاتفاقيات و التي تعد جهداً متواضعاً في هذا المجال ومن أهمها :

- الاتفاقية العربية لحماية حقوق المؤلف (1981): تهدف إلى حماية المصنفات الأدبية والفنية والعلمية التي قد تكون هدفاً للجرائم الإلكترونية عند نشرها على الإنترنت. وألزمت الدول بإنشاء مؤسسات وطنية لحماية هذه الحقوق وتشكيل لجنة دائمة لمتابعة تنفيذها¹

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010): تعد من أبرز الجهود، حيث تهدف لتعزيز التعاون العربي لمكافحة الجرائم التي تهدد أمن المجتمعات. وتتضمن 43 مادة تشمل الأحكام الموضوعية التي تجرم أفعال مثل الاختراق، والاعتداء على سلامة البيانات، والتزوير، والاحتيال الإلكتروني، والإباحية، والجرائم المتعلقة بالإرهاب وغسل الأموال

أما الأحكام الإجرائية تنظم حقوق السلطات في جمع المعلومات، وتتبع المستخدمين، وضبط الأجهزة التقنية ، ومن خلال التعاون الدولي تنظيم تبادل المعلومات بين الدول الأعضاء لملاحقة الجناة.²

2- التشريعات والقوانين النموذجية منها

-القانون الجزائي العربي الموحد (1996) الذي اعتمد كقانون نموذجي وتضمن فصلاً خاصاً بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية و أقر حماية الحياة الخاصة من

¹ الفريجات، عماد حسين محمد. "الجهود العربية والإفريقية لمواجهة الجرائم الإلكترونية في الفترة 2010-2023".

مجلة ابن خلدون للدراسات والأبحاث، المجلد 03، العدد 05، مايو 2023، ص 195

² الفريجات، عماد حسين محمد. المرجع نفسه ، ص من 196 الى 198

خطر المعالجة الآلية للبيانات، ووضع عقوبات على الدخول غير المشروع للأنظمة، وعرقلة تشغيلها، وتزوير أو سرقة المعلومات .¹

- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لسنة 2003 الذي اعتمد من طرف وزراء العدل العرب في الدورة التاسعة عشر استنادا الى قرارها رقم 495 ، القانون مكون من 27 مادة صدر استكمالاً للجهود الرامية لسن قوانين موحدة تساعد الدول العربية في الحد من الجرائم الإلكترونية.²

ان القانون الاسترشادي من القوانين المتقدمة والفعالة في الوطن العربي لمكافحة جرائم شبكة المعلومات الدولية من بينها جريمة الاختيال ، حيث وضع هذا القانون القواعد الاساسية التي يتعين على المشرع العربي اللجوء اليها عند سن قانون وطني لمكافحة هذه الجريمة سواءا أكان القانون مستقلا لمكافحة هذه الجريمة المستحدثة ام كان تعديلا لقانون العقوبات المطبق في أي دولة من الدول العربية³ ولهذا يعتبر هذا القانون النموذجي المسودة التي استلهم منه المشرعين العرب قوانينه الوطنية ضمنهم المشرع الجزائري والمصري.

3 - الجهود المؤسسية والاستراتيجية :

تجلت الجهود العربية المؤسسية والاستراتيجية في الدور المحوري لجامعة الدول العربية، والذي برز بوضوح من خلال ميثاقها الداعي إلى التعاون الوثيق لصيانة سيادة الدول واستقلالها، وهو توجه ينسجم تماماً مع متطلبات مواجهة التهديدات السيبرانية التي قد تستهدف المؤسسات السيادية أو تهدف للتحريض ضد الأنظمة. وفي سياق متصل، أولت الأمانة العامة لمجلس وزراء الداخلية العرب اهتماماً بالغاً بوضع استراتيجية عربية شاملة لمكافحة هذه الجرائم، وهي الاستراتيجية التي شكلت الحجر الأساس الذي انبثقت عنه مختلف الاتفاقيات والقوانين العربية الموحدة في هذا المجال⁴.

¹ الفريحات، عماد حسين محمد. ، المرجع نفسه ، ص 199

² الفريحات، عماد حسين محمد. ، المرجع السابق ، ص 201

³ الفريحات، عماد حسين محمد. ، المرجع نفسه ص 205

⁴ الفريحات، عماد حسين محمد. المرجع نفسه ، ص 198-199

ثانيا: جهود الاتحاد الافريقي :

تتمثل جهود الاتحاد الأفريقي في مواجهة الجرائم الإلكترونية بشكل أساسي في اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي لعام 2014 تتألف الاتفاقية من اربعة فصول، وتهدف هذه الاتفاقية إلى وضع إطار قانوني وتنظيمي شامل لتعزيز الأمن السيبراني وحماية المعطيات الشخصية في القارة الأفريقية من خلال عدة اتجاهات وتدابير تتمثل فيما يلي :

- 1-التدابير والسياسات الوطنية لأمن الفضاء الإلكتروني بحيث ألزمت الاتفاقية الدول الأعضاء باتخاذ مجموعة من الإجراءات لتعزيز السيادة الرقمية والأمن الوطني¹
- 2- وضع سياسة و استراتيجية وطنية اين تلتزم كل دولة طرف بوضع سياسة وطنية لأمن الفضاء الإلكتروني تحدد المخاطر التي تواجه البنية التحتية الأساسية للمعلومات وكيفية تنفيذ الأهداف الأمنية.
- 3- الإصلاح التشريعي وتجريم الأفعال ويتجسد في التزام الدول باعتماد تدابير تشريعية لتجريم الأعمال الجنائية التي تمس سرية ونزاهة أنظمة تكنولوجيا المعلومات والبيانات
- 4-حماية البنية التحتية الحيوية من خلال تحديد القطاعات الحساسة للأمن الوطني والازدهار الاقتصادي واعتبارها بنية تحتية حيوية للمعلومات مع فرض عقوبات صارمة على الاعتداءات التي تستهدفها.
- 5- الحماية القانونية للبيانات الشخصية بحيث تضمنت الاتفاقية أحكاماً مفصلة لضمان خصوصية الأفراد وحقوقهم الرقمية بحيث أقرت الاتفاقية حق الأفراد في الاعتراض على معالجة بياناتهم لأسباب مشروعة، وحقهم في تصحيح أو حذف بياناتهم الشخصية.
- 6-التزامات معالجي البيانات: ألزمت المسؤولين عن معالجة البيانات بمبادئ السرية، واتخاذ احتياطات التأمين اللازمة لمنع تسريب البيانات أو إتلافها، والالتزام بمدد تخزين لا تتجاوز الغرض من الجمع².
- 7 -الجوانب التنظيمية والضبطية تلتزم الدول بإسناد مسؤوليات محددة لمؤسسات وطنية (قائمة أو مستحدثة) لتنفيذ جوانب الأمن السيبراني والتحقيقات الجنائية والنيابة العامة ، إنشاء آليات وطنية لمراقبة الفضاء الإلكتروني ورصد التهديدات

¹ الفريحات، عماد حسين محمد. المرجع السابق ، 208

²الفريحات، عماد حسين محمد. المرجع السابق ، ص208- 214

8- ثقافة الأمن السيبراني: تشجيع ثقافة الأمان الرقمي بين الحكومات والشركات والمجتمع المدني، ودمج مفاهيم الأمن عند تطوير الأنظمة والشبكات. بالاحص الشراكة بين القطاعين العام والخاص وذلك بتطوير نموذج لإشراك القطاع الخاص والمجتمع الأكاديمي في تعزيز الأمن السيبراني الوطني، و من خلال التعليم والتدريب الالتزام ببناء القدرات وتوفير التدريب المتخصص للمهنيين في مجال تكنولوجيا المعلومات لتمكينهم من مواجهة التهديدات الحديثة.

9- التعاون الدولي نظمت الاتفاقية في فصلها الثاني أحكاماً تتعلق بالتعاون الدولي بين الدول الأفريقية للحد من الجرائم العابرة للحدود التي تستخدم تكنولوجيا المعلومات والاتصالات¹

الفرع الثالث: المقارنة بين دور الأمم المتحدة وجهود المنظمات الإقليمية

إذا ما قارنا بين جهود هذه المنظمات التي لعبت أدوار لا يستهان بها في مجال مكافحة هذه الجريمة من حيث الشمولية والفعالية ومدى تأثيرها في القوانين الوطنية نجد انها تختلف بدرجات متفاوتة .

1- من حيث الشمولية:

فبالنسبة للاتحاد الأفريقي اتفاقية مالابو تُصنف الأكثر شمولية من الناحية التنظيمية؛ فهي لم تقتصر على الجانب الجنائي الردي، بل شملت أمن الفضاء الإلكتروني، وحماية البيانات ذات الطابع الشخصي، والمعاملات الإلكترونية في إطار واحد متكامل.

أما الأمم المتحدة تنسم بالشمولية العالمية، حيث تهدف إلى وضع حد أدنى من القواعد المشتركة التي تقبلها جميع الثقافات القانونية، مع التركيز على الجرائم ذات الصبغة الدولية مثل الإرهاب الإلكتروني والاتجار بالبشر.

أما جامعة الدول العربية شموليتها "تخصصية جنائية"؛ حيث ركزت بشكل مكثف على توصيف الجرائم الإلكترونية (الأحكام الموضوعية) والإجراءات القانونية لملاحقتها، لكنها كانت أقل توسعاً في جوانب حماية البيانات والخصوصية مقارنة بالنموذج الأفريقي.

2- من حيث الفعالية التطبيق والتعاون الدولي:

الأمم المتحدة هي الأكثر فعالية في تجاوز الحدود لقدرتها على توفير منصة للتعاون القضائي وتسليم المجرمين بين دول من قارات مختلفة، وهو ما تعجز عنه المنظمات الإقليمية في حال فرار المجرم إلى قارة أخرى.

أما عن جامعة الدول العربية فعاليتها "تشريعية استرشادية"؛ نجحت في توحيد لغة القانون الجنائي العربي، لكن فعاليتها الميدانية تصطدم أحياناً ببطء التنسيق الأمني والتقني بين الدول الأعضاء.

¹ الفريجات، عماد حسين محمد. المرجع السابق ، ص208- 214

في حين ان الاتحاد الأفريقي فعاليتها تكمن في "بناء القدرات"؛ حيث تلزم الاتفاقية الدول بإنشاء هياكل وطنية للرصد والاستجابة للطوارئ المعلوماتية، مما يرفع من جاهزية الدول الأفريقية تقنياً.

3- من حيث التأثير على القوانين الوطنية

إذا كانت جامعة الدول العربية: لها التأثير الأكبر والمباشر على القوانين العربية؛ حيث استلهمت معظم الدول العربية مثل الجزائر ومصر نصوص قوانينها الوطنية من "القانون العربي الاسترشادي" ومن نصوص الاتفاقية العربية لعام 2010، مما أدى لتقارب كبير في العقوبات المطبقة.

نجد ان الاتحاد الأفريقي دفع الدول الأعضاء نحو "الإصلاح الهيكلي"؛ فلم يكتفِ بتغيير النصوص القانونية، بل دفع نحو إصدار قوانين خاصة بحماية المعطيات الشخصية وإنشاء هيئات رقابية وطنية مستقلة.

بينما الأمم المتحدة تعمل كمحرك "للتحديث والنمذجة"؛ حيث تضغط تقاريرها وتوصياتها على الدول لتحديث قوانينها الوطنية بما يتوافق مع المعايير الدولية لحقوق الإنسان ومتطلبات العصر الرقمي. وفي الأخير نستخلص بأنه إذا كان الهدف هو الحماية المتكاملة أمن و بيانات و جريمة ، فإن آلية الاتحاد الأفريقي هي الأبرز وإذا كان الهدف هو الملاحقة الدولية العابرة للقارات، فإن الأمم المتحدة هي الأقوى. أما إذا كان الهدف هو توحيد الصياغة القانونية الجنائية في المنطقة، فإن جامعة الدول العربية كانت الأسبق والأكثر تأثيراً في المشرع العربي.

المطلب الثالث: أشكال التعاون الدولي في مكافحة الجريمة السيبرانية :

تعددت اشكال التعاون الدولي في مكافحة الجريمة السيبرانية لتشمل عدة جوانب قضائية وامنية وتقنية واتفاقية تهدف في مجملها لي محاصرة هذه الظاهرة العابرة للحدود الرقمية والجغرافية

الفرع الاول: التعاون القضائي

يُعد التعاون القضائي ركيزة أساسية في مواجهة الجرائم السيبرانية نظراً لطبيعتها العابرة للحدود والتي تجعل من الصعب على دولة بمفردها ملاحقة الجناة وتبرز اهم صور التعاون القضائي .

اولا- صور وآليات التعاون القضائي : يتخذ التعاون القضائي عدة صور إجرائية تضمن فاعلية الملاحقة الجنائية منها:

1- تبادل المعلومات والوثائق :وذلك من خلال تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أو أمنية أجنبية بخصوص جريمة معينة أو اتهامات موجهة لرعاياها.

2- تبادل السوابق القضائية للجنة للتعرف على ماضيهم الجنائي وتقرير الأحكام الخاصة بالعود أو وقف تنفيذ العقوبة.

3- تبادل نصوص التشريعات النافذة والبحوث القانونية والقضائية المتعلقة بالأنظمة القضائية

4- الإنابات القضائية الدولية تسمح هذه الآلية لسلطة قضائية في دولة ما بأن تطلب من سلطة قضائية في دولة أخرى القيام بإجراء من إجراءات التحقيق مثل سماع الشهود أو جمع الأدلة نيابة عنها أقر التشريع الجزائري في القانون رقم 04-09 إمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجرائم المعلوماتية في شكلها الإلكتروني.¹

5- تسليم المجرمين والمساعدة في المسائل الجنائية حيث دعت مؤتمرات الأمم المتحدة الدول إلى إدراج الجرائم المعلوماتية ضمن المعاهدات المتعلقة بتسليم المجرمين الاستجابة لطلبات المساعدة القضائية الدولية لتبادل المعلومات في إطار الاتفاقيات الدولية وبناءً على مبدأ المعاملة بالمثل.²

ثانياً: الإطار القانوني والاتفاقيات المنظمة

يعتمد التعاون القضائي على أسس قانونية متينة تشمل اتفاقية بودابست التي نصت صراحة في المادة 23 على وجوب توافر التعاون الدولي وتخفيف العوائق لتبادل المعلومات والأدلة واتفاقية الرياض العربية للتعاون القضائي التي أكدت على التبادل المنتظم للمعلومات المتعلقة بالتنظيم القضائي والتشريعات واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة التي شددت في مادتها 18 على تقديم أكبر قدر ممكن من المساعدة القانونية المتبادلة³

الفرع الثاني : التعاون الامني

تعتبر مكافحة الجريمة السيبرانية من التحديات التي تتطلب تنسيقاً أمنياً رفيع المستوى، نظراً لسرعة تنفيذ هذه الجرائم وقدرة الجناة على إخفاء آثارهم الرقمية عبر خوادم موزعة في دول مختلفة.

فيما يلي توضيح لآليات وأشكال التعاون الأمني في هذا المجال

¹ فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية مجلة البحوث في الحقوق والعلوم السياسية المجلد 08 العدد 01 جامعة البليدة 02 الجزائر 2022 ص 440-441

² فريد ناشف المرجع نفسه ، ص 442

³ فريد ناشف المرجع نفسه ، ص 442

اولا : مفهوم التعاون الأمني السيبراني :يتمثل التعاون الأمني في التنسيق بين الأجهزة الشرطية والمؤسسات الأمنية الوطنية والدولية لتبادل المعلومات الاستخباراتية والتقنية حول التهديدات الرقمية بهدف الوقاية من الجرائم أو ضبط مرتكبيها

ثانيا : أبرز آليات التعاون الأمني

1-تبادل المعلومات والبيانات الأمنية حيث يعد التبادل الفوري للمعلومات حول الهجمات السيبرانية والثغرات المكتشفة من أهم صور التعاون ، يتضمن ذلك مشاركة عناوين البروتوكولات الرقمية المشبوهة والبرمجيات الخبيثة المستخدمة في الهجمات

2- الملاحقة والتعقب عبر الحدود من خلال تنسيق الجهود لتعقب مصدر الهجوم الرقمي الذي قد ينطلق من دولة ما ويستهدف ضحايا في دولة أخرى ، العمل المشترك على تحديد الهوية الحقيقية للمجرمين الذين يستخدمون تقنيات التشفير أو التمويه المساعدة التقنية والتدريب تبادل الخبرات بين الدول المتقدمة تكنولوجياً والدول النامية لتطوير قدرات أجهزة مكافحة الجريمة المعلوماتية تنظيم دورات تدريبية مشتركة لضباط الشرطة والمحققين الجنائيين على أحدث تقنيات التحقيق الرقمي.¹

ثالثا: المنظمات الدولية الفاعلة في التعاون الأمني

1-المنظمة الدولية للشرطة الجنائية الإنتربول

تعد المنظمة الدولية للشرطة الجنائية الإنتربول كياناً دولياً محورياً يهدف إلى تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء لمكافحة الجرائم العابرة للحدود. وتعمل المنظمة على تجميع وتبادل البيانات والمعلومات المتعلقة بالمجرمين والأنشطة الإجرامية عبر مكاتبها المركزية الوطنية. وفي مجال الجرائم الإلكترونية، استحدثت وحدة خاصة عام 2004 لمكافحة جرائم التكنولوجيا ووضعت استراتيجيات لمواجهةها بالتعاون مع الدول الكبرى. كما تساهم بفاعلية في تعقب المجرمين الفارين والمساعدة في ضبطهم، وتزويد الدول بكتيبات إرشادية وتدريبات متخصصة للتحقيق في الجرائم المعلوماتية. وقد حققت إنجازات ملموسة في تفكيك شبكات إجرامية دولية، مثل ملاحقة ناشري الفيروسات وشبكات الاستغلال الجنسي للأطفال عبر الإنترنت².

¹ فريد ناشف، المرجع السابق ، ص 437، 439

² فريد ناشف، المرجع السابق ، ص 438

2- المنظمة الأوروبية للشرطة اليوروبول

تعد الشرطة الأوروبية (اليوروبول) التي أنشئت عام 1991 في لوكسمبورغ بمثابة همزة وصل حيوية بين أجهزة الشرطة الوطنية في الدول الأطراف. تهدف المنظمة إلى ملاحقة مرتكبي الجرائم العابرة للحدود، ولا سيما الجرائم المتعلقة بشبكة الإنترنت. وتعمل اليوروبول بالتنسيق مع جهات دولية أخرى مثل الإنتربول والمباحث الفيدرالية الأمريكية لتفكيك الشبكات الإجرامية. ومن أبرز نجاحاتها التعاون في ضبط المواقع التي تنتشر مواد غير قانونية وصور إباحية للأطفال. كما تساهم في تبادل المعلومات الاستخباراتية والخبرات التقنية لتعزيز الأمن القضائي والجنائي الدولي¹.

3-المبادرات والشبكات الإقليمية

"فقد انشا المكتب العربي للشرطة الجنائية من قبل مجلس وزراء الداخلية والعدل العرب سنة 2010 بهدف تامين وتنمية التعاون بين اجهزة الشرطة في الدول الاعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والانظمة المعمول بها في كل دولة بالاضافة الى تقديم المعونة في مجال دعم وتطوير اجهزة الشرطة في الدول الأعضاء"²

الفرع الثالث: اشكاليات التعاون الدولي

تعد إشكاليات التعاون الدولي في مكافحة الجريمة السيبرانية من أعقد العقبات التي تواجه أجهزة إنفاذ القانون، حيث تتصادم فيها السيادة الوطنية مع الطبيعة الرقمية العابرة للحدود ، فيما يلي عرض لأبرز هذه الإشكاليات وفقاً للدراسات القانونية والأمنية

1-تباين الأنظمة القانونية:تختلف الدول في تعريف الجريمة السيبرانية وتصنيف الأفعال المجرمة

يؤدي غياب مبدأ ازدواجية التجريم إلى رفض بعض الدول التعاون إذا كان الفعل المرتكب لا يشكل جريمة في قانونها الوطني.³

2- النزاع حول الولاية القضائية (مشكلة الاختصاص) في الفضاء الإلكتروني حيث يصعب

تحديد مكان وقوع الجريمة بدقة⁴

¹ فريد ناشف ،المرجع السابق ص 439

² فريد ناشف، المرجع السابق، ص 439

³ قطاف سليمان ومن معه ، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية ، مجلة البحوث القانونية والاقتصادية المجلد

05 العدد 02 جامعة الاغواط 2022 ص 82

⁴ قطاف سليمان ومن معه ، المرجع السابق ص 82

3-بطء الإجراءات التقليدية الاعتماد على اتفاقيات المساعدة القانونية المتبادلة التقليدية التي تنسم

بالبطء الشديد لا يتناسب مع سرعة الجريمة الإلكترونية التي قد تُنفذ وتُحمى آثارها في ثوانٍ معدودة

4-الإشكاليات التقنية والفنية:منها تحدي جمع الأدلة الرقمية تتميز الأدلة الرقمية بكونها غير

ملموسة وسهلة التدمير أو التعديل وصعوبة تتبع الجناة الذين يستخدمون تقنيات التشفير المعقدة أو الشبكات المظلمة لإخفاء هوياتهم ومواقعهم

زد على ذلك الفجوة الرقمية بين الدول التفاوت الكبير في الإمكانيات التقنية والمادية بين الدول المتقدمة والنامية يعيق عمليات الملاحقة المشتركة نقص الخبرات البشرية المتخصصة في التحقيق الرقمي لدى الكثير من الأجهزة الأمنية

5- إشكاليات تتعلق بحماية البيانات والخصوصية : ان التصادم مع قوانين حماية الخصوصية تفرض بعض الدول قيوداً صارمة على نقل البيانات الشخصية لمواطنيها إلى دول أخرى مما يعيق تبادل المعلومات الأمنية والخوف من إساءة استخدام المعلومات المتبادلة في أغراض غير الملاحقة الجنائية ضف الى ذلك سرية البيانات لدى الشركات الخاصة حيث تواجه الدول صعوبات في إلزام شركات تكنولوجيا المعلومات ومزودي خدمة الإنترنت بتقديم البيانات المطلوبة للتحقيق دون إجراءات قضائية معقدة

6- الإشكاليات السياسية :غياب الثقة المتبادلة و التوترات السياسية بين بعض الدول تمنع التنسيق الأمني والسيبراني الفعال. عدم انضمام كافة الدول إلى اتفاقيات دولية موحدة مثل اتفاقية بودابست مما يخلق ملا ذات آمنة للمجرمين السيبرانيين.

7- اشكالية التعاون الدولي و السيادة الرقمية :حيث يبرز التوتر بين التعاون الدولي والسيادة الرقمية كأحد أهم التحديات المعاصرة، حيث تسعى الدول من جهة إلى بسط سيطرتها وحماية أمنها القومي، بينما يفرض الفضاء الرقمي بطبيعته العابرة للحدود ضرورة التعاون لمواجهة التهديدات ، وتعتبر الجرائم الماسة بالسيادة الرقمية جرائم عابرة للحدود، مما يجعل أي إجراء انفرادي من قبل الدولة غير كافٍ، ويستلزم رداً دولياً سريعاً في إطار قانوني.بينما تقوم السيادة الوطنية على بسط السلطة على إقليم محدد، فإن المعلومات في الفضاء الرقمي تنتقل ببسر تام بين الدول، مما يجعل الأمن القومي عرضة لتهديدات غير تقليدية تتجاوز الحدود الجغرافية.

المبحث الثاني: آليات مواجهة الجريمة السيبرانية على المستوى الوطني

(دراسة مقارنة بين التشريع الجزائري والتشريع المصري)

يشكل التصدي للجريمة السيبرانية تحديا كبيرا للمشرعين الجزائري والمصري في ظل وجود منظومة عقابية تقليدية تجاوزتها هذه الجريمة المستحدثة التي تقع في فضاءات رقمية افتراضية ، فقد سارعت الجزائر ومصر الى تبني استراتيجيات قانونية تهدف الى مواجهة هذه الجريمة ، سواءا من حيث القواعد الموضوعية او الاجرائية او على مستوى المؤسسات القضائية والاجهزة الرقابية المستحدثة .

المطلب الاول : الآليات القانونية الوطنية لمكافحة الجريمة السيبرانية

حاول المشرع الجزائري والمصري التصدي للجريمة السيبرانية نظرا لخطورتها على الافراد والمؤسسات الوطنية في ظل فراغ تشريعي يغطي هذا النوع من الاجرام الالكتروني المستحدث اين اضطر إلى إيجاد حلول قانونية وذلك بتعديل التشريعات العقابية والاجرائية الجزائية ومن استحداث قوانين خاصة بالجريمة السيبرانية الناجمة عن المعاملات الإلكترونية وسنحاول معالجة كيف تصدى المشرع الجزائري والمصري لهذه الجريمة .

الفرع الاول: مكافحة الجريمة السيبرانية في التشريع الجزائري:

شهدت الجزائر ارتفاع محسوسا و متزايدا في الجريمة السيبرانية في السنوات الاخيرة سواءا على الافراد او المؤسسات وعلى البنى التحتية والامن القومي وفي ظل وجود قوانين تقليدية لا تستوعب هذه الجريمة سعت الجزائر الى مكافحة هذه الجريمة بالياتها التشريعية فاستحدثت المشرع ترسانة قانونية من اجل الردع العقابي .

اولا : تعريف الجريمة الإلكترونية في التشريع الجزائري

اعتمد المشرع الجزائري تسميات وتعريف محددة للجريمة المرتبطة بالتكنولوجيا عبر مراحل تشريعية" جرائم المساس بأنظمة المعالجة الآلية للمعطيات هو المصطلح الأول الذي استعمله المشرع بموجب القانون رقم 04/ 15 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات حيث استحدثت القسم السابع مكرر لتجريم الأفعال التي تستهدف الأنظمة المعلوماتية.¹

¹ مهداوي حنان، "التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري"، مجلة الفكر القانوني والسياسي، جامعة محمد لمين دباغين - سطيف 2، المجلد 06، العدد 02، 2022، ص 1061.

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هذا هو التعريف الأكثر شمولاً الذي ورد في المادة 02 من القانون رقم 04/ 09 حيث عرفها المشرع بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

سعى المشرع الجزائري إلى مواكبة التطورات التي شهدتها التشريعات المقارنة في مجال مكافحة الجريمة الإلكترونية، وذلك من خلال مراجعة وتكييف القوانين التقليدية لتتلاءم مع خصوصية هذا النوع المستحدث من الإجرام. غير أن هذه الجهود، على أهميتها، جاءت في مرحلة لاحقة مقارنة ببعض التجارب التشريعية الرائدة، الأمر الذي يطرح تساؤلات حول مدى قدرتها على الاستجابة الفعالة للتحديات المتسارعة التي تفرضها البيئة الرقمية.¹

ثانيا : مكافحة الجريمة الإلكترونية من خلال تعديل قانون العقوبات

تصدى المشرع الجزائري للجريمة الإلكترونية من خلال دمج نصوص عقابية صريحة في قانون العقوبات، تهدف إلى حماية أنظمة المعالجة الآلية للمعطيات وضمان سلامة الفضاء الرقمي. ويمكن تلخيص أبرز ملامح هذه المكافحة وفقاً للتشريع الجزائري فيما يلي:

استحدث المشرع الجزائري القسم السابع مكرر في قانون العقوبات (بموجب القانون 04-15) تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، والذي تضمن تجريماً للأفعال التالية:

صنف المشرع الجزائري الجرائم المعلوماتية بناءً على دور النظام المعلوماتي فيها إلى نوعين رئيسيين وهما الجرائم المرتكبة بواسطة النظام المعلوماتي، والجرائم الواقعة على النظام المعلوماتي فيما يلي تفصيل لهذه الأنواع²

أولاً: الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي: وهي الجرائم التي يُستخدم فيها الحاسب الآلي كأداة لتنفيذ الفعل الإجرامي، وتشمل:

¹ مهداوي حنان، المرجع السابق، ص 1061.

² خلدون عيشة، "الجريمة المعلوماتية في القانون الدولي والجزائري"، مجلة القانون والعلوم السياسية، جامعة زيان عاشور

بالجلفة، المجلد 09، العدد 01، الجزائر، 2023، ص 139، 140

1- الجرائم الواقعة على الأشخاص: وتشمل الاعتداء على خصوصية الحياة الخاصة عبر اختراق الحاسب الآلي للحصول على معلومات شخصية وسرية مخزنة، واستعمالها في التهديد والابتزاز أو عرضها للغير دون إذن، و الاعتداء على حقوق الملكية الفكرية وهي المساس بالحقوق المعنوية والمالية للمؤلفين أو المبدعين من خلال اختراق معلوماتهم وتخزينها واستخدامها دون إذن، بما يشمل براءات الاختراع والمصنفات الأدبية والفنية

2- الجرائم الواقعة على النظم المعلوماتية الأخرى: تشمل الدخول إلى مراكز المعالجة المعلوماتية للاستيلاء على المعلومات، أو إساءة استعمال البطاقات الائتمانية بطرق غير مشروعة مثل استخدامها بعد انتهاء صلاحيتها أو استخدام بطاقة مسروقة.

3- الجرائم الواقعة على الأسرار: استخدام النظام المعلوماتي للحصول على أسرار الدولة (عسكرية أو اقتصادية) بغرض التجسس، أو الحصول على أسرار المؤسسات المهنية ونشرها لتحقيق مكاسب مالية أو ممارسة الضغط عليها

ثانيا- الجرائم المعلوماتية الواقعة على النظام المعلوماتي: هذه الجرائم تستهدف النظام المعلوماتي بحد ذاته، وقد تناولها المشرع الجزائري في قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات وهي " وتنتمثل :

- 1- الدخول أو البقاء عن طريق الغش (غير المشروع) في نظام المعالجة الآلية للمعطيات
- 2- تخريب نظام المعالجة الآلية للمعطيات أو الاعتداء على سيره.
- 3- المساس بسلامة المعطيات، وذلك من خلال الاعتداء العمدي عليها بالإدخال، أو الإزالة، أو المحو، أو التعديل.
- 4- تجميع وتوفير المعطيات المتحصل عليها بطرق غير مشروعة للغير، بقصد ارتكاب جرائم ماسة بأنظمة المعالجة.
- 5- استعمال والتصرف في المعطيات المتحصل عليها من جرائم المساس بأنظمة المعالجة الآلية
- 6- المشاركة في مجموعة أو اتفاق مسبق بغرض ارتكاب هذه الجرائم
- 7- المحاولة الشروع في ارتكاب أي من الجرائم المذكورة أعلاه¹

¹ خلدون عيشة، المرجع السابق ، ص 139، 140

كما أشار التشريع الجزائري إلى تشديد العقوبات في حال استهدفت هذه الجرائم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام. وبموجب القانون رقم 09-04، عُرِّفت هذه الجرائم بأنها كل مساس بأنظمة المعالجة الآلية للمعطيات أو أي جريمة أخرى تُرتكب أو يُسهل ارتكابها عبر منظومة معلوماتية أو نظام للاتصالات الإلكترونية .

التعديلات والإضافات الهامة

تعديل سنة 2016 (القانون 16-02): أدخل المشرع تعديلاً جوهرياً بإضافة المادة 394 مكرر 8 التي شددت العقوبة على مقدمي خدمات الإنترنت في حال عدم تدخلهم الفوري لسحب أو تخزين المحتويات الإجرامية أو منع الدخول إليها، وتصل العقوبة إلى الحبس 3 سنوات وغرامة 10.000.000 دج .

القانون الخاص (09-04): جاء مكملاً لقانون العقوبات، حيث وضع القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، معرّفاً هذه الجرائم بأنها كل ما يمس أنظمة المعالجة الآلية المحددة في قانون العقوبات أو أي جريمة يسهل ارتكابها عبر نظام معلوماتي¹.

ثالثاً - التدابير الإجرائية لمكافحة الجريمة السيبرانية

نظم المشرع الجزائري مكافحة الجريمة الإلكترونية من خلال قانون الإجراءات الجزائية عبر إقرار قواعد إجرائية تتماشى مع الطبيعة التقنية لهذه الجرائم وذلك من خلال ما يلي:

- تمديد الاختصاص المحلي: نص المشرع في المادة 37 من قانون الإجراءات الجزائية على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية.

- إجراءات التفتيش والمعاينة: أقر المشرع التفتيش المنصب على المنظومات المعلوماتية في المادة 45 الفقرة 7 معتبراً أنه يختلف عن التفتيش التقليدي من حيث الشروط الشكلية والموضوعية غير أن المشرع الجزائري أحاط هذا النوع من التفتيش بقواعد صارمة حيث لا تطبق عليه الأحكام الواردة في المادة 44 المتعلقة بالقواعد الإجرائية العامة إذا تعلق الأمر بجرائم إلكترونية. يسمح بالدخول لغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وإلى المعطيات المخزنة فيها².

¹ مهداوي حنان، "المرجع نفسه"، ص 1068

² مهداوي حنان، المرجع نفسه، ص 1068، 1069

-اعتراض المراسلات والتقاط الصور: بموجب المادة 65 مكرر 5 يُسمح لسلطات التحقيق والاستدلال باعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور يتم اللجوء إلى هذه الإجراءات للضرورة القصوى في التحري عن الجرائم المتلبس بها أو الكشف عن ملابسات الجريمة الإلكترونية مع الاستعانة بكافة الترتيبات التقنية اللازمة.

- توقيف النظر وحجز المعطيات: نصت المادة 51 الفقرة 6 على إجراء توقيف النظر في جرائم المساس بأنظمة المعالجة الآلية للمعطيات عند اكتشاف معطيات مفيدة أثناء التفتيش يتم نسخها على دعامة تخزين إلكترونية وتوضع في أحرار وفق القواعد المقررة في قانون الإجراءات الجزائية في حال استحالة الحجز تقنياً تُتخذ تدابير تقنية لمنع الوصول إلى تلك المعطيات.

- مراقبة الاتصالات الإلكترونية: تتم المراقبة الإلكترونية للوقاية من جرائم الإرهاب التخريب الجرائم الماسة بأمن الدولة أو عند وجود احتمال اعتداء يهدد النظام العام أو الاقتصاد الوطني اشترط المشرع عدم إجراء عمليات المراقبة إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة.¹

"وفي إطار مواعمة القواعد الإجرائية مع الخصوصية التقنية للجريمة السيبرانية، ذهب المشرع الجزائري نحو تبني تدابير استثنائية تخرج عن القواعد العامة المألوفة في قانون الإجراءات الجزائية. وفي هذا الصدد، يؤكد الأستاذ جمال خفيف أن هذه الجرائم باتت تُصنف ضمن الجرائم الخطيرة التي تطلبت معاملة إجرائية خاصة؛ لاسيما فيما يتعلق بالاختصاص القضائي، حيث لم يعد القاضي مقيداً بحدود إقليمية ضيقة، بل امتد اختصاصه ليشمل النطاق الوطني لمواجهة الطبيعة العابرة للحدود لهذه الجرائم"². كما يرى الأستاذ خفيف أن سرعة تبدد الدليل الرقمي وسهولة إتلافه فرضت على المشرع تجاوز القيود الزمنية التقليدية للتفتيش (المحددة قانوناً بين الخامسة صباحاً والثامنة مساءً)، وإباحة التفتيش في أي وقت لضمان فعالية ضبط الأدلة.³

¹ مهداوي حنان، المرجع السابق ، ص 1068، 1069

² جمال خفيف، "القانوني جمال خفيف: توقيع الجزائر على معاهدة مكافحة الجريمة السيبرانية خطوة إستراتيجية"، حوار ملتيميديا، الإذاعة الجزائرية، <http://news.radioalgerie.dz> بتاريخ: 2025/11/09 تاريخ الاطلاع :

2026/05/03 على الساعة: 8:00

³ جمال خفيف المرجع نفسه

ثالثا: مكافحة الجريمة الإلكترونية من خلال استحداث قوانين خاصة

1- القانون 04-09

يعد القانون 04-09 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في الجزائر الركيزة الأساسية للمنظومة القانونية المتخصصة في هذا المجال وتتم مكافحة هذه الجرائم من خلال هذا القانون وفقاً للمحاور التالية:

أ- **تحديد مفهوم الجريمة الإلكترونية ونطاقها:** عرف القانون 04-09 هذه الجرائم في المادة 02 منه بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية مما يوسع نطاق تطبيق القانون ليشمل مختلف الأفعال الإجرامية الرقمية¹

ب- **تدابير مراقبة الاتصالات الإلكترونية:** أجاز القانون اللجوء إلى المراقبة الإلكترونية في حالات محددة المادة 04 وهي الوقاية من جرائم الإرهاب التخريب أو الجرائم الماسة بأمن الدولة وعند وجود احتمال اعتداء على منظومة معلوماتية يهدد النظام العام الدفاع الوطني أو الاقتصاد ولمقتضيات التحريات والتحقيقات القضائية أو في إطار المساعدة القضائية الدولية ولا تجوز هذه العمليات إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة.²

ج- **القواعد الإجرائية الخاصة التفتيش والحجز:** استحدث القانون إجراءات تفتيش تتناسب مع الطبيعة التقنية للجريمة المواد 05 إلى 09 حيث يسمح بالدخول إلى المنظومة المعلوماتية أو جزء منها وحتى منظومات التخزين عن بعد ويمكن للسلطات تسخير أي شخص لديه دراية تقنية بالمنظومة محل البحث لتسهيل مهمة التفتيش وعند اكتشاف معطيات مفيدة يتم نسخها على دعامة تخزين إلكترونية وحجزها وفق قواعد قانون الإجراءات الجزائية

التزامات مقدمي الخدمات.³ يفرض القانون على مقدمي خدمات الإنترنت التزامات محددة للمساهمة في مكافحة بالتعاون مع السلطات القضائية في الكشف عن الجرائم وقد شدد قانون العقوبات

¹ مهداوي حنان، "المرجع السابق"، ص 1069

² مهداوي حنان، "المرجع السابق"، ص 1069

³ مهداوي حنان، "المرجع السابق"، ص 1070

بتعديل 2016 المتماشى مع قانون 04-09 العقوبات على مقدمي الخدمات في حال عدم تدخلهم الفوري لسحب أو تخزين المحتويات الإجرامية أو منع الوصول إليها.¹

د-إنشاء الهيئة الوطنية للوقاية والمكافحة: نص القانون على استحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهي هيئة متخصصة تتولى تنسيق الجهود الوطنية لمواجهة هذه الظاهرة

ج- التعاون الدولي :نظم القانون قواعد التعاون والمساعدة القضائية الدولية معترفاً بأن هذه الجرائم غالباً ما تكون عابرة للحدود حيث يتم طلب المساعدة من السلطات الأجنبية إذا كانت المعطيات مخزنة خارج الإقليم الوطني.²

2-المرسوم الرئاسي : 07/26 المؤرخ في 7 جانفي 2026

الذي يقضي بإنشاء هيكل خاص داخل كل مؤسسة أو إدارة أو هيئة عمومية مكلف بضمان امن الانظمة المعلوماتية وحماية المعطيات الشخصية للجزائريين .

✓ الهيكل ملحق بالمسؤول الأول ويضمن الفصل بين الإدارة التقنية ومهام الحماية.

✓ مسؤوليات الهيكل تشمل إعداد سياسة أمن المعلومات وإدارة المخاطر السيبرانية.

✓ تنسيق مع الجهات المختصة والإبلاغ عن الحوادث السيبرانية.

✓ الامتثال للتشريعات المتعلقة بحماية البيانات والتوعية المستمرة للمستخدمين.

يعكس صدور المرسوم الرئاسي 07-24 المؤرخ في 7 جانفي 2024 إرادة الدولة الجزائرية في تعزيز سيادتها الرقمية وتحسين أمنها القومي ضد التهديدات السيبرانية المتزايدة، حيث يهدف إلى إيجاد إطار قانوني ومؤسسي متكامل ينسق الجهود بين مختلف القطاعات لمواجهة الجرائم المعلوماتية العابرة للحدود. وبإدراك هذا التوجه على سعي المشرع للموازنة بين مقتضيات الرقابة الأمنية الضرورية لحماية البنى التحتية الحساسة وبين ضمان الحقوق والحريات الرقمية، بالتوازي مع تحيين المنظومة الوطنية لتتماشى مع الاتفاقيات الدولية الحديثة، مما يؤسس لبيئة رقمية آمنة تدعم التحول التكنولوجي والاقتصادي في البلاد.³

¹ مهداوي حنان، " المرجع السابق، ص1070

² مهداوي حنان، "المرجع السابق ، ص، 1072

³ انظر الجريدة الرسمية العدد 04 بتاريخ : 18 جانفي سنة 2026 م

رابعاً : التعاون الدولي والعربي: عمل المشرع الجزائري على تعزيز التعاون العربي والدولي لمواجهة الجرائم الإلكترونية من خلال تبني مجموعة من الاتفاقيات والآليات القانونية، وذلك على النحو التالي:

حيث انضمت الجزائر اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية ولعبت دوراً قيادياً في صياغة هذه الاتفاقية حيث ترأست اللجنة المتخصصة المكلفة بإعداد الاتفاقية تمت مراسم التوقيع في العاصمة الفيتنامية هانوي بتاريخ 25 أكتوبر 2025، وذلك عقب اعتمادها في نهاية 2024، لتكون الجزائر ضمن أول مجموعة من الدول الموقعة التي شملت 64 دولة وهيئة.

وتهدف الجزائر من خلال هذا الانضمام الى تعزيز المنظومة القانونية و التعاون القضائي من خلال تسهيل تبادل الأدلة الإلكترونية العابرة للحدود، وتسليم المجرمين بوضع إطار قانوني واضح لملاحقة مرتكبي الجرائم المعلوماتية، كذلك بناء القدرات و الاستفادة من المساعدة التقنية و التدريب الذي تقدمه الاتفاقية للدول الأعضاء .

كما انضمت الجزائر إلى عدة اتفاقيات دولية تهدف إلى توحيد الجهود في مكافحة الإجرام الإلكتروني وحماية الحقوق الرقمية، ومن أبرزها:

1- اتفاقية حماية حقوق المؤلف: تمت المصادقة عليها في باريس عام 1971، وانضمت إليها الجزائر بموجب مرسوم رئاسي في عام 2003 .

2- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: اعتمدها الجمعية العامة في عام 2000، وصادقت عليها الجزائر بتحفظ في عام 2002 .

3- اتفاق الشراكة الأورو متوسطي: المبرم في عام 2002 بين الاتحاد الأوروبي والجزائر، حيث تضمن توصيات لحماية البيانات ذات الصبغة الشخصية وتأمين تدفق المعلومات .

4- الاتفاقيات الثنائية: أبرمت الجزائر اتفاقية مع فرنسا لتعزيز التعاون في مجال الأمن ومكافحة "الاحتيالات" المرتبطة بتكنولوجيات الإعلام والاتصال الجديدة .

كما شهد المجال العربي جهوداً تشريعية استرشادية واتفاقيات ملزمة، منها:

5- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات: اعتمدته جامعة الدول العربية في عام 2003 كمنهج استرشادي للدول الأعضاء عند صياغة قوانينها الوطنية. وقد تضمن تجريم أفعال مثل الدخول غير المصرح به، التزوير المعلوماتي، والجرائم المخلة بالآداب عبر الشبكة .

6--الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية: صادقت عليها الجزائر لتعزيز التعاون الأمني والقضائي مع الدول العربية.¹

الفرع الثالث : مكافحة الجريمة السيبرانية في التشريع المصري

تناول التشريع المصري مكافحة جرائم تقنية المعلومات من خلال القانون رقم 175 لسنة 2018 الذي يتألف من 45 مادة تنظم الجوانب التعريفية والإجرائية والعقابية يتضمن هذا القانون أبواباً وفصولاً توضح التزامات مقدم الخدمة ونطاق تطبيق القانون من حيث المكان والتعاون الدولي بالإضافة إلى الأحكام والقواعد الإجرائية لمأموري الضبط القضائي وتعيين الخبراء وحجية الأدلة الرقمية في الإثبات الجنائي.²

يحدد القانون العقوبات المقررة لمجموعة واسعة من الجرائم مثل الانتفاع بدون حق بخدمات الاتصالات والدخول غير المشروع وتجاوز حدود الحق في الدخول والاعتراض غير المشروع والاعتداء على سلامة البيانات والنظم المعلوماتية كما يجرم التشريع المصري الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة والاعتداء على الأنظمة المعلوماتية التابعة للدولة وسلامة الشبكة المعلوماتية والاعتداء على بطاقات البنوك وأدوات الدفع الإلكتروني واصطناع المواقع والاعتداء على حرمة الحياة الخاصة يمتد نطاق تطبيق هذا القانون ليشمل الجرائم المرتكبة خارج البلاد إذا وقعت على متن وسيلة نقل مسجلة في مصر أو تحمل علمها أو كان أحد المجني عليهم مصرياً أو إذا تم الإعداد للجريمة أو الإشراف عليها أو تمويلها داخل الدولة.³

يقرر القانون المسؤولية الجنائية للشخص الاعتباري في حال ارتكاب الجريمة باسمه أو لحسابه وفق المادة 36 حيث يعاقب المسؤول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو تسهيلها وقد تصل العقوبات إلى إيقاف التراخيص أو حل الشخص الاعتباري ونشر الحكم في جريدتين يوميتين واسعتي الانتشار⁴

¹ عبو غفيف، "الأليات القانونية في الجزائر وتطورها في مكافحة الجريمة الإلكترونية"، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس مستغانم، المجلد 09، العدد 01، جوان 2024، ص 24.

² علوي علي احمد الشارفي ، المرجع السابق، ص 140

³ علوي علي احمد الشارفي ، المرجع السابق، ص 140-141

⁴ علوي علي احمد الشارفي ، المرجع السابق، ص 142

اولا: الأطر الاستراتيجية والرؤى المستقبلية: تمثل هذه الأطر خارطة الطريق التي تحدد توجهات الدولة المصرية في الفضاء الرقمي حيث تبنت عدة استراتيجيات منها :

الاستراتيجية الوطنية للأمن السيبراني 2017-2021 لم تكن مجرد خطة تقنية، بل ركزت على تطوير إطار تشريعي ملائم، وبناء منظومة وطنية لحماية البنية التحتية للاتصالات، وإعداد الكوادر البشرية المتخصصة.

رؤية مصر 2030 تضع الأمن السيبراني كركيزة أساسية لتحقيق الاستقرار الاجتماعي والاقتصادي تهدف الرؤية إلى ضمان استجابة سريعة للآزمات السيبرانية وتحقيق التكامل بين مختلف قطاعات الدولة محليا¹ استراتيجية وزارة الاتصالات 2020 تركز على ثلاثة أهداف رئيسية هي الانتقال الكامل إلى المجتمع الرقمي، تحويل مصر إلى قطب رقمي عالمي، وتعزيز صناعة التكنولوجيا محليا² اما استراتيجية مصر 2022-2026 وهي الامتداد الأحدث الذي يسعى لمواكبة التكنولوجيات الناشئة ودعم جهود بناء مصر الرقمية لمواجهة التهديدات العالمية المتزايدة³

ثانيا :التشريعات والآليات القانونية :انتقلت مصر من مرحلة الفراغ التشريعي إلى مرحلة الحماية الدستورية والقانونية الصارمة

المكانة الدستورية المادة 31 يُعد الدستور المصري الصادر عام 2014 من الدساتير القليلة التي نصت صراحة على أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، مما أعطى حماية السيادة الرقمية صبغة دستورية ملزمة.

1- قوانين الجرائم السيبرانية وتقنية المعلومات

تهدف هذه القوانين إلى وضع تعريفات دقيقة للأفعال الإجرامية الرقمية مثل الاختراق، الاحتيال، أو الاعتداء على البيانات وتحديد العقوبات الرادعة لها

2- القوانين المكملة: قانون التوقيع الإلكتروني 15 لعام 2004 يمنح المعاملات الإلكترونية حجية قانونية، مما يدعم التجارة الرقمية والخدمات الحكومية قانون الاتصالات 10 لعام 2003 ينظم البنية التحتية ويحدد ضوابط عمل شركات الاتصالات وضمان سرية البيانات حماية البيانات الشخصية

¹ بوبصلة أمينة، الإستراتيجية المصرية في مكافحة التهديدات والجرائم السيبرانية دراسة للواقع والرهانات مجلة السياسة

العالمية المجلد 9 العدد 2 السنة 2025 جامعة أمحمد بوقرة بومرداس الجزائر ص 267

² بوبصلة أمينة المرجع نفسه ، ص 267

³ بوبصلة أمينة المرجع السابق ، ص 269

والأحوال المدنية تجرم المادة 72 من قانون الأحوال المدنية مثلاً أي محاولة غير مشروعة للاطلاع على البيانات المخزنة أو التلاعب بها، كذلك قانون الملكية الفكرية رقم 82 لعام 2022¹

كما تم الأخذ ببعض مواد قانون الطفل رقم 12 لعام 1996 وتعديلاته بالقانون رقم 126 لعام 2008 مثل المادة 116 مكرر التي تتعلق بتجريم استغلال الاطفال والاعتداء عليهم عبر الانترنت ، ضف الى ذلك قانون المحاكم الاقتصادية رقم 120 لعام 2008 وقانون الاجراءات الضريبية رقم 150 لعام 1950 المعدل وقانون الاحوال المدنية رقم 143 لعام 1994 حيث تجرم المادة 72 منه اية محاولة للاطلاع او الحصول على البيانات المخزنة على الحواسيب او محاولة التصرف فيها²

ثالثاً: الجانب الإجرائي في مكافحة الجريمة السيبرانية :

فيتناول القواعد والقوانين التي تتبعها السلطات لضبط الأدلة الرقمية وتفتيش النظم المعلوماتية وملاحقة الجناة ونظراً للطبيعة الافتراضية لهذه الجرائم فإن الإجراءات الجنائية التقليدية طُورت لتشمل آليات تقنية متخصصة ويمكن تلخيص أهم ملامح الجانب الإجرائي بالاستناد إلى النظم القانونية الحديثة على النحو التالي:

1- جمع الاستدلالات والضبط القضائي تتطلب هذه الجرائم مهارات فنية خاصة لذا يُمنح مأمورو الضبط القضائي المتخصصون في جرائم تقنية المعلومات صلاحيات تشمل الضبط والتحفظ على الأجهزة والمعدات ووسائل التخزين التي استُخدمت في ارتكاب الجريمة والحصول على البيانات عبر إلزام مزودي الخدمة شركات الاتصالات والإنترنت بتقديم البيانات والمعلومات اللازمة لكشف الحقيقة مع الحفاظ على سرية المحتوى إلا بأمر قضائي³

2- التفتيش والنفوذ إلى البيانات تفتيش النظم المعلوماتية يختلف عن تفتيش المساكن حيث يشمل تفتيش الأجهزة والبرامج والنفوذ قانوناً إلى الحاسبات الآلية وقواعد البيانات للبحث عن الأدلة الرقمية والمراقبة والاعتراض وتسجيل المراسلات الإلكترونية مثل الإيميلات والمحادثات في حالات الجرائم الخطيرة أو

¹ بويصلة أمينة المرجع السابق ، ص 265

² بويصلة أمينة المرجع السابق ، ص 265

³ رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون (175) 2018م

مقارناً بالمواثيق الدولية والتشريعات المقارنة، مجلة البحوث القانونية والاقتصادية، العدد 75، مارس 2021، ص 1204

التي تمس الأمن القومي ويشترط لذلك صدور إذن مسبق ومسبب من الجهة القضائية المختصة النيابة العامة أو قاضي التحقيق ولمدة زمنية محددة¹

3- التزامات مقدمي الخدمة مزودي الإنترنت يفرض القانون التزامات إجرائية على شركات الاتصالات لدعم التحقيقات منها حفظ البيانات والالتزام بحفظ سجلات الاستخدام وبيانات المرور لمدة زمنية معينة غالباً مائة وثمانون يوماً لتمكين السلطات من الرجوع إليها عند الضرورة وتقديم المساعدة الفنية والدعم التقني للسلطات لفك التشفير أو تتبع مصدر الهجمات السيبرانية²

4- حجية الدليل الرقمي من الناحية الإجرائية أصبحت الأدلة المستمدة من الأجهزة والوسائط الإلكترونية لها نفس القوة القانونية للأدلة المادية بشرط أن يتم استخراجها بوسائل فنية تضمن عدم العبث بها وأن تُحفظ بطريقة تضمن سلسلة الثقة منذ لحظة الضبط حتى تقديمها للمحكمة³

5- التدابير الاحترازية المنع من السفر وحجب المواقع يمنح القانون سلطات التحقيق الحق في اتخاذ إجراءات سريعة لدرء الخطر مثل حجب المواقع إذا كان الموقع ينشر محتوى يحرّض على العنف أو يهدد الأمن القومي حيث يجوز صدور قرار إداري أو قضائي بحجبه فوراً والمنع من السفر لمنع الجاني من الهروب خاصة في الجرائم العابرة للحدود⁴

رابعا : التعاون الدولي الإجرائي

بما أن الجاني قد يكون في بلد والمجني عليه في بلد آخر فإن الجانب الإجرائي يعتمد بشكل كبير على طلبات المساعدة القانونية المتبادلة لتبادل الأدلة الرقمية بين الدول وتسليم المجرمين في حال ضبط الجاني في دولة أخرى وفقاً للاتفاقيات الدولية مثل اتفاقية بودابست أو الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتلك الإجراءات تهدف في النهاية إلى تحقيق التوازن بين حق الدولة في العقاب وضمان الأمن الرقمي وبين حق الأفراد في حماية خصوصيتهم وحياتهم الرقمية.⁵

¹ رامي متولي القاضي، المرجع نفسه ص من 1218 الى 1250

² رامي متولي القاضي، المرجع نفسه ، ص من 1148 الى 1152

³ رامي متولي القاضي، ص 1256 ومابعداها

⁴ رامي متولي القاضي، المرجع السابق ، ص 1243 ، 1244

⁵ رامي متولي القاضي، المرجع السابق ، ص 1327

الفرع الثالث : المقارنة بين التشريع الجزائري والتشريع المصري :

سوف نحاول المقارنة بين التشريع الجزائري والمصري من حيث المنهجية التشريعية والتزامات مزودي الخدمة والاجراءات والسياسة العقابية ومسؤولية الاشخاص المعنوية.

اولاً: المنهجية التشريعية والبناء القانوني: تعتمد الجزائر أسلوب التوزيع التشريعي حيث أدرجت الجرائم والعقوبات ضمن قانون العقوبات بموجب تعديلات 2004 و 2006 بينما خصصت القانون 09-04 للقواعد الإجرائية والوقائية الدولية والمحلية لضمان مرونة الملاحقة الجنائية الرقمية وتحقيق التوازن بين القانون العام والخاص. أما المشرع المصري فقد اختار منهج التخصص الكامل بإصدار القانون 175 لسنة 2018 كمدونة قانونية واحدة وشاملة تجمع الجوانب الموضوعية والإجرائية والتقنية في نص واحد مما يسهل عملية حصر الجرائم السيبرانية وتطبيق الجزاءات المقررة لها بعيداً عن تشتت النصوص التقليدية.

ثانياً: التزامات مزودي الخدمة التقنية: يلزم التشريع الجزائري مزودي الخدمة بالتعاون مع السلطات القضائية والأمنية في إطار إجراءات المعاينة والتحقيق الرقمي وفق ما نص عليه القانون 09-04 وقانون البريد والاتصالات الإلكترونية مع التركيز على الكشف عن هوية المستخدمين عند الضرورة القضائية. وفي المقابل جاء التشريع المصري أكثر تفصيلاً في المادة 2 من القانون 175 حيث فرض التزاماً تقنياً دقيقاً بحفظ بيانات الاستخدام والاتصال لمدة 180 يوماً وإتاحتها لجهات الأمن القومي مع إقرار عقوبات جنائية ومالية رادعة على الشركات المخالفة لهذه الالتزامات التقنية.

ثالثاً: الصلاحيات الإجرائية والرقابة الرقمية: منح المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم السيبرانية صلاحيات واسعة لمراقبة الاتصالات الإلكترونية بهدف مكافحة الإرهاب والجرائم الماسة بأمن الدولة بشرط الحصول على إذن قضائي مكتوب لضمان دستورية الإجراءات وحماية الخصوصية. بينما توسع المشرع المصري في منح جهات التحقيق سلطة إصدار قرارات فورية بحجب المواقع أو الروابط الإلكترونية التي تبث محتوى يهدد الأمن القومي أو الاقتصاد الوطني مع تنظيم حق المتضرر في التظلم قضائياً مما يجعل الإجراء المصري يميل أكثر نحو الفاعلية الوقائية الآتية.

رابعاً: السياسة العقابية وحماية القيم: يركز التشريع الجزائري في سياسته العقابية على حماية أنظمة المعالجة الآلية للمعطيات والسرية المصرفية والبيانات الشخصية مع تغليب العقوبة في حال استهداف مؤسسات الدولة أو المنشآت الحيوية الوطنية بما يضمن حماية السيادة الرقمية. أما التشريع المصري فقد استحدث حماية خاصة لما يسمى بالقيم الأسرية والمبادئ الأخلاقية للمجتمع في المادة 25 مجزماً

الاعتداء على حرمة الحياة الخاصة بعبارات واسعة مع اشتراك التشريعين في تشديد العقاب إذا كان الجاني موظفاً عمومياً استغل سلطته للوصول غير المشروع للبيانات.

خامساً: المسؤولية الجنائية للأشخاص المعنوية: أقر المشرع الجزائري صراحة مسؤولية الشركات والمؤسسات عن الجرائم السيبرانية المرتكبة لحسابها أو باسمها من طرف أجهزتها المسيرة مع تقرير عقوبات تشمل الغرامة المضاعفة والمصادرة وصولاً إلى حل الشخص المعنوي أو منعه من النشاط. ويسير المشرع المصري على نفس النهج في القانون 175 حيث قرر مسؤولية مماثلة لضمان عدم إفلات الكيانات التقنية من العقاب في حال تقصيرها أو تورطها في تسهيل الجرائم الإلكترونية مما يعكس التزام البلدين بالمعايير الدولية والاتفاقية العربية لمكافحة الجريمة المعلوماتية.

المطلب الثاني: الآليات المؤسسية الوطنية في مكافحة الجريمة السيبرانية

ان إعداد ترسانة من القوانين لمكافحة الجريمة السيبرانية وحده لا يكفي بل لابد من مؤسسات وهيئات متخصصة ومؤهلة ينظمها القانون ، توكل لها مهام وقائية ردعية ورقابية ومهمة التتبع والتحري وملاحقة الجناة و هيئات اخرى لا يقع العقاب بالجناة .

الفرع الاول: الآليات المؤسسية في الجزائر: اعتمدت الجزائر استراتيجية مزدوجة، فلم تكتفي بإعداد ترسانة من القوانين فقط بل كان لزاما عليها خلق نظام مؤسسي متخصص منوط به مهمة مكافحة والوقاية من الجريمة السيبرانية ، فاستحدثت الجزائر عدت هيئات.

اولا : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : تعد هذه الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالاستقلال المالي والشخصية المعنوية التبعية والتنظيم توضع تحت سلطة وزارة الدفاع الوطني وتضم مجلسا للتوجيه ومديرية عامة مهامها الأساسية مساعدة السلطات القضائية وأجهزة الشرطة القضائية في التحريات المتعلقة بالجرائم الإلكترونية، مراقبة الاتصالات الإلكترونية للوقاية من الجرائم الإرهابية أو التخريبية التي تمس أمن الدول تنسيق جهود الوقاية وتبادل المعلومات مع الهيئات الأجنبية لتحديد هوية ومواقع مرتكبي الجرائم جمع وتوثيق المعطيات الرقمية وتحديد مصادرها لتوظيفها في الإجراءات القضائية¹.

ثانيا: الأقطاب الجزائرية المتخصصة :استحدث المشرع أقطابا قضائية متخصصة للنظر في الجرائم المعقدة ومنها:

¹ مشتة نسرين، وثام بغياني. "الجرائم المستحدثة وآليات التصدي لها في التشريع الجزائري - الجريمة الالكترونية نموذجا".

1-القطب الجزائي المتخصص لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: أنشئ بموجب الأمر 11-21 على مستوى محكمة مقر مجلس قضاء الجزائر وبممارس اختصاصه عبر كامل الإقليم الوطني يختص بجرائم المساس بأمن الدولة ترويج الأخبار الكاذبة والمساس بأنظمة المعالجة الآلية للمعطيات التابعة للمؤسسات العمومية

2-القطب الجزائي الاقتصادي والمالي: استحدث بموجب الأمر 04-20 لمعالجة الجرائم الاقتصادية والمالية المعقدة وما يرتبط بها من قضايا رقمية الهيئات الأمنية والتقنية الداعمة تتمثل في: المعهد الوطني للأدلة الجنائية وعلم الإجرام و الدرك الوطني يضم دائرة متخصصة في الإعلام الآلي والإلكتروني تتولى معالجة وتحليل الأدلة الإلكترونية وتقديم الدعم التقني للمحققين.¹

ثالثا - المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأمن الوطني: تتولى تقديم الدعم الفني لمصالح الشرطة القضائية والمساهمة في تأمين الأنظمة المعلوماتية وتنفيذ التحريات ذات الطابع الوطني والدولي²

رابعا: المديرية العامة للأمن الوطني: "تتصدى للجريمة الالكترونية من عدة جوانب ، منها الجانب القانوني المهمة بتطبيقه ، والجانب التوعوي الذي سمح لها بتنظيم دروس توعوية في مختلف المراحل الدراسية ، وكذا المشاركة في الملتقيات والندوات الوطنية ذات الصلة بالتوعية بخطورة هذا النوع من الجرائم ، وكذا تأكيدا لعضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL التي تسهل التبادل المعلوماتي الدولي وتسهل الاجراءات القضائية الخاصة بتسليم المجرمين ومباشرة الانابات القضائية ونشر اوامر القبض للمبحوث عنهم دوليا"³

"وتتجسد فاعلية الآليات المؤسسية والأمنية في ميدان مكافحة الجريمة المعلوماتية في الجزائر من خلال الدور العملياتي النشط الذي تلعبه مصالح الضبطية القضائية؛ ويبرز ذلك في الحصيلة الميدانية للمجموعة الإقليمية للدرك الوطني بسوق أهراس (مصلحة البحث والتحري)، والتي تمكنت بتاريخ 2026/05/15 من تفكيك شبكة إجرامية منظمة تتكون من خمسة أشخاص تخصصت في النصب

¹ مشتة نسرين، وثام بغياني المرجع السابق ، ص 1244

² مشتة نسرين، وثام بغياني ،المرجع السابق، ص 1245

³ خلدون عيشة، "الجريمة المعلوماتية في القانون الدولي والجزائري"، مجلة القانون والعلوم السياسية، جامعة زيان عاشور

بالجلفة، المجلد 09، العدد 01، الجزائر، 2023، ص 142

والاحتتيال وسلب أموال الغير باستخدام تكنولوجيات الإعلام والاتصال، وهو ما يعكس التنسيق المؤسسي الوثيق بين الأجهزة الأمنية وجهات القضاء نيابة الجمهورية لدى محكمتي سوق أهراس وتاوردة لتطبيق الامتدادات التقنية لهذه الجرائم وحماية الأمن السيبراني للمواطنين¹ .

الفرع الثاني: الآليات المؤسسية في مصر

تعتمد جمهورية مصر العربية على مجموعة من الآليات المؤسسية المتكاملة لمواجهة الجرائم السيبرانية وتأمين فضاءها الرقمي، ومن أبرز هذه الآليات

أولاً: المجلس الأعلى للأمن السيبراني يتبع مجلس الوزراء ويترأسه وزير الاتصالات وتكنولوجيا المعلومات. يضم ممثلين عن الأطراف المعنية بالأمن القومي وإدارة البنى التحتية الحيوية، بالإضافة إلى ذوي الخبرة في القطاع الخاص والجهات البحثية والتعليمية. يتولى المجلس وضع الإستراتيجية الوطنية للأمن السيبراني ولمواجهة الهجمات السيبرانية، والإشراف على تنفيذها وتحديثها دورياً لمواكبة التطورات التقنية. كما يضم المجلس مكتباً تنفيذياً ولجنة فنية تم اعتماد تشكيلهما وتوصيف مهامهما في جوان 2016² .

ثانياً: المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات يعمل كمنظومة وطنية لحماية أمن الفضاء السيبراني وتأمين البنى التحتية للاتصالات ونظم المعلومات القومية. وتعتبر هذه الفرق مسؤولة عن أعمال المتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحاسب المتصلة بها، والتعامل مع أية أخطار أو هجمات سيبرانية توجه إليها. كما تساهم في تبادل المعلومات لضمان الأمان وتقديم الدعم التقني المباشر للجهات الحكومية³ .

ثالثاً: المؤسسات الأكاديمية والبحثية: تم افتتاح أقسام وتخصصات أكاديمية متخصصة في الأمن السيبراني في الجامعات المصرية لزيادة الاهتمام ببحوث الأمن السيبراني وتطوير إجراءات المواجهة. ويهدف ذلك إلى إعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف

¹ الجريدة الإلكترونية الحياة DZ <https://hyat.cz/3v4lz> تاريخ النشر 2026/05/15 تاريخ الاطلاع: 26/05/16

² بوصلة أمينة ، المرجع السابق ، ص 265

³ وبوصلة أمينة المرجع السابق، ص 265

القطاعات. كما يتم تشجيع التعاون بين الجهات البحثية والشركات الوطنية في مجالات متقدمة مثل تحليل الأدلة الرقمية، التشفير، التوقيع الإلكتروني، وحماية البنى التحتية¹.

رابعاً: المحاكم الاقتصادية: تعد من الأطر القانونية والقضائية الهامة، حيث تختص بالنظر في القضايا والنزاعات المتعلقة بتكنولوجيا المعلومات وفقاً لقانون المحاكم الاقتصادية رقم 120 لعام 2008²

خامساً: فرق الاستجابة للطوارئ في القطاعات الحيوية: يتم إعداد وتفعيل هذه الفرق في القطاعات الحيوية على المستوى الوطني انطلاقاً من تجربة قطاع الاتصالات وتكنولوجيا المعلومات. وتتمثل مهمتها في حماية تأمين البنى التحتية للاتصالات، ونظم وقواعد البيانات، وبوابات الخدمات والمواقع الحكومية على الإنترنت³ تتكامل هذه الآليات المؤسسية مع الأطر التشريعية والبرامج الوطنية، مثل رؤية مصر 2030 وإستراتيجية الأمن السيبراني، لضمان بيئة رقمية آمنة

الفرع الثالث : المقارنة بين الآليات المؤسسية في التشريعين الجزائري والمصري

تعد التجربتان الجزائرية والمصرية من النماذج التشريعية الرائدة في المنطقة العربية والأفريقية التي حاولت انشاء منظومة المؤسسية متخصصة في مكافحة الجريمة السيبرانية، تمثل هذه الهيئات الذراع الفني للقضاء في كلا الدولتين مع اختلاف في التبعية والتخصص فعلى المستوى التقني أنشأ المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وهي هيئة ذات طابع سيادي وقائي وفي المقابل يلعب الجهاز القومي لتنظيم الاتصالات في مصر دوراً محورياً مزدوجاً تنظيمي وقضائي في تطبيق العقوبات الإدارية والحجب الفني وعلى المستوى القضائي نلمس تطوراً نوعياً في التشريعين حيث اعتمدت الجزائر نظام الأقطاب الجزائية المتخصصة المتمثل في القطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بينما أسند المشرع المصري الاختصاص للمحاكم الاقتصادية وهو توجه يؤكد القناعة بضرورة وجود قاضٍ متخصص يمتلك الحد الأدنى من المعرفة التقنية للفصل في هذه المنازعات المعقدة.

¹ بوبصلة أمينة ، المرجع السابق ، ص 264

² بوبصلة أمينة المرجع السابق ، ص 265

³ بوبصلة أمينة المرجع السابق ، ص 264، 266، 267

المطلب الثالث : مدى انسجام وفعالية التشريعين الجزائري و المصري مع المعايير الدولية

حاول المشرع الجزائري والمشرع المصري مواكبة القوانين المقارنة والاليات الدولية لمكافحة الجريمة السيبرانية، في محاولة منهم للالتحاق بمصاف الدول المتطورة واستعاب هذه الظاهر ومحاصرتها والسيطرة عليها والسعي للانسجام مع المعايير الدولية وتجسيد ذلك بكل فعالية.

الفرع الاول :تقييم التجربة الجزائرية

من خلال تقييم التجربة الجزائرية في مكافحة الجريمة السيبرانية يظهر لنا التزاما قويا بمواكبة المعايير الدولية وخاصة اتفاقية بودابست لعام 2001 رغم عدم المصادقة الرسمية عليها حتى الآن حيث اعتمد المشرع الجزائري نهجا يتوافق مع الجوانب الموضوعية للاتفاقية الدولية وظهر ذلك من خلال تعديل قانون العقوبات عبر القانون رقم 15/04 الذي استحدث قسماً خاصاً بالمساس بأنظمة المعالجة الآلية للمعطيات .

تجريم الأفعال الأساسية شمل التشريع الجزائري تجريم الدخول عن طريق الغش إلى المنظومات المعلوماتية وإزاحة أو تعديل المعطيات وتخريب أنظمة الاشتغال وهو ما يتماشى مع جوهر جرائم الحاسب في اتفاقية بودابست ولا يفوتنا ان ننوه ان التشريع الجزائري أقر المسؤولية الجزائية للشخص المعنوي الشركات والمؤسسات عن الجرائم السيبرانية تماشياً مع متطلبات المادة 12 من الاتفاقية الدولية و لم يكتفِ المشرع بالقواعد العامة بل استحدث ترسانة قانونية متخصصة القانون رقم 04 /09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي وضع آليات إجرائية خاصة للتحقيق والتحري في هذا النوع من الجرائم الحماية الدستورية والمدنية كرس دستور 2020 حماية سرية المراسلات والاتصالات الخاصة كحق أساسي كما يوفر القانون مدني المادة 124 أساساً للتعويض عن الأضرار الناجمة عن الاعتداءات الإلكترونية استنادا لما سبق ذكره نجد ان الجزائر سارعت لتدارك الفراغ التشريعي منذ عام 2004 لمواجهة التطور المتسارع للتهديدات الرقمية.

كما اشتهد المشرع الجزائري من اجل تحقيق الموازنة بين فعالية المكافحة وبين احترام الحقوق والحريات الأساسية وحماية الخصوصية .

الفرع الثاني: تقييم التجربة المصرية

تتجسد التجربة المصرية في مكافحة التهديدات السيبرانية من خلال ممارسات متعددة تهدف لحماية الأمن القومي وتقليل المخاطر الاجتماعية والأمنية حيث حققت الدولة إنجازات رقمية ملموسة بحصولها على المركز الثالث والعشرين عالمياً في مؤشر الأمن السيبراني لعام ألفين وعشرين كما تصدرت المرتبة الأولى عالمياً في كفاءة قطاعي الإنترنت والهاتف عام ألفين وواحد وعشرين 2021 وترتكز قوة هذه التجربة على وجود إطار مؤسسي فعال يتمثل في المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء بالإضافة إلى وجود مركز للاستجابة الطارئة للأزمات السيبرانية وتستند الدولة في تحركاتها إلى غطاء دستوري وقانوني صريح حيث تنص المادة 31 من الدستور على أن حماية الفضاء المعلوماتي جزء لا يتجزأ من الأمن القومي وقد تم تعزيز ذلك بإصدار قوانين متخصصة لمكافحة جرائم تقنية المعلومات وحماية البيانات الشخصية، ورغم هذه النجاحات تواجه التجربة تحديات مستمرة تتمثل في غياب الوعي المجتمعي بالتهديدات الإلكترونية وضعف التمويل اللازم لحماية البنية التحتية الرقمية في بعض القطاعات فضلاً عن نقص عدد المختصين والتقنيين الذين يمتلكون المهارات اللازمة كما تزداد الخطورة بسبب تطور أسلحة المجرم المعلوماتي واعتماده على تقنيات عالية تجعل من الصعب تتبع مصدر الهجمات أو التعرف على المنفذين بسهولة غير أن الواقع المصري يشير إلى زيادة إقليمية واضحة خاصة مع الاستثمار في الكوادر البشرية .

خلاصة الفصل:

يتناول الفصل الثاني الآليات القانونية والمؤسسية لمكافحة الجريمة السيبرانية من خلال رؤية تحليلية مقارنة، مبرزاً الترسانة القانونية التي استُحدثت لمواجهة التحديات التقنية المعاصرة. ينقسم الفصل إلى محورين أساسيين:

الآليات الدولية ركزنا فيه على ضرورة التعاون الدولي لمواجهة الطبيعة العابرة للحدود للجريمة الرقمية، ويوضح التطور من اتفاقية بودابست 2001 التي واجهت انتقادات تتعلق بالسيادة، إلى اتفاقية الأمم المتحدة 2024 التي مثلت تحولاً نحو عالمية المواجهة والموازنة بين السيادة الوطنية وتسهيل تبادل الأدلة الرقمية كما اشرنا إلى التحديات الإجرائية التي فرضها الذكاء الاصطناعي، مثل التزييف العميق، والتي تتطلب تحديث مفاهيم التفتيش الرقمي.

الآليات الوطنية الجزائر ومصر نموذجاً يستعرض الإجراءات الجنائية المبتكرة للتعامل مع الطبيعة غير المادية للجريمة. فبينما اعتمد المشرع المصري منهج "التخصص الكامل" عبر القانون 175 لسنة 2018 الذي جمع القواعد الموضوعية والإجرائية في نص واحد مع منح حماية دستورية لأمن الفضاء المعلوماتي، يركز التشريع الجزائري على إلزامية التعاون في كافة الحالات.

أما وفي الجانب المؤسسي، تبرز الأقطاب القضائية المتخصصة في الجزائر ومركز بلاغات جرائم التقنية في مصر كأدوات تقنية لملاحقة المجرمين.

يخلص الفصل إلى أن نجاح المواجهة لا يتوقف فقط على وجود الهيئات، بل على تأهيل العنصر البشري وامتلاك القضاة والمحققين لثقافة رقمية تمكنهم من تحليل الأدلة. ويؤكد أن "البصمة الجديدة" للمكافحة تكمن في القدرة على تحقيق توازن دقيق بين فعالية التحقيق الجنائي وبين قدسية الخصوصية الرقمية للمواطنين.

الخاتمة

بعد الإحاطة بالأبعاد المختلفة لموضوع مكافحة الجريمة السيبرانية في هذه الدراسة، يمكن القول إننا أمام ظاهرة إجرامية متطورة لا تعترف بالحدود الجغرافية للدول، مما جعل البحث في إطارها المفاهيمي وخصائصها الفنية مدخلاً ضرورياً لفهم طبيعة التهديدات التي تمس الأمن القومي والسيادة الرقمية، وقد خلصت دراستنا إلى أن المواجهة القانونية لهذا الإجرام المستحدث لا يمكن أن تكتمل إلا عبر منظومة متكاملة تجمع بين القواعد القانونية المرنة والآليات المؤسسية المتخصصة على المستويين الوطني والدولي.

وتأسيساً على ما سبق، توصلنا إلى مجموعة من النتائج تمثلت في:

1. تعد الجريمة السيبرانية جريمة مستحدثة ومتطورة باستمرار، ترتبط ارتباطاً وثيقاً بالتقدم التكنولوجي، مما جعلها تشكل تهديداً للأمن على المستويين الوطني والدولي.
2. تتميز بخصائص فريدة تجعلها تختلف جذرياً عن الجرائم التقليدية، فهي عابرة للحدود الجغرافية، وتنفذ في بيئة رقمية افتراضية، وتتسم بالسرعة في التنفيذ وصعوبة الإثبات نظراً لسهولة طمس الأدلة الرقمية وبذلك فهي جريمة شديدة الخطورة
3. أن القوانين التقليدية لم تعد قادرة على استيعاب هذا النوع من الجرائم
4. ان الجريمة السيبرانية جريمة متطورة باستمرار تسبق القوانين التي تجرمها
5. صعوبة التوفيق بين متطلبات الأمن القومي والسيادة الرقمية من جهة وصون الحريات الفردية وحرمة الحياة الخاصة للمواطنين من جهة أخرى.
6. فجوة الكوادر البشرية والنقص الفادح في الاطارات المتخصصة من قضاة ورجال القانون الذين يجمعون بين الخبرة القانونية والمعرفة التقنية العميقة.

وفقاً للنتائج السابقة نقترح مايلي :

1. تبني تشريعات ديناميكية قادرة على ملاحقة التسارع التكنولوجي وتقليص حالات الفراغ التشريعي التي قد يستغلها مرتكبو الجرائم السيبرانية، وضع تعريفات قانونية واضحة مثل التفتيش الرقمي والحفظ السريع للبيانات لتفادي الغموض القانوني
2. التوجه نحو قوانين تستهدف الانسان الرقمي وحقوقه بذات القدر الذي تحمي به الفضاء الرقمي من التهديدات.
3. تطوير الكوادر البشرية والتدريب بحيث يكون تكوين تخصصي مزدوج يجمع بين المعرفة القانونية والخبرة التقنية لرجال القانون.

4. تحسين قدرات الاجهزة الامنية ومراكز الامن السيبراني في مجال التحقيق والتدريب على استخدام ادوات التحليل البيانات لتعقب الجناة الذين يستخدمون التشفير.
5. الاستثمار في الذكاء الاصطناعي وتقنيات التحقيق الرقمي الحديثة لرف كفاءة استخراج الادلة الرقمية ومنع طمسها والتلاعب بها .
6. دعم الدول النامية في بناء قدراتها الفنية والتقنية لتمكينها من تطبيق الاتفاقيات الدولية بفعالية
7. إن تكريس السيادة الرقمية وحماية المصالح العليا للمجتمع في عصر المعلومات يتطلب استشرافاً مستمراً للمستقبل واستثماراً في تقنيات التحقيق المتقدمة والذكاء الاصطناعي، مع الانفتاح الدائم على آليات التعاون الدولي التي تضمن ملاحقة الجناة أينما وجدوا، لتظل العدالة قائمة حتى في الفضاءات الافتراضية الأكثر تعقيد .

قائمة

المصادر والمراجع

أولاً: المصادر

- الاتفاقيات والمعاهدات الدولية

1. اتفاقية مجلس أوروبا المتعلقة بالجريمة المعلوماتية (اتفاقية بودابست)، (2001).
2. اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية، (2024).

- القوانين ومراسيم:

3. الأمر رقم 66-156 المؤرخ في 18 جوان 1966، المتضمن قانون العقوبات الجزائري، المعدل والمتمم لا سيما بموجب القانون رقم 04-15 المستحدث للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، والقانون رقم 16-02
4. قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الصادر بتاريخ 14 أغسطس 2018، الجريدة الرسمية لجمهورية مصر العربية، العدد 32 مكرر ج
5. قانون مكافحة الجرائم الإلكترونية رقم 5 لسنة 2022، الصادر عن مجلس النواب الليبي. قانون الجرائم الإلكترونية رقم 27 لسنة 2015، وقانون جرائم أنظمة المعلومات رقم 30 لسنة 2010.
6. المرسوم الرئاسي رقم 24-07 المؤرخ في 7 جانفي سنة 2024 المتعلق بالاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، العدد 04 الصادر بتاريخ 18 جانفي 2024.
7. القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت سنة 2009، الجريدة الرسمية للجمهورية الجزائرية، العدد 47.

ثانياً: المراجع:

- الكتب:

1. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت الجرائم الالكترونية دراسة مقارنة في النظم القانونية لمكافحة جرائم المعلوماتية والانترنت مع الاشارة الى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، 2007، لبنان بيروت
2. نهلاء عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2010، الأردن عمان
3. أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، 2011، مصر الإسكندرية
4. أسامة أحمد المناعسة، جلال محمد الزغبى، جرائم تقنية نظم المعلومات الالكترونية دراسة مقارنة، دار الثقافة للنشر والتوزيع، 2014، الأردن عمان
5. غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها خصائصها كيفية التصدي لها قانونا، دار الثقافة، 2016 ، الأردن عمان
6. عبد الإله النوايسة، جرائم تكنولوجيا المعلومات شرح الاحكام الموضوعية في قانون الجرائم الالكترونية، دار وائل للنشر والتوزيع، 2017، الأردن عمان
7. محمود أحمد القرعان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، 2017، الأردن عمان
8. سعيدي سليمة وحجازي بلال، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، 2017، مصر الإسكندرية
9. علوي علي أحمد الشارفي، الوجيز في جرائم تقنية المعلومات، المركز الديمقراطي العربي للدراسات الاستراتيجية الاقتصادية والسياسية، 2024، ألمانيا برلين

- مجالات ومقالات:

1. خلدون، عيشة. (2023). "الجرائم المعلوماتية في القانون الدولي والجزائري". مجلة القانون والعلوم السياسية، المجلد 09، العدد 01، جامعة زيان عاشور بالجلفة، الجزائر.
2. رزاق بارة، كريمة. (2024). "الجريمة الالكترونية المتعلقة بالأشخاص وفقاً للتشريع الفرنسي والتشريع الجزائري". المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 08، العدد 02، المركز الجامعي عبد الحفيظ بوالصوف ميله، الجزائر.
3. رضا، مهدي. (2021). "الجرائم السيبرانية وآلية مكافحتها في التشريع الجزائري". مجلة ابليلز للبحوث والدراسات الجامعية، المجلد 06، الصادر بتاريخ 13/12/2021، جامعة محمد بوضياف المسيلة، الجزائر.
4. شويرب، جيلالي ومراد، فايزة. (2023). "الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية". مجلة الدراسات القانونية والسياسية، المجلد 09، العدد 02، جوان، جامعة عمار ثلجي الأغواط، الجزائر.
5. مانيو، جيلالي؛ وعروس، كوثر. (2022). "الجريمة السيبرانية في صورها المستحدثة". مجلة القانون والتنمية، المجلد 04، العدد 01، جويلية، جامعة طاهري محمد بشار، الجزائر.
6. مشته، نسرین؛ وبغياني، وئام. (2025). "الجرائم المستحدثة وآليات التصدي لها في التشريع الجزائري - الجريمة الالكترونية أنموذجاً". مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 08، العدد 02، المركز الجامعي بركة، الجزائر.
7. الهاجري، نايف شافي المظافرة. (2023). "جرائم تقنية المعلومات في التشريع الأمريكي مقارنة بالتشريعات العربية"، العدد 38، مارس.
8. لفريحات، عماد حسين محمد. (2023). "الجهود العربية والإفريقية لمواجهة الجرائم الإلكترونية في الفترة 2010-2023". مجلة ابن خلدون للدراسات والأبحاث، المجلد 03، العدد 05، مايو.
9. بوبصلة، أمينة. (2025). "الإستراتيجية المصرية في مكافحة التهديدات والجرائم السيبرانية دراسة للواقع والزهانات". مجلة السياسة العالمية، المجلد 09، العدد 02، جامعة أمحمد بوقرة بومرداس، الجزائر.

10. إسلام عبد ربه رمضان عبد ربه هديب، "مكافحة الجريمة السيبرانية في ضوء القانون الدولي"، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية، المجلد 27، العدد 1، 2026.
11. سعيد مسعود الكثيري، الجريمة الالكترونية في ضوء اتفاقية بودابست الاطار المفاهيمي والتصنيفي مجلة البحوث القانونية والاقتصادية ، جامعة ظفار عمان ، المجلد 9 العدد 1 2026
12. مهداوي حنان، "التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري"، مجلة الفكر القانوني والسياسي، جامعة محمد لمين دباغين - سطيف 2، المجلد 06، العدد 02، 2022، ص 1061.
13. عبو عفيف، "الأليات القانونية في الجزائر وتطورها في مكافحة الجريمة الإلكترونية"، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس مستغانم، المجلد 09، العدد 01، جوان 2024، ص 24.
14. رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون (175) 2018 مقارناً بالمواثيق الدولية والتشريعات المقارنة، مجلة البحوث القانونية والاقتصادية، العدد 75، مارس 2021
15. فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية مجلة البحوث في الحقوق والعلوم السياسية المجلد 08 العدد 01 جامعة البليدة 02 الجزائر 2022
16. وهيبة عبد الرحيم، ومن معها ،الجرائم الالكترونية من خلال مؤشرات عالمية واثارها على المؤسسات ،مجلة دراسات الصادرة عن جامعة الأغواط، المجلد 16، العدد 01، في شهر جانفي من عام 2019
17. عبد الحميد بوديار، رشيد طبال ، مقال الجريمة السيبرانية وتأثيراتها على الفرد والمجتمع في عصر التكنولوجيا ، مجلة الباحث في العلوم الانسانية والاجتماعية ، المجلد 16/العدد 01- السنة 2025
18. قطاف سليمان ومن معه ، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية ، مجلة البحوث القانونية والاقتصادية المجلد 05 العدد 02 جامعة الاغواط 2022

المواقع الإلكترونية :

1. موقع الأمانة العامة للحكومة الجزائرية (SGG) للاطلاع على أعداد الجريدة الرسمية للجمهورية الجزائرية والقوانين والمراسيم الوطنية مثل القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الرابط الإلكتروني: <https://www.sgg.gov.dz> : فبراير 2026م.
2. موقع ديوان التشريع والرأي الأردني: للاطلاع على نصوص التشريعات والقوانين الأردنية المقارنة (قوانين الجرائم الإلكترونية)، الرابط الإلكتروني: <https://www.lob.gov.jo> :، تاريخ الاطلاع: 14 فبراير 2026م.
3. موقع منصة "منشورات قانونية" (الأرشيف الرقمي للتشريعات): للاطلاع على أعداد الجريدة الرسمية المصرية والقوانين المقارنة (مثل قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018)، الرابط الإلكتروني: <https://manshurat.org> :، تاريخ الاطلاع: 14 فبراير 2026م.
4. موقع الإذاعة الجزائرية (بوابة الملتيميديا والأخبار): جمال خفيف، حوار إذاعي بعنوان "توقيع الجزائر على معاهدة مكافحة الجريمة السيبرانية خطوة إستراتيجية"، تاريخ النشر: 09 نوفمبر 2025م، الرابط الإلكتروني: <http://news.radioalgerie.dz> :، تاريخ الاطلاع: 03 ماي 2026م.
5. منصة يوتيوب قناة الأخبار الدولية: AL24 New تقرير إعلامي مصور بعنوان "معاهدة مكافحة الجريمة السيبرانية ثمرة 5 سنوات من المفاوضات الدولية بقيادة الجزائر"، الرابط الإلكتروني: <https://www.youtube.com/watch?v=@AL24newschannel> :، تاريخ الاطلاع: 01 أبريل 2026م.
6. منصة يوتيوب (قناة الجزيرة الوثائقية): برنامج وثائقي ضمن سلسلة علوم الإجرام بعنوان "الجرائم الإلكترونية"، تاريخ الاطلاع: 01 أبريل 2026م.
7. موقع أسترا للأمن السيبراني العالمي (GetAstra) للاطلاع على التقارير والإحصائيات والبيانات الرقمية المتعلقة بالتهديدات والاختراقات الأمنية، الرابط الإلكتروني: <https://www.getastra.com> :، تاريخ الاطلاع: 01 أبريل 2026م.
8. موقع أسترا للأمن السيبراني العالمي (GetAstra) للاطلاع على التقارير والإحصائيات والبيانات الرقمية المتعلقة بالتهديدات والاختراقات الأمنية، الرابط الإلكتروني: <https://www.getastra.com> :، تاريخ الاطلاع: 01 أبريل 2026م.
9. موقع أسترا للأمن السيبراني العالمي (GetAstra) للاطلاع على التقارير والإحصائيات والبيانات الرقمية المتعلقة بالتهديدات والاختراقات الأمنية، الرابط الإلكتروني: <https://www.getastra.com> :، تاريخ الاطلاع: 01 أبريل 2026م.
10. الرابط الإلكتروني: <https://www.getastra.com> :، تاريخ الاطلاع: 01 أبريل 2026م.

فهرس المحتويات

الصفحة	عنوان
	كلمة الشكر
	اهداء
02	مقدمة
	الفصل الأول: الاطار المفاهيمي والقانوني للجرائم السيبرانية
08	المبحث الاول: مدلول الجرائم السيبرانية
08	المطلب الأول: مفهوم الجرائم السيبرانية فقها وتشريعا
19	المطلب الثاني: خصائص الجرائم السيبرانية وتمييزها عن الجرائم التقليدية
22	المطلب الثالث: أركان الجريمة السيبرانية
28	المبحث الثاني: صور الجرائم السيبرانية وآثارها
28	المطلب الأول: أنواع الجرائم السيبرانية
33	المطلب الثاني: اثار الجريمة السيبرانية
	الفصل الثاني: الآليات القانونية والمؤسسية على المستويين الدولي والوطني لمكافحة الجرائم السيبرانية
42	المبحث الاول: آليات مواجهة جريمة السيبرانية على المستوى الدولي
42	المطلب الأول: الآليات القانونية الدولية لمكافحة الجريمة السيبرانية
53	المطلب الثاني: الآليات المؤسسية الدولية لمكافحة الجريمة السيبرانية
58	المطلب الثالث: اشكال التعاون الدولي لمكافحة الجريمة السيبرانية
63	المبحث الثاني: آليات المواجهة جريمة السيبرانية على المستوى الوطني (دراسة مقارنة بين التشريعي الجزائري والمصري)
63	المطلب الأول: الآليات القانونية الوطنية لمكافحة جريمة السيبرانية
76	المطلب الثاني: الآليات المؤسسية الوطنية لمكافحة جريمة السيبرانية
80	المطلب الثالث: مدى انسجام وفعالية التشريعين الجزائري والمصري مع المعايير الدولية
84	الخاتمة
87	قائمة المصادر والمراجع
	فهرس المحتويات