وزارة التعليم العالي و البحث العلمي

جامعة د. مولاي الطاهر سعيدة

كلية الحقوق و العلوم السياسية

قسم : الحقوق

العنوان:

آليات التعاون الدولي لمكافحة الجريمة السيبرانية

مذكرة تخرج لنيل شهادة الماستر تخصص : قانون جنائي.

من إعداد الطالب:

شوال بومدين

تحت إشراف:

د. عبد اللطيف بومليك

أعضاء لجنة المناقشة

د. إلياس نعيمة	جامعة د. مولاي الطاهر سعيدة	رئيسا
د.عبد اللطيف بومليك	جامعة د. مولاي الطاهر سعيدة	مشرفا ومقرّرا
د. بن عودة حورية	جامعة د. مولاي الطاهر سعيدة	عضوا

السنة الجامعية : 2025/2024

وزارة التعليم العالي و البحث العلمي

جامعة د. مولاي الطاهر سعيدة

كلية الحقوق و العلوم السياسية

قسم : الحقوق

العنوان:

آليات التعاون الدولي لمكافحة الجريمة السيبرانية

مذكرة تخرج لنيل شهادة الماستر تخصص : قانون جنائي.

من إعداد الطالب:

شوال بومدين

تحت إشراف:

د. عبد اللطيف بومليك

أعضاء لجنة المناقشة

د. إلياس نعيمة	جامعة د. مولاي الطاهر سعيدة	رئيسا
د.عبد اللطيف بومليك	جامعة د. مولاي الطاهر سعيدة	مشرفا ومقرّرا
د. بن عودة حورية	جامعة د. مولاي الطاهر سعيدة	عضوا

السنة الجامعية : 2025/2024

إهداء:

إلى روحِ أمّي...

يا نبعَ الحنانِ الأبديِّ، يا ظِلَّ اللهِ في أرضه،

رحلتِ، فصار الفرحُ منقوصًا،

وصوتُكِ في الذاكرةِ صلاة،

وفي قلبي دعاءٌ لا ينقطع.

إلى والدي...

سندي، ومعلّمي، وأوّل دروسي في الصبر والحكمة،

ما انحنيتُ إلا لتقبيلِ يديك، وما ارتفعتُ إلا بدعائك.

إلى إخوتي وأخواتي...

من أشتدُّ بهم في ليلِ الانكسار،

وفي دفئهم يزهر عمري.

إلى زوجتي .. وإلى أبنائي إسلام وآدم، وزهرة الدار "رابحة"،

أنتم العمرُ حين يُزهر، والمستقبلُ حين يُؤمَل.

إلى رفاق الدرب...

إلى كلّ من تقاسم معي مشقة السّير وطول الطريق،

إلى أخي الدكتور عبد الرحمن حليمي،

من انطبعت لمساته في ثنايا هذا العمل.

إلى أستاذي عبد اللطيف بومليك...

الذي نحت فينا الفكرَ، وفتح أمامنا نوافذ العلم والوطن.

إلى نفسي...

إلى من سهر وكتب وارتقى.

إلى كلّ من يحمل في قلبه ضمير أمة،

إلى وطني الجريح، وإلى أهل غزة،

حيثُ المجدُ تحت القصف،

والكرامةُ تنبت من بين الركام.

إلى الأرواح التي عبرت الروح همسًا، ومضيا دون ضجيج،

لكنّ الذكرى ما زالت تورق في خاطري كزهرٍ لم يذبل...

لذكرياتي من الحكايا ما لا يُكتب، ومن الوفاء ما لا يُنسى.

إلى الإنسانية جمعاء...

علّ في هذا الحرف قبسُ نورٍ يشعُّ في دروب العدل والسّلام.

شكر وتقدير

إلى أولئك الذين زرعوا في دربي نورًا، وفي فكري بذورًا، فأنبتت معرفةً وأزهرت يقينًا...

إلى الطاقم الجامعي بكلية الحقوق – جامعة سعيدة، أنتم الضوء الذي أضاء عتمة السؤال، والسند في لحظات التردّد، فلكم من القلب ألف تحية وسلام.

إلى أساتذتي الأفاضل، من علّموني كيف يكون العلم التزامًا، والبحث رسالة، لا أملك أمام عطائكم إلاّ صمتًا يعانقه الامتنان.

إلى لجنة المناقشة الموقّرة، أنتم نبل العلم حين يكتمل بالحكمة، شكري لكم يفيض من حبر هذا العمل.

الى أستاذي الدكتور عبد اللطيف بومليك، من نقش ببصيرته خارطة هذا المشروع، فكنت الدليل حين غاب الاتجاه، والمحفّز حين سكن الحرف، لك منّي امتنان لا يبلغه الكلام.

وإلى زملائي ورفقاء الدرب، من تقاسموا معي التعب، والقلق، واليقظة في محراب البحث... دمتم رفقة الفكر والضمير.

لكم جميعًا، أهدي هذا العمل، حبًا، وامتنانًا، وذكرى لا تغيب.

– قائمة المختصرات–

- الصفحة: ص.
- الصفحة نفسها: ن ص.
- مجلد: مج.
- العدد: ع.
- الطبعة: ط.

المقدمة

في زمن تتسارع فيه التطورات التكنولوجية والتحولات الرقمية وتندمج فيه الوقائع المادية بالفضاءات الافتراضية، تولدت تهديدات جديدة – بأقنعة غير مألوفة تتسلل إلى الأنظمة والمجتمعات– لا ترى بالعين المجردة ولا تقاس بقوة السلاح التقليدي بل تمارس فعلها التخريبي من خلف الشاشات وتحت ظلال الشبكات.

في هذا العصر الذي باتت فيه السيادة الوطنية تختبر في عوالم رقمية موازية، ظهرت الجريمة السيبرانية كأحد اخطر التحديات التي تواجه الأمن العالمي والعدالة الجنائية وحقوق الإنسان والمؤسسات الديمقراطية.

فكان أول ظهور للجريمة السيبرانية في ستينيات القرن الماضي في أعقاب استخدام الحواسيب التجارية، لكنها لم تكن تشكل في بداياتها إلا انتهاكا محدود النطاق[1]، ومع تطور الأنترنت وانتشارها في تسعينيات القرن الماضي بدأ هذا النمط الحديث يتخذ أبعادا أكثر تعقيدا لتتحول هذه الجريمة في العقود الأخيرة إلى ظاهرة عالمية معقدة، تمارسها جهات منظمة ودول راعية، وفاعلون جدد من فئة القراصنة أو "الهاكرز" مستهدفة البنى التحتية الحيوية، والبيانات الشخصية، والمؤسسات المالية العسكرية والسياسية، إنها الجريمة التي لا تعترف بالحدود وتضرب في كل مكان وفي كل لحظة حاملة في طياتها مخاطر التجسس، والتخريب الإرهاب والابتزاز الرقمي[2].

ولان هذه الجريمة تتجاوز الإمكانات الفردية للدول أضحى التعاون الدولي ضرورة وجودية لمكافحتها، ويتطلب هذا التعاون توحيد المفاهيم القانونية وتبادل المعلومات والمساعدة القضائية والتنسيق الأمني عبر شبكات واتفاقيات متعددة الأطراف، لكن هذه المساعي تصطدم بجملة من التحديات مثل اختلاف في التشريعات، ضعف الإرادة السياسية، غياب الثقة بين الدول، وانعدام في آلية ملزمة وموحدة لذلك فان البحث في آليات التعاون الدولي يعد خطوة أساسية لفهم سبل التصدي لهذه الظاهرة وتجاوز معيقات مكافحتها[3].

[1]– سمير بوثلجة، الجريمة السيبرانية المعلوماتية، دراسة في القانون الجزائري والمقارن، دار هومة، الجزائر، 2013، ص25.

[2]– عبد الحفيظ بوزيد، الجرائم المعلوماتية والتعاون الدولي ومكافحتها، دار المعرفة، الجزائر، 2020، ض47.

[3]– اتفاقية بودابست، مجلس أوروبا، الجريمة السيبرانية، 2001/11/27، المادة:35.

من بين الأسباب المحفزة لاختيار موضوع: **آليات التّعاون الدّولي في مكافحة الجريمة السيبرانيّة**. دوافع موضوعيّة وأخرى ذاتية تمثّلت في:

أ- الجريمة السيبرانية بوصفها ظاهرة حديثة تمس كل المجتمعات.

ب- ندرة الدّراسات القانونية العربية المتخصّصة في آليّات التّعاون الدّولي.

ج- التعرف على مضمون التّعاون الدّولي في مكافحة الجريمة السيبرانيّة بموجب الاتّفاقيّات الدّولية

د- المساهمة في إثراء النقاش الأكاديمي حول الموضوع.

هـ- دراسة سبل التّعاون الدّولي ومدى تجاوبه وحيثيّات مبادراته من خلال الوقوف على أهمّ النّصوص القانونيّة المتعلّقة بالجريمة السيبرانيّة.

يكتسب موضوع: - **آليات التّعاون الدّولي في مكافحة الجريمة السيبرانيّة-** أهميّته من طبيعة الظّاهرة التي يتناولها، متجلية في:

أ- الجريمة السيبرانيّة من الجرائم العابرة للحدود عبر الفضاء الرّقمي فيمكن أن يكون الفاعل في دولة والضّحية في دولة أخرى.

ب- خطورة هذه الجرائم التي أصبحت تشكّل تهديدا عالميا على الدّول والأفراد، في ظلّ هشاشة التشريعات الوطنيّة وفشلها في مواكبة تطورات عالم الجريمة الذي يتطلّب تعاونا دوليا لمكافحة هذة الجريمة المستحدثة.

ج- تميّز الجريمة السيبرانيّة عن الجرائم التّقليدية من حيث أدوات الاستعمال، أو من حيث محل الجريمة ومسرحها

د- إفلات مرتكبي الجرائم السيبرانيّة من الإيقاف نظرا للثّغرات القانونية، وقصور التّشريعات الوطنيّة التي مازالت تعامل هذا النّوع من الجرائم تعاملا تقليديا.

هـ- تصاعد وتزايد الجرائم السيبرانيّة بشكل مخيف عبر العالم، واتّساع مجالاتها التي أصبحت تهدّد الأمن السيبراني للدّول.

ومن الأهداف المرجاة من الموضوع :

أ- تحليل مفهوم الجريمة السيبرانيّة وأبعادها القانونيّة.

ب- يهدف البحث إلى استعراض آليات التّعاون الدّولي وتقييم مدى فعاليته.

ج- يهدف البحث إلى دراسة الإطار القانوني الدولي لمكافحة الجريمة السيبرانيّة.

د- يهدف البحث إلى إبراز أهمّ الصّعوبات والمعيقات التي تواجه التّعاون الدّولي في مكافحة الجرائم السيبرانيّة وسبل تعزيز مواجهتها.

كما أن هناك جملة من الدّراسات التي تناولت في فحواها الجريمة السيبرانيّة مثل:

أ- مذكرة ماستر للطالبين: معتوق محمد آكلي، عاشور شمام، بعنوان: التّعاون الدّولي في مكافحة الجريمة الإلكترونيّة، جامعة محمد البشير الإبراهيمي - برج بوعريريج- كليّة الحقوق والعلوم السّياسية، 2023-2024م.

ب- مذكرة ماستر للطالبين: شريف جمال، زقرار عبد العزيز، بعنوان: آليات مواجهة الجرائم السيبرانيّة في الجزائر، جامعة محمد البشير الإبراهيمي - برج بوعريريج- كليّة الحقوق والعلوم السّياسية، 2023-2024م.

ج- رسالة دكتوراه للطالبة: عائشة الحاجي، تحت عنوان: المسؤولية الدوليّة في مكافحة الجرائم السيبرانية، جامعة تونس، 2020-2021م.

ومنه يمكننا طرح الإشكالية التالية - كيف يمكن تفعيل أليات التّعاون الدولي بشكل فعّال في مكافحة الجريمة السيبرانيّة؟

للإجابة عن الإشكالية اعتمدنا في هذه الدّراسة على المنهج التّحليلي المقارن الذي يهدف إلى دراسة حالة بغية رصد إشكاليّة ما وتحليل عناصرها واقتراح حلول لها.

وبما أنه لا يخلو بحث من المصاعب كونها جزء منه نعددها في الآتي:

أ- قلّة المصادر العربيّة لحداثة هذا النّوع من الجرائم.

ب- صعوبة الوصول إلى الوثائق والاتّفاقيّات التقنيّة الحديثة وترجمتها.

ج- تشعّب البحث وتداخله البيني مع فروع قانونيّة أخرى.

د- ضيق الوقت وعدم كفايته لدراسة موضوع واسع المجال وبالغ الأهميّة كالذي بين أيدينا.

في سبيل مقاربتنا الإجابة عن الإشكاليّة المطروحة اقتضى منّا البحث تقسيمه إلى فصلين رئيسين:

- **الفصل الأوّل**: الإطار المفاهيمي والقانوني للتّعاون الدّولي في مكافحة للجريمة السيبرانيّة.
  - **المبحث الأوّل**: الجريمة السيبيرانيّة بوصفها جريمة عالميّة معقّدة.
  - **المبحث الثّاني**: الإطار القانوني الدّولي لمكافحة الجريمة السيبرانيّة.
- **الفصل الثّاني**: واقع التّعاون الدّولي وتحدّياته وآفاق تطويره.
  - **المبحث الأوّل**: الميكانيزمات المؤسّساتيّة والتّقنية للتّعاون الدّولي.
  - **المبحث الثاني**: التّحديات التي تواجه التّعاون الدّولي والحلول القائمة.

الفصـــــــل الأوّل

الإطار المفاهيمي والقانوني للتّعاون الدّولي في مكافحة للجريمة السيبرانيّة

الفصل أوّل: الإطار المفاهيمي والقانوني للتّعاون الدّولي في مكافحة للجريمة السيبرانيّة.

شهد العالم مع مطلع الألفيّة الثّالثة تحولات جذرية في التطورات التكنولوجيّة، والطّفرة الرقمية الهائلة التي غيرت ملامح العلاقات البشرية وأعادت رسم الحدود الدولية، فأمام هذه التحولات الرقمية المتسارعة، لم تعد الجريمة ظاهرة تقليدية محصورة في حدود جغرافية أو محاطة بجدران سيادية، بل باتت تنتمي إلى فضاء جديد مفتوح تتوارى في الوجوه، وتتعقد فيه الأدلة، وتتشظى فيه المسؤوليات، حتى أصبحت تسمى بهاجس العصر أو الجريمة السيبرانيّة التي لم تفرز فقط تحديات تقنية وبشرية وأمنية حديثة، بل كشفت هذه الجريمة عن ثغرات عميقة في قدرة الدول على مواجهتها بشكل منفرد[1].

من هذا المنطلق يأتي هذا الفصل مؤسّسا لطرح عالمي متكامل، ينطلق أوّلا من تحليل طبيعة هذا التهديد الرقمي وخصوصيته التي جعلته محل تكييف جنائي ونقاش فقهي واسع، ثم استقراء المرجعيات القانونية الدولية التي وضعت لمواجهته، بين هذين البعدين يتشكل الإطار المفاهيمي الذي لا غنى عنه لفهم الجريمة السيبرانية وتحديد معالم التعاون الدولي.

المبحث الأوّل: الجريمة السيبرانية بوصفها جريمة عالمية معقّدة.

في ظل الانفجار الرقمي الهائل لم يعد النشاط الإجرامي حبيس الحدود الجغرافية أو الوسائط التقليدية، بل اتخذ لنفسه هيئة متطورة تتخفى خلف الشاشات وتنتشر في الأنساق الشبكية العابرة للسيادات، فقد ظهرت الجريمة السيبرانيّة بوصفها ظاهرة جنائية جديدة متجاوزة كل الأطر الكلاسيكية للجريمة، فيأتي هذا المبحث ليستكنه عمق الجريمة محل البحث من حيث؛ المفهوم والخصائص والتصنيفات، تمهيدا لفهم إطارها القانوني.

[1] – سمير بوثلجة، الجريمة المعلوماتية، مرجع سابق، ص18-20.

المطلب الأوّل: المفهوم العام للجريمة السيبرانية.

رغم حداثة الجريمة السيبرانيّة إلا أنها اعتبرت من أخطر التّحديات القانونية والأمنية في العصر الرقمي، ما استدعى مقاربة مفهومية دقيقة تزيل عنها الغموض وتميّز خصائصها عن الجرائم الكلاسيكيّة، ومنه التّوسع نحو تصنيفها وفق المعايير الدولية المعتمدة[1].

الفرع الأوّل: التعريف اللّغوي والاصطلاحي(الفقهي والقانوني).

في سبيل بناء تصوّر دقيق لمفهوم الجريمة السيبرانية، اقتضت ضرورة البحث العودة إلى الجذور المفهوميّة للمصطلح، واستقراء الرّؤى الفقهية الحديثة قبل الانتقال إلى الضّبط القانوني الدولي والوطني، لما لهذا التحليل من بعد لغوي، وتصوّر فقهي،وتكييف قانونيّ.

أوّلا: التعريف اللّغوي والاصطلاحي للجريمة السيبرانيّة.

يحمل مفهوم الجريمة السيبرانيّة خلفية لغويّة ودلالية متشابكة نابعة من تداخل مصطلحي (الجريمة) والفضاء (السيبراني).

أ- الجريمة لغة: تدل على كل فعل مخالف للعدالة، أو خرق لقاعدة أخلاقية أو قانونية، وتعرف كذلك على أنها الفعل المحضور والمعاقب عليه قانونا[2].

ب- الجريمة اصطلاحا: هي فعل أو امتناع عن فعل يجرّمه القانون ويقدّر له عقوبة جنائية حال ارتكابه من قبل شخص مسؤول[3].

كما أنّها سلوك غير مشروع يصدر عن إرادة جنائية، يتسبّب في إحداث ضرر للمجتمع ويعاقب عليه القانون[4].

---

[1] - اتفاقية بودابست، مصدر سابق، المادة: 22.

[2] - المعجم الوسيط، معجم اللغة العربية، ط4، دار الدعوة، القاهرة، 2004، ص132.

[3] - محمد نجيب حسني، شرح قانون العقوبات-القسم العام- دار النهضة العربية، القاهرة، ط5، 1992، ص81.

[4] - أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دار هومة، الجزائر، ط7، 2013، ص94.

ج- السيبرانيّة لغة: هي كلمة معرّبة من الإنجليزية "cyber" المشتقة من الأصل اليوناني القديم "kuberneles" والتي تعني "الرّبان أو قائد السّفينة" أو "القيادة و التوجيه" وهي الكلمة الأصلية التي اشتق منها مصطلح "cybernetics" في اللغة الإنجليزية والذي استخدمه العالم "نوربرت وينر" في أربعينيّات القرن الماضي، لوصف علم التحكم والاتصال في الكائنات الحية والألة، فمصطلح "cyber" يعادل في اللّغة العربية "الفضاء الإلكتروني أو الرّقمي" وتستخدم "السيبرانية" توصيفا مشتقّا منه للدّلالة على علاقته بالتحكم في الأنظمة الإلكترونية[1].

د- السيبرانيّة اصطلاحا: تشير إلى كل ما يتعلّق بالفضاء الرّقمي والشّبكات والمجالات المرتبطة باستخدام تكنولوجيا المعلومات والاتصال، وما ينشأ عنها من ظواهر قانونية وأمنية تتطلب تشريعا خاصّا[2]، كما أنها؛ مجموعة الوسائل التقنية والأنشطة المرتبطة بالفضاء الرقمي والتي تستعمل في التفاعل، أو التسلّل، أو الاعتداء، بما يشمل كافة الأنشطة الجرمية أو الوقائية في العالم الافتراضي ومنه فالجريمة السيبرانية؛ هي فعل إجرامي ترتكب فيه الجريمة عبر أو ضد نظام معلوماتي، فهي كل سلوك عمدي أو غير عمدي يخل بأمن أو خصوصية أو كفاءة النظام المعلوماتي، ويُرتكب عبر أدوات إلكترونية[3].

ثانيا: التعريف الفقهي للجريمة السيبرانيّة:

يعرف فقهاء القانون الجريمة السيبرانيّة بأنها: كل سلوك غير مشروع يتم عبر الحواسيب أو الشبكات الإلكترونية، يعد خرقا للنصوص القانونية ويمس بحقوق الأفراد أو الجماعات أو يمثل تهديدا لأمن المعلومات أو سلامة الأنظمة الرقمية، وقد اختلفت الصياغات الفقهية بحسب الزاوية التي تُتناول منها الجريمة، فقد عُرفت على أنها؛ " كل سلوك إجرامي يتم عبر وسط معلوماتي يهدف إلى المساس بالأنظمة المعلوماتية أو البيانات المحمية قانونا" وعُرِّفت بأنها: " استعمال

[1] - مجمع اللغة العربية-القاهرة- معجم المصطلحات التقنية، إصدار المنظمة العربية للترجمة، بيروت، 2015، ص177.

[2] - جامعة الدول العربية-الأمانة العامة- المعجم القانوني الموحد للمصطلحات الإلكترونية، القاهرة، 2017، ص61.

[3] - اتفاية بودابست، مصدر سابق 2001، المادة: 2.

التقنيات الحديثة للقيام بسلوك مخالف للقانون، يُرتكب عبر الحواسيب أو أنظمة التشغيل ويمس بالأمن أو الخصوصية أو المال أو السّلامة"[1].

ثالثا: التعريف القانوني للجريمة السيبرانيّة:

عرفت اتفاقية بودابست 2001 وهي المرجع الدولي الأهم من خلال تصنيفها إلى أربعة أنماط رئيسة دون تعريف جامع، وركزت على الأفعال المجرّمة كالدخول غير المشروع إلىالنظم، واعتراض البيانات وتزوير المعطيات.

أما على المستوى الوطني جاء التأطير القانوني للجريمة السيبرانيّة ضمن القانون رقم: 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها؛ "كل فعل معاقب عليه قانونا يُرتكب منظومة معلوماتية"[2]

وتعرّف المعلوماتية في ذات القانون بأنها "كل جهاز أو مجموعة من الأجهزة المترابطة فيما بينها أو المتصلة، التي تسمح بمعالجة آلية للمعطيات أو تخزينها أو إرسالها أو استقبالها أو عرضها"[3]

أما في التشريعات المقارنة، جاء في القانون المصري رقم: 175 لسنة 2018، بشأن مكافحة جرائم تقنيات المعلومات، ليعرف الجريمة السيبرانية بأنها: كل فعل مرتكب باستخدام الحاسب الآلي أو الأنترنت أو غيره من الوسائط الرقمية، يشكل جريمة وفق أحكام هذا القانون أو القوانين الأخرى.[4]

[1] – سامية عبد الوهاب، الجريمة الإلكترونية أو السيبرانية، مذكرة ماستر، 2016-2017، جامعة القاهرة، ص18.

[2] – القانون رقم: 09-04 المادة 2، يتعلّق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد47، الصادرة بتاريخ: 16 أوت 2009، ص2 وما بعدها.

[3] – المرجع نفسه.

[4] – الجريدة الرسمية المصرية، الصادرة بتاريخ: 14 أوت 2018، قانون مكافحة جرائم تقنية المعلومات رقم: 175، 2018. الباب الأول، الأحكام العامة، تعريفات، المادة:15.

كما عرّف قانون مكافحة الجرائم الإلكترونية الأردني رقم: 27 لسنة 2015، الجريمة السيبرانية على أنها؛ كل استخدام غير مشروع أو غير مصرّح به للوسائل التقنية الحديثة بقصد ارتكاب أفعال تُجرمها القوانين النافذة.[1]

الفرع الثّاني: تمييز الجريمة السيبرانية عن غيرها من الجرائم:

الجريمة السيبرانيّة من الظواهر الإجرامية الحديثة التي فرضتها التطورات التكنولوجية والرقمية في العصر الحالي، هذا النوع من الجرائم يتسم بالخصوصية كونها تحدث ي فضاء غير مادي عبر اللاأنترنت، ومنه سنبرز أوجه التشابه والاختلاف، ثم الخصوصية البنوية من خلال هذا الفرع.

أوّلا: أوجه التشابه:

على الرغم من التطورات التكنولوجية التي تميز الجريمة السيبرانيّة، إلا أن هناك العديد من أوجه التشابه بين هذه الجرائم والجرائم التقليدية الأخرى.

أ- يشترك النوعان في الجوهر الأساسي للجريمة والمتمثل في النية الإجرامية، والإضرار بالضحية أو التسلّط على ممتلكات الغير، فالمجرم يسعى إلى تحقيق منفعة غير مشروعة على حساب الضحية من خلال سرقة أموال أو معلومات أو إلحاق الضرر بالممتلكات المادية والمعنوية[2].

ب- إن السلوك الإجرامي في السلوك الرقمي يتخذ أشكالا قد تكون متشابهة في الهدف مع الجرائم التقليدية الأخرى لكن الوسائل تختلف، ففي الجرائم السيبرانيّة يتم استخدام أدوات وتقنيات رقمية لسرقة البيانات أو تنفيذ هجمات إلكترونية، في مقابل ذلك فالجرائم التقليدية نوع من استخدام الوسائل مثل الأسلحة أو أدوات السرقة المباشرة، وعليه فإن الجريمة – سيبرانية كانت أو تقليدية- تتضمّن عملية إجرامية تتسم بالنية الجرمية والضرر المباشر للضحية[3] رغم اختلاف

[1] – الجريدة الرسمية الأردنية، الصادرة بتاريخ: 12 أوت 2023، قانون الجرائم الإلكترونية الأردني رقم: 17 سنة 2015، ع 5911.

[2] – عبير علي محمد النجار، إشراف مازن إسماعيل هنية، جرائم الحاسب الآلي في الفقه الإسلامي، رسالة مقدمة لنيل درجة الماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2009، ص12.

[3] – أحسن بوصقيعة، الوجيز في القانون الجزائري العام، الجزائر، ط5، 2018، ص112.

الوسائل، فهذا التمثيل يوحي بأن الفرق في الأساليب لا يُغني عن كونه ممارسة إجرامية تؤدي إلى التهديد المباشر للمجتمع واقتصاده[1].

ثانيا: أوجه الاختلاف:

أ- لا تعترف بالحدود الدولية: المجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق المكان والزمان دون أن تخضع لحرس الحدود، فلا تحكمها حدود مرتبة أو ملموسة تقف أمامها فهذه الميزة قد أدّت إلى نتيجة أن أماكن متعددة في دول مختلفة تتأثر بالجريمة السيبرانية في آن واحد.[2]

ب- جريمة يصعب اكتشافها: الجريمة السيبرانية في أكثر صورها خفية لا يلحظها الضحية أو يدري حتى بوقوعها[3]، وحين الإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تُسجل البيانات عن طريقها أمرا ليس عسيرا، ففي الكثير من الأحيان يحكم توافر المعرفة والخبرة في المجال الرقمي لدى مرتكبيها.

ج- جريمة يصعب إثباتها: تتم في الفضاء الإلكتروني ولا تتطلّب وجودا ماديا فعليا[4]، فالجريمة السيبرانية تقع في بيئة غير تقليدية؛ أي خارج الواقع المادي الملموس، لتقوم جميع أركانها في بيئة الحاسوب أو الأنترنت مما يجعل الأمور تزداد تعقيدا لأجل ملاحقتها، ففي هذه البيئة تكون البيانات والمعلومات عسيرة الكشف خلافا للجرائم التقليدية فمسرح الجريمة يكون فيها مكشوفا وواضحا لما تُرتّبه من آثار أو تبليغات مباشرة من قبل الضحية، ومنه فمسرح الجريمة السيبرانيّة يتضاءل محور أدلته لسببين:

- الأول: كون الجريمة السيبرانية لا تخلف آثارا مادّية.

[1] - تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة (unod) لعام 2013، ص21.

[2] - نهلا عبد القادر المومني، جرائم المعلوماتية، ط1، 2008، دار الثقافة والتوزيع، الأردن، ص51.

[3] - المرجع نفسه، ص54.

[4] - رضا مهدي، الجرائم السيبرانية وآليات مكافحتها، مجلة النيل للبحوث والدراسات، مجلد6، ع2، 2021، ص114.

– الثاني: بين زمن وقوع الجريمة ووقت اكتشافها مدة طويلة نسبيا، الأمر الذي يعطي الجاني فسحة لتغيير الآثار المادية إن وجدت.

د– أسلوب ارتكابها: على اعتبار أنها جريمة هادئة بطبعها (soft crime) لا تحتاج إلى إلى العنف وإنّما للقدرة على التعامل مع جهاز الحاسوب وتقنيات الفضاء الرقمي، عكس الجرائم التقليدية الواضحة في أسلوب الارتكاب مما تحمله من عنف وقوة بدنية والوسائل (أسلحة بيضاء أو نارية).

هـ– جريمة مستحدثة: في ظل العولمة والتوسع الرقمي فإن التقدم العلمي والتكنولوجي تجاوز قدرات الدول من حيث الرقابة والإمكانيات وكذا تحقيق الأمن السيبراني، هذا الأخير الذي أضعف قدراتها – في تطبيق القوانين– بالشكل الذي أصبح يهدد أمنها، وأفرز إشكالات عديدة وتحديات كبرى على الأمن الدولي من أجل التصدي له.

ثالثا: الخصوصية البنيوية للجريمة السيبرانية:

أحدثت الثورة المعلوماتية نقلة نوعية في طبيعة التفاعلات الاجتماعية والاقتصادية، إلا أنها صاحبت بروز نمط جديد من الجرائم جالب للأنظار يرتكز على طبقة خفية من المجرمين، ويتميز بسمات تجعل منه تحديا معقدا أمام التشريعات والسلطات الوطنية والدولية، سمات سنتناول أبرز خصوصياتها فيما تعلّق بالجريمة السيبرانيّة[1].

أ– الطبيعة غير المادية للجريمة السيبرانيّة: تعد الطبيعة غير المادية من أهم خصائص الجريمة السيبرانية؛ حيث تتم الأعمال الإجرامية في الفضاء الرقمي وباستخدام البيانات والبرمجيات دون الحاجة إلى تدخل مادي مباشر، ويمثل غياب الأثر المادي التقليدي تحديا أمام الكشف عن الجريمة وإثباتها[2].

[1] – نهلا عبد القادر المومني، مرجع سابق، ص58.

[2] – رضا مهدي، مرجع سابق، ص114.

ب– سمة اللّامحدودية: تتميز الجرائم السيبرانية بقدرتها على تجاوز الحدود الجغرافية للدول، مما يخلق صعوبات قانونية تتعلق بالاختصاص القضائي وتطبيق القوانين الوطنية، فبالإمكان أن يُرتكب الفعل الإجرامي في دولة ويقع أثره في دولة أخرى، مما يفرض ضرورة تعزيز التعاون الدولي[1].

ج– السرعة والانتشار: يمتاز العالم الرقمي بسرعة نقل المعلومات ما يساعد على انتشار الأفعال الإجرامية السيبرانية، يحدث هذا في شكل لحظي وعلى نطاق واسع جدّا، مما يؤدي إلى تفاقم الخسائر قبل اكتشاف الجريمة[2].

د– التطور التكنولوجي المستمر: اعتماد الجريمة السيبرانية على بنية تكنولوجية ديناميكية؛ حيث تتطور أدوات وتقنيات الهجوم والدفاع باستمرار مما يستوجب تطوير متواصل في أساليب المواجهة التشريعية والتقنية[3].

هـ– تنوع الضّحايا والأهداف: الجرائم السيبرانية لا تقتصر على الأفراد فقط: بل تمتد إلى الشركات والمؤسّسات الحكومية وكذا البنية التحتية الحيوية، مما يرفع من مستوى التهديد الذي تمثله هذه الجريمة على استقرار الأمن الوطني والدولي[4].

و– تعدد الأطراف الفاعلة: يمكن أن ترتكب الجريمة السيبرانية من قبل أفراد عاديون أو جماعات إجرامية أو منظمات إجرامية، أو حتى جهات رسمية أو دول مدعومة في بعض الأحيان مما يوسع من نطاقها ويجعل من مكافحتها تحديا استراتيجيا.

[1] – عبير علي محمد النجار، مرجع سابق، ص18.

[2] – واجعوط سعاد، مكافحة الجريمة السيبرانية على المستوى الوطني، مجلة البحوث العلمية، المركز الجامعي تيبازة، مج2، ع2، ص419.

[3] – سي حمدي عبد المؤمن، قيرة سعاد، الجريمة الإلكترونية وآليات التصدي لها في القانون الجزائري، مجلة البنيان للدراسات القانونية والسياسية، مج7، ع1، ص 63.

[4] – عبير علي محمد النجار، مرجع سابق، ص13.

الفرع الثّالث: تصنيف الجرائم السيبرانيّة وفقا للمعايير الدّولية:

إن الجرائم السيبرانية ليست فئة واحدة أو نوعا واحدا منفردا؛ بل هي مجموعة من الأفعال الإجرامية اللّامتناهية والتي تتعدد من حيث الوسيلة والتنوع البنوي، من نماذج وغايات وسياقات اجتماعية وسياسية.

أوّلا: تصنيفات تبعا للجرائم التي تستهدف الأنظمة المعلوماتية:

الجرائم السيبرانيّة المعتمدة على التقنية الحديثة هي جرائم لا يمكن ارتكابها إلا من خلال استخدام البيانات وأنظمة الحاسوب، وقد عرّفتها اتفاقية بودابست بأنها: أفعال ترتكب ضد سرّية وسلامة تكنولولوجيا ومعلومات الاتصال؛ بحيث تكون الأنظمة المعلوماتية هي الهدف الأساسي للجريمة وتشمل[1]:

- الوصول غير المشروع إلى الأنظمة (الاختراق).
- التّدخل في البيانات (تعديل أو حذف أو إتلاف البيانات).
- التدخل في الأنظمة (تعطيل أو تدمير الأنظمة).
- إساءة استخدام الأجهزة (استخدام أدوات القرصنة).

ثانيا: تصنيف الجرائم السيبرانيّة وفق المعايير الدولية:

بالاعتماد على المعايير الدولية الخاصة بتصنيف الجرائم السيبرانية تعد شبكة الأنترنت بيئة خصبة لامتداد الجرائم التقليدية إلى الفضاء الرقمي، حيث لم تعد الجرائم مقتصرة على العالم المادي؛ بل أصبحت تُنفّذ عن بعد وبسرعة وانتشار يفوقان كل الحدود، ويبرز هذا النّمط في

[1] - اتفاقية بودابست، الاتحاد الأوربي، 2001، لمكافحة الجريمة السيبرانية، المادة 1.

الجرائم التي ترتكب عبر الأنترنت، بحيث يتحوّل الوسيط الرقمي إلى أداة مركزية لتمكين أو تنظيم الأثر الإجرامي في خرق مباشر لمقتضيات النّظام العام السيبراني[1]، وتتمثل أنواع هذه الجرائم في:

أ- جريمة الابتزاز الإلكتروني (cyber extortion): وهي عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة، أو عادة ما يتم تصيّد الضّحايا عن طريق البريد الإلكتروني أو وسائل التواصل الاجتماعي الاجتماعي المختلفة، وتتزايد جريمة الابتزاز الإلكتروني في ظل تنامي عدد مستخدمي وسائل التواصل الاجتماعي والتّسارع المشهود في أعداد برامج المحادثات المختلفة.

كما تشكل هذه الجريمة مساسا خطيرا بحرية الأفراد وخصوصياتهم الرقمية، وهي مجرّمة دوليا حسب اتفاقية بودابست 2001 في المادة 02 و06[2]، كما نصّ عليها قانون العقوبات الجزائري المعدل بالقانون رقم: 09-04 في المادة 394 مكرر[3].

ب- جريمة النصب والاحتيال الإلكتروني (cybr frand):

تعد جريمة النصب والاحتيال الإلكتروني من أبرز الجرائم السيبرانيّة التي ترتكب عبر الأنترنت، حيث تستغل هذه الجريمة البيئة الرقمية للتغرير بالضحايا وخداعهم بوسائل احتيالية محكمة تهدف إلى سلب أموالهم أو الحصول على منافع غير مشروعة، وهي من الجرائم ذات الطابع الاقتصادي التي انتقلت من المجال التقليدي إلى الفضاء الرقمي مع الاحتفاظ بالنية الجرمية نفسها؛ التدليس، الخداع، الاستيلاء غير المشروع.

كما تعرّف على أنها: " سلوك احتيالي يتم باستخدام أدوات إلكترونية أو عبر شبكة الأنترنت، بقصد خداع الضحية والاستيلاء على أموالها وبياناتها أو منافعها دون وجه حق"[4] ويشير هذا

[1]- بلال حناجرة، الأنترنت والابتزاز الإلكتروني، مكتبة النور الإلكترونية، 2019، ص25، تم الاطّلاع عليه يوم: 29-04-2025، سا18:30

[2]- اتفاقية بودابست، الاتحاد الأوربي، 2001، لمكافحة الجريمة السيبرانيّة، المادة 02 و 06.

[3]- القانون الجزائري، رقم: 04-09 المادة 394 مكرر.

[4]- عبد الله منصور، الجرائم الإلكترونية في القانون الجنائي، دار الفكر الجامعي، الإسكندرية، 2020، ص134.

المفهوم إلى أن الركن المادي للجريمة يتم عبر الوسط السيبراني، بينما يبقى الركن المعنوي قائما على القصد الاحتيالي وسوء النّية.

ج- جريمة تعاطي المخدرات عبر الأنترنت (cyber drug trafficking):

تعد جريمة الاتجار أو تعاطي المخدرات عبر الأنترنت من أبرز مظاهر تطور الجريمة المنظمة في العصر الرقمي، حيث تحول الفضاء السيبراني -لاسيما الويب المظلم[1]- إلى سوق خفي مفتوح للمخدرات، يتم من خلاله الترويج والتوزيع والدفع بسرية تامة، فقد أفرزت التطورات التكنولوجية وسائل حديثة لتجاوز المراقبة الأمنية من خلال استخدام برامج التشفير، والمنصّات الرسمية التي تمكن من إخفاء الهوية والبيانات[2].

تم تصنيف هذه الجريمة ضمن الجرائم السيبرانيّة التي ترتكب عبر الأنترنت، لأن ارتكابها يستلزم بيئة رقمية فقط بوصفها وسيلة للإنجاز دون أن تكون ناتجة عن اختراق أو تدمير نظم معلوماتية كما في الجرائم المعتمدة على الأنظمة.

ثالثا: جرائم سيبرانيّة ذات طابع دولي (التّجسّس-الإرهاب السيبراني):

في ظل التحولات العميقة التي فرضها العالم الرقمي، برزت أشكال من الجرائم العابرة للحدود بأدوات وتقنيات متطورة، وصارت هذه الجرائم أدوات إستراتيجية تُمارس بها الدول والمنظمات أعمال إجرامية دولية مثل: التجسس والإرهاب الرقميان ضمن نطاق ما يعرف بالحرب غير المعلنة.

أ- التجسس السيبراني (من المعلومة إلى الهيمنة): جريمة التجسس السيبراني من أخطر أشكال الجرائم الرقمية، حيث تستهدف الأسرار السيادية والعسكرية والاقتصادية وقد باتت تمثل امتدادا للحروب الباردة لكن بأساليب إلكترونية، فعمليات التجسس الإلكتروني أصبحت تمثل

[1]- الويب المظلم: هو جزء مخفي من الأنترنت لا يمكن الوصول إليه عبر محرّكات البحث التقليدية ويستخدم لأنشطة سرية. المصدر ويكيبيديا، تم الاطلاع عليه يوم: 2025/02/03، على الساعة 19:45 على الوصلة:https : //wikipedia.org/wiki

[2]- لامية طالة، المخدرات الرقمية (جريمة الإدمان الجديد في الفضاء السيبراني)، مجلة الرسالة للدراسات الإسلامية، مج6، ع1، 2020، ص121.

التهديد الأخطر للأمن القومي للدول كونها تستهدف البنى التحتية والمؤسّسات الحيوية[1] وكونها لا تُكتشف بسرعة، ومن أمثلتها برنامج التجسس للكيان الصهيوني (pegasus) الذي استخدم لاختراق هواتف سياسيين وصحفيين وحقوقيين حول العالم بما في ذلك دول عربية.

ب- الإرهاب السيبراني (سلاح الجماعات المتطرّفة): الإرهاب السيبراني أصبح أداة مركزية تعتمدها التنظيمات الإرهابية الحديثة مثل: (داعش والقاعدة) في بث خطاب الكراهية والتجنيد الإلكتروني، وجمع التمويل عبر العملات المشفّرة؛ بل وحتى تنفيذ هجمات رقمية على منشآت أمنية ومدنية، فالإرهاب الإلكتروني بحداثته قد بات جزءا من عقيدة التنظيمات المتطرفة[2] بل ويستخدم كسلاح بديل عندما يعجز عن المواجهة الميدانية.

يكتسب الخطر السيبراني بعدا أكثر خطورة حينما يتم الدمج بين عمليات التجسس والإرهاب ما يؤدي إلى إنتاج شكل جديد من العنف السيبراني القادر على إسقاط أنظمة أو التسبب بكوارث إنسانية.

المطلب الثّاني: الطابع الدولي للجريمة السيبرانيّة وأبعدها القانونية.

في عصر تتشابك فيه المصالح الاقتصادية والسياسية والثقافية عبر الشبكات الإلكترونية، لم تعد الجريمة السيبرانيّة شأنا محليا محصورا في حدود دولة معينة، بل أضحت تمثل تحديا عابرا للحدود والقارّات، فالتعقيدات التقنية لهذه الجرائم وامتدادها عبر النطاق العالمي تفرض على الدول تحديات قانونية عميقة، وهذا ما يستوجب توضيح الطبيعة القانونية والفاعلين الرّئيسيين ومن ثمة توضيح آثارها ومخلّفاتها على الأمن والسلم العالميين.

[1]- غجاتي سهيلة، راهم أميرة، الهجمات السيبرانية وأثرها على تهديدالأمن والسلم الدوليين، مذكرة مكملة لمتطلبات نيل شهادة الماسترفي القانون، كلية الحقوق، جامعة قالمة، 2023-2024، ص 28.

[2]- بولنوار حنان، الإرهاب السيبراني كتهديد للأمن القومي، مذكرة ماستر، جامعة الجزائر2، قسم الحقوق والعلوم السياسية، 2020-2021، ص87.

الفرع الأوّل: الطبيعة القانونية والتقنية للجريمة السيبرانيّة.

تتميز الجريمة السيبرانيّة بكونها ظاهرة ذات طبيعة مزدوجة الدّمج بين البعد القانوني المتعلق بالنصوص والتكييفات الجنائية، والبعد التقني الذي يتصل بالبيئة الرقمية والأدوات المستخدمة في ارتكابها، وهو ما سيتم عرضه من خلال طبيعتها العابرة للحدود، وتعقيدات الاختصاص القضائي، وصعوبات الإثبات[1].

أوّلا: طبيعة الجريمة السيبرانيّة العابرة للحدود:

تعتبر الجريمة السيبرانيّة هاجس العصر فهي واحدة من أكثر التّحديات الأمنية والقانونية تعقيدا في القرن الحالي، وذلك نتيجة انفلاتها من الضوابط الجغرافية التقليدية وتغلغلها في بنى الدولة والمجتمع عبر الوسائط الرقمية، فمن حيث الماهية لا تتقيّد الجريمة السيبرانيّة بحدود وطنية ضيقة، بل تتخذ من الفضاء الرقمي منطلقا، وتصل آثارها إلى مساحات جغرافية متعددة ما يجعلها ذات طبيعة عابرة للحدود بامتياز، وهذا ما يفرض ضرورة التعاون الدولي والقانوني الجنائي المقارن.

ثانيا: تعقيدات الاختصاص القضائي في الفضاء السيبراني:

يعد الاختصاص القضائي في الجرائم السيبرانية من أعقد الإشكالات القانونية التي تواجه الأنظمة الجنائية الحديثة، وذلك بالنظر إلى الطبيعة اللّامركزية وغير المادية للفضاء الرقمي، هذا التداخل يُصعب مهمة القاضي في تحديد أي دولة لها الحق في تسوية النزاع وتملّكها للولاية القضائية، مع أن نطاق القوانين الوطنية مقيد بحدود الدولة وبالتالي لا يمكن لأي دولة أن تفرض قوانينها داخل حدود الدول الأخرى[2]، الأمر الذي يثير تساؤلات حول المبادئ التقليدية للاختصاص مثل: مبدأ الإقليمية، مبدأ شخصية الجانب، مبدأ عينيّة الجريمة، مبدأ العالمية.

[1]- محمد زكي أبوعامر، علي عبد القادر القهوجي، قانون العقوبات، القسم الخاص، دط، دار النهضة العربية، القاهرة، 1993، ص9.

[2]- عبد المنعم محمد مجدي خليفة، التغلب على تضارب الاختصاص في الجرائم الإلكترونية، رسالة ماجستير، الجامعة الأمريكية، القاهرة، 2020-2021، ص59.

ثالثا: صعوبات الإثبات والأدلة الرقمية في الفضاء السيبراني:

صعوبات الإثبات واحدة من أبرز التحديات القانونية البالغة التعقيد نظرا للطبيعة الرقمية للأدلة وتوزّعها عبر عدة نظم معلوماتية وبيئات تقنية تتجاوز الحدود الجغرافية التقليدية، فالأدلة في هذا السياق غالبا ما تكون افتراضية أو زائلة أو قابلة للتعديل أو الإتلاف بسرعة، فالدليل الرقمي مفهوم يحتوي التطور والتنوع ذلك لأن هذا المصطلح يتضمن كافة أشكال وأنواع البيانات الرقمية التي يمكن تداولها رقميا، بحيث تكون بين هذه البيانات والجريمة رابطة أو علاقة منها تلك التي تتصل بالضحية أو المجني عليه على النحو الذي يحقق هذه الرابطة[1].

الفرع الثّاني: الفاعلون الرئيسيون في الجريمة السيبرانيّة:

في ظل تعقيد الجريمة السيبرانية وتوسع رقعتها اللامحدودة، لم تعد تقتصر على فاعل فردي بل أصبحت تشمل أطرافا متنوعة.

أوّلا: الأفراد فاعلون رئيسيون في الجريمة السيبرانيّة:

في زوايا الفضاء الرقمي المظلم يقف الفرد أحيانا خصما لا يقل خطرا على المؤسسات أو الدول بوصفه أحد أخطر الفاعلين في مشهد الجريمة السيبرانيّة، غير أن الحديث عن الأفراد لا يستقيم دون الوقوف على ظاهرة (الهاكرز)[2] التي تحولت من مجرد تجلٍ لمهارات تقنية استثنائية إلى واحدة من أبرز التحديات الأمنية في الوقت الحالي.

فالهاكرز ليسوا جماعة متجانسة، فمنهم من يسلك مسار القبعات البيضاء الذين يستخدمون مهاراتهم لأغراض أخلاقية مثل: اختبار الثّغرات وتأمين الأنظمة، ومنهم من يتخذ مسلك القبعات

[1]- حسام أحمد كيلاني علي، الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون، ع47، أكتوبر 2024، ص49.

[2]- بن عزوز عبد العلي، الجرائم الإلكترونية والتحديات الأمنية في الفضاء السيبراني، دار المعرفة، الرباط، 2021، ص91.

السوداء الذين يخترقون الشبكات لأغراض إجرامية مالية أو سياسية، وتظهر فئة القبعات الرمادية الذين ينتقلون بين الشرعية والخرق وفقا لمواقفهم من النظام أو الضحية[1].

ثانيا: المنظمات الإجرامية السيبرانيّة:

في أعماق الشبكة المظلمة حيث تتوارى الأفعال الإجرامية خلف طبقات التشفير اللامرئية تنشط كيانات تتجاوز فكرة الجريمة العرضية أو الدوافع الفردية، فالجريمة السيبرانيّة لم تعد مجرد اختراقات عشوائية؛ بل تحولت إلى نظام إجرامي محكم له قيادة وتكتيك وتمويل وتوزيع للمهام، فالمنظمات الإجرامية التي تنشط كجيوش خفية منسقة متخصصة ومدعومة برأس مال وخبرة رقمية عالية، حيث تعمل هذه المنظمات بأسلوب عابر للحدود باستثمار أدوات هجومية متقدمة، وتدير منصّات للخدمات الإجرامية الجاهزة مثل: الابتزاز والقرصنة المؤجرة، فهذه الشبكات الإجرامية تمثل العمود الفقري للجريمة السيبرانية المعاصرة، وهي تشمل جماعات مثل: منضمات (darkside revil) التي نفذت هجمات شلّت مؤسسات حيوية في أمريكا وأوربا[2]، ومنظمة (لازاروس– group lazarus) التي اخترقت البنك المركزي البرتغالي، ولا تتوقف هذه المنظمات عند حدود السرقة أو الابتزاز؛ بل تدخل في المشهد الجيوسياسي في هجمات تشل المستشفيات، وأنظمة الطّاقة، والموانئ البحرية، كما أنها تعد امتدادا للجريمة التقليدية لكنها في وسط رقمي[3].

ثالثا: الدول الرّاعية للهجمات السيبرانيّة:

لم تعد الهجمات السيبرانيّة حكرا على جماعات الجريمة المنظمة أو القراصنة الأفراد، بل دخلت الدول ذاتها على الخط بوصفها فاعلا مباشرا أو راعيا غير مباشر لأنشطة اختراق وتجسس رقمي.

---

[1] – المرجع نفسه، ص ن.

[2] – تقرير المركز الأوربي للجرائم السيبرانيّة–اليوروبول– تقييم تهديدات الجريمة المنظمة عبر الأنترنت، 2020، لاهاي، ص12.

. تم الاطلاع عليه يوم 2025/02/20 سا 18:15. https// www.europol.europ.eu/ioctu-2020.

[3] – خلف حسين، الجريمة المنظمة في العصر الرقمي– دراسة قانونية تحليلية، دار السنهوري، بغداد، 2021، ص87.

في مشهد ضبابي من أي وقت مضى، تقف بعض الدول في مفترق الطرق بين الحماية السيبرانيّة الداخلية واستغلال الفضاء الرقمي ساحة خفية للصراع السياسي والاستخباري، تستهدف بها خصومها الاستراتجيين أو إلى ترسيخ هيمنتها السيادية في العالم الرقمي، فالهجمات السيبرانية المدعومة من الدول تُصمّم بعناية لتتجنب الاكتشاف ومن بين المجالات المستهدفة من قبل هذه الدول؛ البرمجيات الحكومية، سلاسل التوريد الرقمية، البيانات الانتخابية... كلها من أجل الضغط السياسي أو الاقتصادي. هناك دول ليست راعيا مباشرا لكنها تُستخدم بؤرة لانطلاق الهجمات وذلك استغلالا لضعف البنية التحتية القانونية لها وغياب قوانين مكافحة الجريمة السيبرانيّة وصعوبات التعاون القضائي الدولي مثل: بعض دول أوربا الشرقية وأفريقيا وآسيا الوسطى، وهناك دول أصبحت ضحية لهجمات من منظمات إجرامية دولية خاصة الدول المتقدمة وهي الأكثر عددا وتشمل الدول الصناعية الكبرى، بغرض سرقة بياناتها والحصول على فدية[1].

رابعا: عمليات إجرامية سيبرانيّة للكيان الصهيوني:

لا يخفى أن الكيان الصهيوني يمثل الأنموذج الأوضح لحرب لا تخاض بوجه مكشوف سواء في ميادين الحرب التقليدية أو عبر الهجمات السيبرانيّة، فقد حوّل الفضاء السيبرني إلى جبهة عدوانية خفية يمارس عبرها كل أشكال الحرب من التجسس والاختراق وقطع الاتصالات، ففي عدوانه المتكرر على قطاع غزة اعتمد على هجمات سيبرانية موجهة لتعطيل شبكات الاتصالات والبث ووسائل البنية الرقمية للقطاع، هذا تزامنا مع قصف المستشفيات والمؤسسات الحيوية لإحداث عزلة كاملة عن العالم الخارجي كما حدث في أكتوبر 2023[2]، وتُتهم أجهزة للكيان مثل: الموساد والوحدة 8200 العسكرية، بتنفيذ عمليات اختراق لمنصات حكومية عربية، والتنصّت على هواتف قادة ومقاومين واستخدام برمجيات تجسسية مثل: (pegasus) التابعة لشركة (NSO) الصهيونية، والتي كشفتها منظمة العفو الدولية في عدة تقارير، هذه الأعمال امتداد للعقيدة

[1] – الجمّال شريف، الأمن السيبراني والصراع الجيوسياسي في الشرق الأوسط، مركز دراسة الخليج، أبو ظبي، 2021، ص56.

[2] – مركز الأبحاث الفلسطيني، العدوان السيبراني على غزة– عزل رقمي ضمن عدوان عسكري، غزة، 2023، ص7.

الصهيونية التي تقوم على الضّربات الاستباقية والاغتيالات الرقمية[1]، وهي جرائم حرب رقمية تضاف إلى سجل الكيان الصهيوني الغاشم الحافل بالانتهاكات.

الفرع الثّالث: آثار الجريمة السيبرانيّة على الأمن والسلم العالميين:

في ظل التحول الرقمي المتسارع أضحى الفضاء السيبراني ساحة مركزية للصراع والنفوذ وتحوّلت الجريمة السيبرانيّة من مجرد اختراقات فردية إلى تهديدات ممنهجة ضد الأمن الوطني والدولي، من خلال هذا الفرع نستعرض الآثار الاقتصادية والاجتماعية على السيادة الوطنية وتأثيرهما على العلاقات الدبلوماسية الدولية.

أوّلا: الأثر الاقتصادي والاجتماعي للجريمة السيبرانيّة:

تخلف الجريمة السيبرانيّة خسائر جسيمة تهدد استقرار الاقتصاد العالمي وتؤثر على استدامة التنمية والأمن المالي للدول ولا تقتصر على الجانب المالي فقط، بل تمتد لتضرب في عمق المجتمعات من خلال الانقسامات الاجتماعية وتقويض الثقة بين المواطن والدولة، وتغذي مظاهر العنف الذي يهدد الأمن الاجتماعي.

الجريمة السيبرانيّة أحد أخطر التهديدات الاقتصادية التي تواجه الدول نظرا للخسائر الفادحة التي تلحقها بالبنى الرقمية والمؤسسات المالية والاقتصادية، حيث يتم استغلال ضعف الحماية السيبرانيّة لاختراق شبكات بنوك مركزية وشركات متعددة الجنسيات مما يؤدي إلى زعزعة الثقة في النظام الاقتصادي الدولي[2]، كما ترقى إلى مستوى التهديد المنهجي للأمن الاقتصادي العالمي واختلال موازين القوى الاقتصادية بين الدول[3].

إلى جانب الخسائر الاقتصادية تُخلف الجريمة السيبرانيّة آثار اجتماعية عميقة تهدد النسيج الاجتماعي للأمم خصوصا عندما تمس قطاعات حساسة مثل التعليم والصحة والمعلومات

[1] – الدجني أسامة، السيادة الرقمية في فلسطين ومخاطر الاحتلال السيبراني، المركز الفلسطيني لأبحاث السياسات، رام الله، 2021، ص22.

[2] – غجاتي سهيلة، راهم أميرة، مرجع سابق، ص 65.

[3] – اتفاقية بودابست، مرجع سابق، المادة 12.

العمومية ونقص الثقة في قدرة الدول على تأمين مواطنيها، فالجريمة السيبرانيّة أصبحت وسيلة فعّالة في إثارة الفتن الطّائفية والتحريض الرقمي عبر مواقع التواصل الاجتماعي، فمواجهة الأثر الاجتماعي للجريمة السيبرانيّة يتطلب مقاربة قانونية شاملة ترعى حماية الحقوق الرقمية للمواطنين وتوازن بين الأمن والحرّيات[1].

ثانيا: تهديد الجريمة السيبرانيّة للسيادات الدولية واستقرارها السياسي:

السيادة الوطنية من أبرز المبادئ المؤسسة للقانون الدولي العام، وتعني تمتع الدولة بالولاية الكاملة على إقليمها وسكانها دون تدخل خارجي، غير أن الجريمة السيبرانيّة باتت تمثل اختراقا مباشرا لهذا المبدأ من خلال استهداف البنى التحتية الحرجة والحساسة، والمؤسسات السيادية مثل وزارة الدفاع والداخلية بما يفضي إلى تعطيل عمل الدولة أو التأثير على إرادتها السياسية خصوصا مع تصاعد الهجمات السيبرانية التي تنفذها جهات فاعلة ترعاها دول، بهدف التجسس أو التأثير في الانتخابات أو ابتزاز حكومات أجنبية أو من أجل خلق فوضى وزعزعة النظام والأمن الوطنيين للدول، فهذه الانتهاكات السيبرانيّة للسيادات الوطنية أضحت نمطا جديدا للحروب الخفية غير المسلحة[2]، ففي ضوء هذه المعطيات أصبح من الضروري تطوير آليات قانونية دولية تعترف بالهجمات السيبرانيّة بوصفها أعمال عدائية تهدد السلم والأمن الدوليين.

ثالثا: التأثير على العلاقات الدولية والدبلوماسية:

تمثل الجريمة السيبرانيّة تحدٍّ ناشئ أعاد تشكيل معادلات القوة والتوازن في العلاقات الدولية، مع تزايد الهجمات الإلكترونية ضد المؤسسات الحكومية الحساسة وسفارات وخوادم وزارات الخارجية، باتت الدول تعتبر الفضاء السيبراني ساحة صراع غير معلنة تؤثر مباشرة في مسارات التعاون، عبر التصعيد الدبلوماسي بين الفاعليين الدوليين، فالهجمات السيبرانية التي تنسب لدولة ما وتلحق ضررا ملموسا بسيادة دولة أخرى قد تعتبر استخداما غير مشروع للقوة، ومنه قد تظهر ردود

[1] – جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010، المادة 05.

[2] – غجاتي سهيلة، راهم أميرة، مرجع سابق، ص 66.

دبلوماسية أو حتى إجراءات مضادة ضمن إطار الشرعية الدولية، فهذه الاعتداءات تعتبر تهديدا مباشرا للثقة المتبادلة بين الدول[1].

المبحث الثّاني: الإطار القانوني الدولي لمكافحة الجريمة السيبرانيّة.

شهد القانون الدولي تطورا ملحوظا في استجابته لتحديات العصر الرقمي لاسيما في ظل اتساع رقعة الجرائم السيبرانية التي تجاوزت الحدود التقليدية للدول وهددت سيادتها وأمنها واستقرار مجتمعاتها، فقد أظهرت هذه الجرائم التي ترتكب عبر الفضاء الرقمي الذي يضاف إلى مجالات البر والبحر والجو والفضاء الخارجي هشاشة البنى القانونية القائمة، وأبرزت الحاجة إلى آليات تنظيمية دولية مرنة وشاملة تتناسب مع الطابع العابر للحدود لهذه الظاهرة.

المطلب الأوّل: الاتفاقيات الدولية لمحاربة الجريمة السيبرانيّة.

مع تحول الجريمة من ميدانها المادي إلى البيئة الرقمية العابرة للحدود، كان لزاما على الدول استحداث أدوات قانونية جديدة تكفل تعقب الجناة وتجاوز العقبات السيادية وتنسق الجهود العابرة للقارّات، وقد أسفر هذا التحدي عن ولادة منظومة من الاتفاقيات الدولية والإقليمية لتشكل حجر أساس في المعركة القانونية ضد الجريمة السيبرانيّة، وتفتح آفاقا غير مسبوقة للتعاون القضائي والتقني[2]، لنقف في هذا المطلب وقفة تحليلية لأهم الاتفاقيات انطلاقا من اتفاقية بودابست الرائدة مرورا بدور الأمم المتحدة وجهودها وصولا إلى الأدوار التي تضطلع بها منظمات إقليمية ودولية في سد الفجوات القانونية.

الفرع الأوّل: اتفاقية بودابست.

تعد اتفاقية بودابست أول صك دولي ملزم يهدف إلى مكافحة الجريمة السيبرانية، وقد تم اعتمادها من قبل مجلس أوربا بتاريخ: 23 نوفمبر 2001 في مدينة بودابست عاصمة المجر،

[1] – UNODC، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الجرائم الإلكترونية، الوحدة 7، التعاون الدولي ضد الجرائم الإلكترونية.

[2] – لخضر دهيمي: النظام القانوني لعمل الشرطة في الجزائر، أطروحة دكتوراه في الحقوق، جامعة البليدة 2، 2014-2015، ص245.

ودخلت حيّز التنفيذ في جوان 2004، تهدف إلى معالجة الجرائم التي ترتكب عبر النظم المعلوماتية حيث أصبحت مرجعا دوليا معتمدا للتشريعات الوطنية[1].

أولا: الخلفية القانونية والضرورات الدولية:

جاءت اتفاقية بودابست استجابة حتمية للتطور السريع لتقنيات المعلومات والاتصالات وما نجم عنه من جرائم جديدة تتسم بالعالمية واللامادية لاسيما تلك التي تستهدف نظم المعلومات أو تُرتكب من خلالها، وقد أدرك مجلس أوربا بالتنسيق مع دول غير أوربية، أن غياب إطار قانوني موحد يعوق التعاون الدولي ويعطل التحقيقات ويمنح الجناة مساحة للإفلات من العقاب، منه تم وضع هذه الاتفاقية لتوحيد التشريعات الوطنية في مجال مكافحة الجرائم المعلوماتية وتحديد آليات التعاون القضائي العابر للحدود، مع مراعاة حماية حقوق الإنسان والحريات الأساسية.

ثانيا: المحاور الأساسية للاتفاقية ومجالات التجريم:

تضمنت الاتفاقية أربعة فصول رئيسة:

أ- الفصل الأوّل تضمن تعريفا للمصطلحات الأساسية في نص المادة 01.

ب- الفصل الثاني جاء تحت عنوان: الخطوات الواجب اتخادها على الصعيد الوطني وانقسم إلى ثلاثة أقسام[2]:

- القسم الأوّل: المواد التي تعالج النصوص الموضوعية لجرائم الحاسوب من المادة 02 إلى 13.

- القسم الثّاني: يضم المواد التي تتعلق بالقواعد الإجرائية من المادة 14 إلى 21.

- القسم الثّالث: يتعلق بالاختصاص، المادة 22.

[1] - اتفاقية بودابست، مصدر سابق، المعاهدة رقم: 185.

[2] - الطاهر باكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، مج4، ع4، 2022، ص22.

ج- الفصل الثّالث: جاء تحت عنوان: التعاون الدولي من المادة 23 إلى 35.

د- الفصل الرّابع: تضمّن الأحكام الختامية من المادة 36 إلى 48.

وقد غطّت الاتفاقية أربعة محاور تشريعية رئيسة:

أ- الجرائم الموجهة ضد نظم المعلومات.

ب- الجرائم المرتكبة عبر الحاسوب.

ج- الجرائم ذات المحتوى غير المشروع.

د- الجرائم المتعلقة بانتهاك حقوق الملكية الفكرية.

تهدف الاتفاقية إلى إرساء حد أدنى مشترك من التجريم بين الدول، مع الحفاظ على هامش التقدير الوطني بما يسهل التعاون القضائي[1].

ثالثا: الأثر الدولي والانتقادات الموجهة للاتفاقية:

رغم أن الاتفاقية نشأت في إطار أوربي إلا أن طبيعتها المفتوحة للانضمام مكنتها من تجاوز الحدود الجغرافية لتشمل دولا من مختلف القارات مثل: الولايات المتحدة وكندا واليابان، بينما امتنعت دول أخرى مثل: الصين وروسيا، لأسباب تتعلق بسيادتها الرقمية ومخاوفها من التجسس.

كما وُجهت لها عدة انتقادات تتعلق بانتهاك الخصوصية الرقمية وتسع صلاحيات أجهزة التحقيق وغياب التوازن الكافي بين الأمن وحقوق الإنسان، كما يدعو البعض إلى تحديث الاتفاقية أو صياغة بديل دولي شامل يتسم بالتمثيل الجغرافي العادل[2].

[1] - التقرير التفسيري لاتفاقية بودابست، مجلس أوربا لاتفاقيات الجريمة السيبرانية، المعاهدة رقم: 185، 2001، فقرات من 01 إلى 20.

[2] - مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة حول الجريمة السيبرانيّة، 2013، الفصل 04.

الفرع الثّاني: دور الأمم المتحدة في مكافحة الجريمة السيبرانيّة.

تزايدت أهمية الأمم المتحدة في مكافحة الجرائم السيبرانيّة مع تصاعد المخاطر الناجمة عن إساءة استخدام الفضاء الإلكتروني، وذلك لما تسببه من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء، وإيمانا منها بأن منع هذه الجرائم يتطلب استجابة دولية في ضوء الأبعاد الدولية لإساءة استعمال الفضاء الرقمي والجرائم المتعلقة به، ونظرا لمجهوداتها الفعّالة كانت فاعلا مركزيّا في الدفع نحو اعتماد رؤية جماعية متوازنة وشاملة لمواجهة هذا التحدي العالمي[1].

أوّلا: البعد المؤسساتي لدور الأمم المتحدة في مواجهة الجريمة السيبرانيّة:

اضطلعت الأمم المتحدة عبر مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) بدور محوري في دعم قدرات الدول الأعضاء على مستوى السياسات والتشريعات، فعملت على تقديم الدعم الفني، وتقديم برامج تدريبية وإعداد أدوات قانونية مرجعية تساعد الدول على بناء استجابات فعالة ضد الجريمة السيبرانية[2]، ومن أبرز هذه المساعدات إصدار الدراسة الشاملة حول الجريمة السيبرانيّة سنة 2013 التي اعتبرت من الوثائق المرجعية الأساسية في رصد الفجوات القانونية والمؤسساتية، وتحليل أنماط الجرائم السيبرانيّة وتحديد أولويات التعاون الدولي في مواجهتها[3]، كما تناولت قضية الجريمة السيبرانية في مؤتمراتها الدولية حول منع الجريمة والعدالة الجنائية مثل: المؤتمر 12 (2010 البرازيل) والمؤتمر الدولي 13 (2015 الدوحة) حيث تم التأكيد على التعاون الدولي لمكافحة هذه الجرائم[4]، والمؤتمر 14 (2021 كيوتو) الخص بالابتكارات التكنولوجية وأثرها على الجريمة السيبرانيّة.

---

[1]- قطاف سليمان، بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقصادية، مج5، ع2، 2022، ص73.

[2]- الجمعية العامة للأمم المتحدة، القرار 74/247 بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصال لأغراض إجرامية، 2019.

[3]- تقرير مكتب الأمم المتحدة (UNODC) حول الجريمة السيبرانية، 2013، الفصل 04.

[4]- الأمم المتحدة، إعلان الدوحة بشأن منع الجريمة والعدالة الجنائية في أجندة الأمم المتحدة الأوسع، المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية، الدوحة، 2015.

ثانيا: المبادرات التشريعيّة والإجرائية للأمم في مكافحة الجريمة السيبرانيّة:

لعبت الأمم المتحدة دورا دبلوماسيا وتشريعيا مهما في تعزيز الحوار الدولي بشأن وضع اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيا المعلومات لأغراض إجرامية، وقد توج هذا التوجه بصدور القرار الأممي رقم: 74/247 عن الجمعية العامة سنة 2019 وتمثل هذه المبادرات محولة لتطوير إطار قانوني عالمي بديل أو مكمل لاتفاقية بودابست يأخذ بعين الاعتبار مصالح الدول التي تنظم له خاصّة من بلدان جنوب العالم.

ثالثا: الرؤية الأممية المتوازنة بين الأمن السيبراني وحماية الحقوق الرقمية:

تسعى الأمم المتحدة من خلال مبادراتها إلى بناء توازن دقيق بين مقتضيات الأمن السيبراني وحماية الحقوق والحريات الرقمية بما يجنب الانزلاق نحو المراقبة الشاملة أو الاستخدام السياسي للتكنولوجيا، ويعد هذا التوجه الأممي ناضجا في رؤيته ومنفتحا على تعددية النماذج القانونية مما يمنحه مشروعية واسعة ويؤهله ليكون أساسا لاتفاق دولي جامع يسد الفراغ التشريعي ويعزّز فعالية التعاون القضائي في المجال السيبراني[1].

الفرع الثّالث: الاتفاقيات الإقليمية الأحرى (الاتحاد الأوربي، الاتحاد الأفريقي، الدول العربية).

أمام تصاعد الطبيعة العابرة للحدود للجريمة السيبرانيّة اتجهت التكتلات الإقليمية إلى صياغة اتفاقيات خاصة بها من أجل مواكبة التحديات التي تفلاضها بيئتها القانونية والتقنية والسياسية، وقد شكلت هذه المبادرات الإقليمية خطوة مهمة نحو تعزيز التعاون العابر للحدود وسد الثّغرات التشريعية.

[1]- اتفاقية بودابست، مصدر سابق، المادة 32.

أوّلا: الاتحاد الأوربي:

سعى الاتحاد الأوربي إلى تبني منظومة شاملة من السياسات التشريعية والمؤسساتية لمواجهة هذا التهديد المتزايد فقد تبنى استراتيجية الأمن السيبراني الأولى سنة 2013 والتي تعد إطارا مرجعيا لتنسيق جهود الدول الأعضاء وتعزيز قدراتها في الوقاية من التهديدات المعلوماتية، وتم تحديث هذه الاستراتيجية باصدار ثان عام 2020، ركزت على تطوير البنى التحتية الرقمية وتبادل المعلومات بين الدول الأوربية[1].

في ذات السياق أصدر الاتحاد توجيه (nis رقم 2016/1148) وهو أول تشريع أوربي ملزم في مجال الأمن السيبراني بشأن أمن الشبكات ونظم المعلومات[2]، إلى جانب الإطار التشريعي أنمشأ الاتحاد الأوربي هيئات متخصصة أبرزها وكالة الأمن السيبراني (ENISA) التي تقوم بتقديم الدعم التقني للدول الأعضاء وتنسيق التدابير الوقائية للحوادث السيبرانيّة، كما أنشأ الاتحاد المركزي الأوروبي للجرائم السيبرانية (EC3) التابع لوكالة اليوروبول سنة 2013 بهدف تنسيق التحقيقات المعقدة ودعم التعاون القضائي والشرطي العابر للحدود[3].

من خلال هذه الآليات يتضح أن الاتحاد الأوربي التزم بتبني مقاربة متعددة الأبعاد لمواجهة الجريمة السيبرانيّة.

[1]- المفوضية الأوربية، إستراتيجية الإتحاد الأوربي للأمن السيبراني- فضاء إلكتروني مفتوح وآمن ومضمون- بروكسل، 2013، النسخة المحدثة، https// eur.lex.europa.eu.2020 تم الاطلاع عليه يوم: 2025/02/22 سا 17:30.

[2]- توجيه البرلمان الأوربي والمجلس رقم: 2016/1148، المؤرخ في: 06 جوان 2016، تدابير تحقيق مستوى عال من أمن الشبكات ونظم المعلومات في اتحاد الاتحاد. https//eur.europa.eu/eli/dit2016 تم الاطلاع عليه يوم: 2025/02/22 سا 18:15.

[3] - وكالة يوروبول، تقرير المركز الأوربي للجرائم اليبرانية، الموقع الرسمي، 2013.

ثانيا: جهود الاتحاد الأفريقي:

سعى الاتحاد الأفريقي إلى صياغة إطار قانوني قاري ينظم الفضاء الرقمي ويعزز الأمن السيبراني، وقد توجت هذه الجهود بإصدار اتفاقية (مالابو) حول الأمن السيبراني وحماية البيانات الشخصية سنة 2014 وهي أوّل وثيقة إقليمية مُلزمة في أفريقيا تهدف إلى مواجهة الجريمة السيبرانيّة[1].

تجسد اتفاقية مالابو تحولا نوعيا في تعاطي الدول الأفريقية مع الأمن الرقمي، إذ تنص على تجريم الأفعال السيبرانية مثل: الدخول غير المشروع، واعتراض المعطيات، وهي خطوة تقدمية لتعزيز البنية التشريعية والقضائية والأمنية[2]، على الرغم من أنها لم تدخل حيز التنفيذ بعد إلا أن التعاون قائم بين الاتحاد الأفريقي وشركائه الدوليين لاسيما مكتب الأمم المتحدة (UNODC) من مبادرات دعم لبناء قدرات الدول الأفريقية في هذا المجال[3].

ثالثا: الدول العربية:

سعت جامعة الدول العربية إلى تعزيز تعاون الدول الأعضاء لمواجهة هذه الظاهرة العابرة للحدود من خلال اعتماد اتفاقية عربية ملزمة، وقد أقر مجلس وزراء العدل العرب سنة 2010 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي تمثل إطارا قانونيا إقبيميا يسعى إلى توحيد التشريعات الجنائية العربية في مجال الجرائم السيبرانيّة[4]، وقد تناولت الاتفاقية في صلبها مختلف الجرائم المرتكبة عبر الوسائل الإلكترونية مثل الدخول غير المشروع، والاحتيال المعلوماتي كما نصّت على آليات التعاون في مجال تبادل المعلومات وتسليم المدرمين والتحقيقات المشتركة.

[1]- الاتحاد الأفريقي، اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو) 2014. https//au.int/enLtreaties/african-union-cokventio. تم الاطلاع عليه يوم: 2025/02/25 سا 16:30.

[2]- بوفليح محمد السعيد، أطر التعاون الدولي للتصدي للتهديدات السيبرانية، مجلة الدراسات القانونية التطبيقية، جامعة قسنطينة1، 2024، ص6

[3]- UNODC، تقرير مكتب الأمم المتحدة ومفوضية الاتحاد الأفريقي لتعزيز قدرات الدول الأفريقية، 2021، مرجع سابق.

[4]- جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم المعلومات، مجلس وزراء العدل العرب، 2010، مرجع سابق.

وقد بادرت جامعة الدول العربية إلى تنظيم ورشات تدريبية ولقاءات إقليمية تهدف إلى رفع كفاءة الأجهزة القضائية والأمنية في مواجهة الجرائم السيبرانيّة بالتعاون مع منظمات أوربية مثل الإسكوا (ESCWA) ومكتب الأمم المتحدة (UNODC) إلا أن هذه الاتفاقية تغلب عليها الصيغة العمومية وتفتقر إلى الآليات التنفيذية مقارنة بالاتفاقيات الدولية[1].

المطلب الثّاني: التشريعات الوطنية ودورها في مكافحة الجريمة السيبرانية.

تعد التشريعات الوطنية الركيزة القانونية الأساسية في مواجهة التحدياتن التي تفرضها الجريمة السيبرانية في العصر الرقمي، إذ تضطلع بدور محوري في تجريم الأفعال الإلكترونية وتحديد المسؤوليات وإرساء آليات التحقيق والملاحقة، غير أن تفاوت مقاربات الدول في هذا المجال من حيث المفاهيم والعقوبات وأدوات الإثبات، أدى إلى بروز إشكالات حقيقية أمام فعالية التعاون الدولي، على هذا الأساس فإن دراسة التشريعات الوطنية يعد أمرا جوهريا لفهم مكامن القصور والنقاط المشتركة وتقييم أثرها.

الفرع الأوّل: المقارنة بين قوانين بعض الدول في مكافحة الجريمة السيبرانيّة.

تظهر مقارنة التشريعات الوطنية حول الجريمة السيبرانية تباينا وضحا في النهج القانوني سواء من حيث التعريفات أو آليات التجريم أو العقوبات، ما يعكس التفاوت في الاستجابة التشريعية لمخاطر الفضاء السيبراني، وفيما يلي نستعرض نماذج قانونية عند بعض الدول مع التركيز على الاتجاهات العالمية.

أولا: النموذج الأوربي (ألمانيا، فرنسا):

اعتمدت ألمانيا وفرنسا مقاربات متقدمة في مكافحة الجريمة السيبرانية، حيث أدخلت ألمانيا تعديلات متقدمة على قانون العقوبات الألماني (STGB) بموجب المادة 202 وما يليها لتجريم

[1]– عواد محمد، الجهود القانونية العربية لمكافحة الجريمة السيبرانيّة– بين الطموح والتنفيذ، مجلة دراسات الجريمة السيبرانية، مج2، ع1، ص41.

الدخول غير المشروع، وعمليات التنصت وتعطيل النظم المعلوماتية، كما أنشأت هيئة (BSI) المتخصصة في أمن المعلومات والتي تلعب دورا في الوقاية والتنسيق[1].

أما فرنسا فقد عززت تشريعاتها عبر قانون الأمن الداخلي وقانون العقوبات الفرنسي إلى جانب تبنيها استراتيجية وطنية للأمن السيبراني، أنشأت بموجبها الوكالة الوطنية لأمن نظم المعلومات (ANSSI) كما تعد فرنسا من الدول الرائدة في اعتماد التوجيه الأوربي (NIS) ضمن تشريعها الداخلي[2].

ثانيا: النموذج الآسيوي (الصين، الهند):

تتبنى الصين نهجا صارما ومركزيا في تشريعات الأمن السيبراني، حيث يعد قانون الأمن السيبراني لعام 2017 من أكثر القوانين شمولا، وينص على سيطرة الدولة على البيانات والبنى التحتية الحساسة، ويمنح صلاحيات موسعة للسلطات في المراقبة والحجب[3].

أما الهند فقد شرعت قانون تكنولوجيا المعلومات لسنة 2000 (ITACT) بوصفه أداة رئيسة لمكافحة الجرائم الإلكترونية سنة 2008 ويعد من أوائل التشريعات في جنوب آسيا التي تعلج مسائل الجرائم السيبرانية[4].

[1]- المكتب الاتحادي لأمن المعلومات في ألمانيا(BSI) https//www.europarabet.de تم الاطلاع عليه يوم:2025/02/27 سا 20:15.

[2]- الوكالة الوطنية لأمن نظم المعلومات في فرنسا(ANSSI) الموقع الرسمي. https//www.diptomati.fr تم الاطلاع عليه يوم: 2025/02/27 سا 20:45.

[3]- قانون الأمن السيبراني لجمهورية الصين الشعبية 2017. https//www.youm7.com تم الاطلاع عليه يوم: 2025/02/27 سا 21:05.

[4]- قانون تكنولوجيا المعلومات الهندي 2000، المعدل في 2008، وزارة الإلكترونيات وتكنولوجيا المعلومات، الموقع الرسمي. https//www.meity.gov.in تم الاطلاع عليه يوم: 28 أفريل 2025 سا 12:00

ثالثا: الاتجاهات العربية (الجزائر، مصر، العراق):

نشهد التشريعات العربية تطورا ملحوظا وإن كان متفاوتا، ففي الجزائر صدر القانون 18-04 المؤرخ في: 10 ماي 2018 المتعلق بحماية الأشخاص من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ويتضمن فصولا متخصص في التجريم والتحقيق والعقوبات[1].

أما مصر فقد أقرت القانون رقم: 175 سنة 2018 بشأن مكافحة جرائم تقنية المعلومات، والذي يتضمن عقوبات مشددة على الجرائم المرتكبة عبر الأنترنت، ويعد من أبرز التشريعات العربية من حيث الشمول[2]، وفي العراق أصدر مجلس النواب مسودة قانون الجرائم المعلوماتية لعام 2022 والتي أثارت جدلا واسعا بسبب مخاوف تتعلق بحرية التعبير والخصوصية رغم الحاجة الملحة لتنظيم الفضاء الرقمي في ظل هشاشة البنية التشريعية[3].

رغم أهمية دور التشريعات الوطنية في مواجهة الجرائم السيبرانيّة وتطورها الملحوظ إلا أنها تبقى غير كافية من حيث التفاوت في المعايير والمفاهيم القانونية وكذا القصور التكنولوجي والتقني وضعف حماية الحقوق والحريات.

الفرع الثّاني: أثر اختلاف التشريعات على التعاون الدولي.

يعد التعاون الدولي أحد الركائز الأساسية في مكافحة الجرائم السيبرانيّة نظرا للتطور التقني والفني لهذا التهديد العابر للحدود، غير أن تباين الأطر التشريعية الوطنية يطرح تحديات جوهرية أمام فعالية هذا التعاون من حيث المفاهيم القانونية، والأطر الإجرائية ، وأسس تجريم الأفعال السيبرانيّة.

[1] – الجريدة الرسمية الجزائرية، الصادرة بتاريخ: 07 جوان 2018، القانون رقم: 18-04 المؤرخ في: 10 ماي 2018. 2018.

[2] – القانون المصري رقم: 175 لسنة 2018، مكافحة جرائم تقنية المعلومات الصادر بتاريخ: 14 أوت 2018.

[3] – تقرير مجلس النواب العراقي، مسودة قانون مكافحة الجرائم المعلوماتية 2022.

أوّلا: التفاوت في تعريف الجريمة السيبرانية:

يعد غياب تعريف موحد للجريمة السيبرانيّة في التشريعات الوطنية من أبرز العوامل التي تعيق التعاون بين الدول[1]، حيث تعتمد بعض القوانين على تعريفات تقنية ضيقة، بينما توسع أخرى المفهوم ليشمل الأفعال ذات الطابع المعلوماتي، هذا التباين يؤدي إلى الصعوبة في تطبيق مبدأ التجريم المزدوج، وهو شرط أساسي في التجريم والمساعدة القانونية المتبادلة.

ثانيا: اختلاف النظم الإجرائية وأثره في تسهيل المساعدة القانونية المتبادلة:

تعتمد بعض الدول نظما إجرائية صارمة تتطلب قرارات قضائية لتبادل البيانات الرقمية أو مراقبة الأنشطة السيبرانية، بينما تسمح أخرى بالإجراءات الإدارية التشريعية[2]، هذا التباين يبطئ الاستجابة في القضايا السيبرانية التي تتطلب سرعة في التتبع وجمع الأدلة قبل صياغتها، كما تثير هذه الاختلافات مخاوف من انتهاك خصوصية الأفراد في حال التعامل مع دول لا تحترم الضمانات القانونية.

ثالثا: الحاجة إلى مواءمة تشريعية لتحقيق الأمن السيبراني العالمي:

في ظل تزايد التهديدات السيبرانيّة العالميّة أصبحت الحاجة إلى مواءمة السياسات والتشريعات الوطنية مع الاتفاقيات الدولية والإقليمية، مثل اتفاقية بودابست، فقد أوصت عدة منظمات دولية مثل الاتحاد الأوربي والأمم المتحدة بضرورة اعتماد أطر تشريعية متناغمة تسمح بتوحيد إجراءات الملاحقة القضائية، وتبادل الأدلة والمعلومات بشكل آمن وقانوني[3].

[1]- علي قويدري، أمال العايش، الجريمة السيبرانية مفهومها وسبل الوقاية منها، مجلة نوميروس الأكاديمية، مج3، ع1، 2022، ص 193.

[2]- تقرير مكتب الأمم المتحدة، مرجع سابق، ص200.

[3]- تقرير مكتب مجلس أوربا، المبادئ التوجيهية للتعاون بين أجهزة إنفاذ القانون ومزودي خدمات الأنترنت، 2008.

الفرع الثّالث: جهود الدول في تطوير قوانين مكافحة الجريمة السيبرانيّة.

أمام التحول الرقمي العالمي وتنامي التهديدات السيبرانيّة وتعقّد تقنياتها، أدركت الدول الحاجة الماسة لتحديث أطرها القانونية الوطنية ليس لمواكبة تطور الجريمة السيبرانيّة فحسب، بل لتعزيز فعالية التعاون الدولي أيضا، ومنه سنوضّح تبني الدول لنماذج تشريعية جديدة وإصلاح تشريعاتها من أجل تيسير التعاون الدولي.

أوّلا: تبني الدول لنماذج تشريعية من الاتفاقيات الدولية:

أقدمت عدة دول على تبني قوانين وطنية مستوحاة من اتفاقية بودابست 2001 التي تشكل الإطار الدولي الأبرز في هذا المجال وتكييفها مع تشريعاتها الوطنية لضمان توافق القواعد القانونية مع متطلبات التعاون الدولي، فقد اعتمدت اليابان قانون الجرائم الإلكترونية الذي يُجرم الاختراق والتجسس السيبراني، كما اعتمدت كندا وأستراليا أحكاما متقاربة تُجرّم الدخول غير المشروع واعتراض البيانات وتخريب الأنظمة، إن انسجام التشريعات مع المعايير الدولية يزيد من سرعة التحقيقات العابرة للحدود ويسهل مشاركة الأدلة الرقمية بين الدول الأعضاء[1].

ثانيا: إصلاح التشريعات لتيسير التعاون القضائي العابر للحدود:

كثيرة هي الدول التي عدلت قوانينها لإزالة العقبات التي تعرقل التعاون القضائي، حيث قامت دول الاتحاد الأوربي بموجب توجيه (NIS2) لعام 2022 بفرض التزام على الأعضاء بإنشاء سلطات وطنية مستقلّة للأمن السيبراني وتحديد نقاط اتصال لتعزيز تبادل المعلومات بشأن التهديدات والهجمات السيبرانيّة، كما خطّت بنفس النّهج سنغافورة وكوريا الجنوبية نصوصا صريحة في قوانينها، تنظم المساعدة القانونية المتبادلة وتسليم المجرمين في القضايا الإلكترونية[2]، إن

[1]- تقرير منظمة التعاون الاقتصادي والتنمية (OFCD)إطار سياسات الأمن الرقمي، 2022، ص17. https//www.oecd.org/content/damLoecd/ reports/2022. تم الاطلاع عليه يوم: 2025/02/28 سا 19:30

[2]- المعهد الدولي للسلام، تقرير عن الجريمة السيبرانية العابرة للحدود والاستجابات القانونية العالمية، 2021، ص4. https//www.ipnst.org/wp.com.tent.convention.pdf تم الاطلاع عليه يوم: 2025/02/28 سا 19:45.

التعاون القضائي الفعال بين الدول يعتمد على تشريعات واضحة تحكم الاتصالات العابرة للحدود، وتوفر آليات جمع الأدلة الرقمية بشكل سريع وفعال.

ثالثا: التجربة العربية في تطوير التشريعات الوطنية لمواكبة التعاون الدولي:

في إطار الجهود الدولية من أجل تطوير قوانينها في مكافحة الجريمة السيبرانيّة وتسهيل التعاون الدولي قامت بعض الدول العربية بتسجيل تطورات هامة في تحديث تشريعاتها بما ينسجم مع التوجهات الدولية[1]، فقد أصدرت الجزائر قانون مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب الأمر رقم: 09-01 سنة 2009 متضمنا مواد حول تسليم المجرمين والتعاون القضائي، كما سنّت مصر القانون رقم: 175 سنة 2018 الذي يشمل خصوصا تنظيم التعاون مع السلطات الأجنبية في جرائم الأنترنت، كما اعتمدت الإمارات العربية المتحدة تعديلات متكررة على قانونها الاتحادي رقم: 05 سنة 2012 لضمان مرونته واستجابته للمتطلبات الدولية[2].

إن تفاوت مستوى التطوير القانوني بين الدول لا يزال يعيق التكامل الإقليمي والتعاون الدولي في غياب تشريعات متوافقة.

[1] – المنظمة العربية لتكنولوجيا الأعلام والاتصال والمعلومات – دراسة حول الاستراتيجية العربية للأمن السيبراني– (2023-2027)

[2] – دراسة حول الإطار القانوني للأمن السيبراني في دول مجلس التعاون الخليجي، مجلة دراسات الخليج والجزيرة العربية، ع113، 2018، ص52.

خلاصة الفصل الاول:

الجريمة السيبرانية تمثل تحديًا قانونيًا وأمنيًا غير مسبوق، نظرًا لطابعها اللامادي والعابر للحدود. فهي تختلف جوهريًا عن الجرائم التقليدية من حيث الفاعلين، الوسائل، والآثار، مما يستدعي فهمًا دقيقًا لطبيعتها التقنية والقانونية. كما تبيّن أن التعدد في تصنيفاتها دوليًا يعكس تعقيدها وتشعّب صورها. وقد أظهر التحليل أن الطابع الدولي للجريمة السيبرانية يجعل من التعاون بين الدول ضرورة لا خيارًا، لاسيما مع تورط أطراف من دول مختلفة في الفعل الإجرامي.

على الصعيد القانوني، فإن الإطار الدولي لا يزال غير موحد رغم وجود اتفاقيات مثل بودابست ومبادرات الأمم المتحدة، في ظل تباين واضح في التشريعات الوطنية وغياب تجانس قانوني دولي شامل. هذا التفاوت يشكل عائقًا فعليًا أمام تنسيق الجهود لمواجهة الجريمة. وتخلص الدراسة إلى أن أي مكافحة فعالة تتطلب مقاربة شاملة قائمة على تنسيق قانوني دولي، وتطوير التشريعات الداخلية بما يتوافق مع المعايير العالمية، مع تعزيز الإرادة السياسية للتعاون في مواجهة هذا الخطر الرقمي المتزايد.

الفصـــــــل الثاني

ميكانيزمات التعاون الدولي في مكافحة الجريمة السيبرانية وتحدياتها

الفصل الثاني: ميكانيزمات التعاون الدولي في مكافحة الجريمة السيبرانية وتحدياتها.

يشكل التعاون الدولي حجر الزاوية في التصدي للجريمة السيبرانية التي باتت تتجاوز الحدود الجغرافية والسيادية للدول، مما أفرز تحديات قانونية وأمنية معقدة أمام الأنظمة التقليدية. ومع تسارع وتيرة الابتكارات التكنولوجية، أصبح من الضروري إرساء آليات تعاون متينة بين الدول، تشمل تبادل المعلومات، وتوحيد التشريعات، وتعزيز القدرات التقنية. وفي هذا السياق، تسعى العديد من الدول والمنظمات الإقليمية والدولية إلى تفعيل شراكات متعددة المستويات لمواجهة هذا التهديد العابر للحدود. ويستند هذا التعاون إلى أطر قانونية دولية، أبرزها اتفاقية بودابست الى جانب المبادرات الإقليمية والمنظمات الدولية تطرقنا في هذا الفصل الى مبحثين. تناولنا في المبحث الأول الميكانيزمات المؤسساتية والتقنية للتعاون الدولي من خلال استعراض مبادئ التعاون القضائي ودور الهيئات الإقليمية ثم المبحث الثاني فيخصص لتحليل التحديات التي تعترض هذا التعاون مع التعزيز بالحلول القائمة.

المبحث الأول: الميكانيزمات المؤسساتية والتقنية للتعاون الدولي.

لم تعد مكافحة الجريمة السيبرانية ممكنة من خلال الجهود الفردية للدول أو المؤسسات، بل أضحت تستلزم نسقًا تعاونيًا مركبًا يقوم على ميكانيزمات مؤسساتية وتكنولوجية دقيقة. فالتداخل بين الاختصاصات، وتعدد مسارح الجريمة، وسرعة التطور الرقمي، كلها عوامل فرضت إعادة تشكيل أدوات التعاون الدولي. وبناءً عليه، يتناول هذا المبحث مقومات هذا التعاون من خلال المطلب الأول المعني بالتعاون الأمني والقضائي بين الدول، ثم المطلب الثاني الذي يعالج أبعاد الشراكة الفاعلة بين القطاعين العام والخاص.

المطلب الأول : دور الأنتربول واليوروبول.

إن التعاون الأمني والقضائي بين الدول ضرورة حتمية في مواجهة الجريمة السيبرانية التي تتجاوز النطاقات الإقليمية والسيادية التقليدية. فهذا التعاون يتيح تبادل المعلومات وتعقب الجناة وتنسيق الإجراءات الجنائية بشكل فعّال. ويُستعرض هذا المطلب من خلال ثلاث محطات أساسية: الفرع

الأول دور الأنتربول واليوروبول في مكافحة هذه الجريمة ثم فرع ثاني في تبادل المعلومات بين الأجهزة الأمنية والقضائية ثم فرع ثالث فيه اتفاقية تسليم المجرمين بين الدول

الفرع الأول :دور الأنتربول واليوروبول في مكافحة الجريمة السيبرانية.

يعتبر الإنتربول واليوروبول حجر الزاوية في الجهود الدولية لمكافحة الجريمة السيبرانية، حيث يعملان ضمن إطار قانوني وتنظيمي يتيح لهما التنسيق مع الأجهزة الأمنية للدول الأعضاء وتسهيل التحقيقات العابرة للحدود، في هذا الفرع سنتطرق الى الإطار القانوني والتنظيمي لعمل الإنتربول واليوروبول، ثم آليات التنسيق وتبادل المعلومات بين الدول الأعضاء، المبادرات العملياتية والتقارير التقنية لمكافحة الجريمة السيبرانية.

أولا : الإطار القانوني والتنظيمي لعمل الإنتربول واليوروبول في المجال السيبراني

يستند العمل المؤسسي لكل من الإنتربول واليوروبول في مكافحة الجريمة السيبرانية إلى منظومة قانونية وتنظيمية معقدة ومتعددة المستويات، تجمع بين الطابع الدولي والتقني، وتُكرّس آليات فعالة للتعاون العابر للحدود.

أ–الإنتربول: وهو اختصار لـ المنظمة الدولية للشرطة الجنائية[1] يعمل وفقًا للنظام الأساسي المعتمد سنة 1956، والذي يُحدّد أهدافه في دعم التعاون بين أجهزة الشرطة بالدول الأعضاء، مع الالتزام الصارم بمبدأ عدم التدخل في القضايا السياسية أو العسكرية أو الدينية أو العرقية (المادة 3)[2]. وقد أنشأ الإنتربول وحدة متخصصة تحت اسم Cybercrime Directorateتشرف على التنسيق في التحقيقات الرقمية، وتوفير قواعد بيانات تقنية متقدمة، إلى جانب تشغيل شبكة الاتصال العالمية الآمنة I-24/7 بين الأجهزة الأمنية.

[1]- المنظمة الدولية للشرطة الجنائية (الإنتربول)، النظام الأساسي للإنتربول ،1956 https://www.interpol.int
تم الاطلاع يوم: 08/03/2025، سا 21:12.
[2]- النظام الاساسي لمنظمة الانتربول المادة 3.
https://eur-lex.europa.euEUR-Lex – Regulation (EU) 2016/794
تم الاطلاع يوم: 08/03/2025، سا 21:19.

ب– اليوروبول: فقد تم تأسيسه بموجب اتفاقية يوروبول لعام 1995، وأعيد تنظيمه بموجب القرار رقم EC 2009/371/الصادر عن مجلس الاتحاد الأوروبي[1]، والذي مكّنه من التحول إلى وكالة تابعة للاتحاد الأوروبي تُعنى بإنفاذ القانون على المستوى الأوروبي. وفي سنة 2013، أسس اليوروبول المركز الأوروبي لمكافحة الجريمة السيبرانية[2] (EC3) والذي يُعد المنصة التقنية الأولى لتنسيق جهود الدول الأعضاء في مواجهة التهديدات الرقمية المتطورة. ويرتكز الإطار القانوني لهذا المركز على القرار (Ec /2016/794) الذي عزّز صلاحيات اليوروبول في مجال تبادل المعلومات وتحليل البيانات السيبرانية[3].

وتتمثل الأهمية القانونية في هاتين المؤسستين بقدرتهما على المواءمة بين الالتزامات القانونية الدولية وبين متطلبات التحقيق التقني، عبر اتفاقيات وشراكات متعددة مع شركات التكنولوجيا، ومراكز البحوث، وهيئات الأمم المتحدة، بما يجعل من دورهما آلية مركزية في بنية التعاون الدولي لمكافحة الجريمة السيبرانية.

ثانيا/آليات التنسيق وتبادل المعلومات بين الدول الأعضاء:

يشكل التنسيق بين الدول واجهزة انفاذ القانون ركيزة جوهرية في مكافحة الجريمة السيبرانية، العابرة للحدود وتعقيدها التقني المتنامي ، في هذا الإطار اضطلعت المنظمات الشرطية الدولية بدور محوري في بناء بنى تحتية وآليات مؤسسية تسمح بتدفق البيانات الجنائية بشكل آمن وسريع بين الدول الأعضاء.

[1]- وكالة الاتحاد الأوروبي للتعاون في إنفاذ القانون (اليوروبول)، اللائحة (EU) رقم 2016/794 بشأن وكالة الاتحاد الأوروبي للتعاون في إنفاذ القانون (يوروبول)/https://eur-lex.europa.eu الرابط تم الاطلاع يوم: 14/03/2025، سا 22:08.

[2]- المنظمة الدولية للشرطة الجنائية (الإنتربول)، التقرير السنوي لآليات التعاون لمكافحة الجريمة السيبرانية. https://www.interpol.int/en/Crimes/Cybercrime تم الاطلاع يوم: 14/03/2025، سا 10:35

[3]- الوكالة الأوروبية لمكافحة الجريمة (اليوروبول)، معلومات حول النظامSIENA
https://www.europol.europa.eu/activities-services/services-support/information-exchange
تم الاطلاع يوم: 14/03/2025، سا 23:00.

ويوفر الإنتربول منصة تنسيقية عالمية من خلال شبكة الاتصال الآمنةI-24/7 التي تتيح لأجهزة الشرطة في 194 دولة عضوًا تبادل بيانات فورية حول الهجمات السيبرانية و الجهات الفاعلة، وعينات البرمجيات الخبيثة، تُدار هذه العمليات من قبل مديرية الجريمة السيبرانية، التي تعمل عبر المجمع العالمي للابتكار التابع للانتربول وتقوم هذه البنية المؤسسية بتطوير آليات للإنذار المبكر، ودعم التحقيقات، وإعداد ملفات تحليلية مشتركة، خاصة عند وقوع اختراقات للبنية التحتية الحيوية أو شبكات مالية. كما ينخرط الإنتربول في مشاريع دولية مثل تبادل المعرفة حول الجريمة السيبرانية التي تسهل التعاون الميداني.

أما على مستوى الاتحاد الأوروبي، فيُعد المركز الأوروبي لمكافحة الجريمة السيبرانية (EC3) التابع لليوروبول البنية التقنية والاستراتيجية الأساسية للتنسيق بين الدول الأعضاء. كما يدير اليوروبول نظامًا خاصًا لتبادل المعلومات يُعرف باسم تطبيق الشبكة الآمنة لتبادل المعلومات يسمح بمراسلات مشفّرة عالية السرعة بين السلطات القضائية والأمنية الأوروبية،ضمن احترام حماية الخصوصية والبيانات.

ثالثًا: المبادرات العملياتية والتقارير التقنية لمكافحة الجريمة السيبرانية:

في إطار مواجهة التهديدات السيبرانية المتطورة، أطلقت كل من الإنتربول واليوروبول سلسلة من المبادرات العملياتية المتخصصة والتقارير التقنية عالية الدقة، وتعد هذه المبادرات أدوات عملية تمكّن الدول الأعضاء من تكييف استراتيجياتها الوطنية، بناءً على تحليل استخباراتي محيّن، وخبرات ميدانية

أ- جهود الإنتربول العملياتية والتقنية:

ينفّذ الإنتربول عمليات دولية دورية تستهدف أنشطة الجريمة السيبرانية، مثل عملية الموجة السيبرانية الافريقية ، التي أطلقت في 2022 بالشراكة معAFRIPOL وأسفرت عن اعتقال مئات[1]

[1]- الأنتربول، الإجرام السيبراني، 14-05-2014، مجالات، https://www.interpol.int تم الاطلاع عليه يوم: 14/03/2025، سا 01:45.

المشتبه فيهم في عمليات احتيال مالي وهجمات إلكترونية، كما يصدر الإنتربول تقارير تقنية دورية، مثل تقرير الاتجاهات في الجريمة السيبرانية الذي يُعد مرجعًا لفهم التهديدات الناشئة مثل (برمجيات الفدية) والاحتيال عبر العملات الرقمية. وتوفر هذه التقارير معلومات تحليلية ومقترحات للرد السيبراني، وتُسهم في دعم قدرات الدول التي تعاني من ضعف في بنيتها الرقمية[1].

ب- جهود اليوروبول الاستباقية والمعلوماتية:

من جانبها، يحرص المركز الأوروبي لمكافحة الجريمة السيبرانية في إطار اليوروبول، على إصدار تقارير سنوية مثل التقييم السنوي للتهديدات الناتجة عن الجريمة المنظمة عبر الانترنت IOCTA والذي يُعتبر من أهم المراجع الاستراتيجية لفهم أنماط الجريمة عبر الإنترنت كما شارك في تنفيذ عمليات كبرى بالتعاون مع الدول الأعضاء، من أبرزها عملية التورنيكيه TORNIQUETضد جماعات دولية ، أدت إلى توقيف عناصر أساسية في شبكات دولية للجريمة السيبرانية، وتظهر أهميتها في انه كيف يمكن للتنسيق متعدد والتعاون الدلي أن يحدّ من الإفلات من العقاب[2].

ج- التأثير والتقييم الدولي:

تؤكّد دراسات صادرة عن مكتب الأمم المتحدة، ومنظمة الأمن والتعاون في أوروبا أن مشاركة الدول في هذه المبادرات تُمثّل أساسًا لرفع مستوى الجاهزية السيبرانية، وتعزيز التوأمة القانونية بين النظم الدولية[3].

---

[1] - منظمة الإنتربول – عملية الموجة السيبرانية الإفريقية،
https://www.interpol.int/en/News-and-Events/News/2022/Africa-Cyber-Surge-operation
تم الاطلاع يوم: 14/03/2025، سا 02:00.

[2]- اليوروبول – التقييم السنوي للتهديدات الناتجة عن الجريمة المنظمة عبر الإنترنت (IOCTA) لسنة 2023 : https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 تم الاطلاع يوم 05-05-2025 سا 11:15

[3] - مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة البحوث والدراسات، مج12، ع2، 2019، ص709.

الفرع الثاني : تبادل المعلومات بين الاجهزة الامنية والقضائية بين الدول:

في ظل الطابع العابر للحدود للجريمة السيبرانية، أصبح تبادل المعلومات بين الأجهزة الأمنية والقضائية أمرًا بالغ الأهمية لضمان فعالية التعاون الدولي. ويستعرض هذا الفرع ثلاث فقرات رئيسية: الإطار القانوني والمؤسسي لهذا التبادل، الوسائل التقنية المعتمدة، والتحديات والآفاق المستقبلية لتعزيز هذه الآليات.

أولا/: الإطار القانوني والمؤسسي الدولي لتبادل المعلومات الأمنية والقضائية:

تعد اتفاقية بودابست لعام 2001 من أبرز المعاهدات الدولية في هذا المجال[1] ,حيث تنظم التعاون القضائي وتبادل المعلومات بين الدول الأطراف، وتُحدّد آليات المساعدة القانونية المتبادلة في الجرائم السيبرانية. كما تبرز الدراسة الشاملة حول الجريمة السيبرانية الصادرة عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة[2] أهمية تطوير أطر قانونية ُتعزز من فعالية تبادل المعلومات بين الدول، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (باليرمو) (2000) وتهدف إلى تعزيز التعاون الدولي لمكافحة الجرائم التي تتجاوز حدود الدول مع التركيز على الأطر القانونية الوطنية[2].

ثم في السياق الأوربي تلعب اليوروبول دورا رئيسيا في التنسيق بين الأجهزة الأمنية ومن الاتفاقيات الإقليمية تهدف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 إلى تعزيز التعاون بين الدول العربية في مجال الجرائم الالكترونية[3] وتحديد الاطر المشتركة من خلال تبادل المعلومات والخبرات وتوحيد التشريعات ذات الصلة بما في ذلك الجرائم السيبرانية.

ثم اتفاقية الاتحاد الإفريقي للأمن السيبراني وحماية البيانات الشخصية (مالابو) (2014) تبرز الاتفاقية الحاجة إلى تطوير تشريعات وطنية تعزز من حماية البيانات الشخصية، وتواجه التحديات المتزايدة في مجال الأمن السيبراني.

---

[1]- اتفاقية بودابست. 2001، مرجع سابق، المواد 23-28.
[2]- مكتب الامم المتحدة المعني با المخدرات والجريمة. الدراسة الشاملة للجريمة السيبرانية 2013. مرجع سابق.
[3]- جامعة الدول العربية . الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 مرجع سابق، المادة 32.

وعلى المستوى الوطني في الجزائر، ينظّم القانون رقم 18-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها عمليات التنسيق بين مختلف الأجهزة الأمنية[1] , مع نصوص تُتيح تبادل المعلومات على المستويين الوطني والدولي في إطار التعاون القضائي والأمني حيث تم إنشاء الهيئة الوطنية للوقاية من الجرائم الإلكترونية سمح بتعزيز التنسيق الداخلي، وتوفير نقطة اتصال للتعاون مع الهيئات الأجنبية، وفق المعايير الدولية.

ثانيا: التعاون الأمني في تبادل المعلومات السيبرانية:

يُعد التعاون بين الأجهزة الأمنية في ميدان الجريمة السيبرانية حجر الزاوية لأي إستراتيجية فعالة في مكافحة هذا النوع المعقد من الجرائم.

تعد الاتفاقيات الثنائية والإطارات متعددة الأطراف القاعدة الأساسية لتبادل المعلومات. وأهم هذه الاتفاقيات هي اتفاقية بودابست بشأن الجريمة السيبرانية (2001)، التي خُصصت فيها المواد 29 إلى33 لتنظيم التعاون الفوري وتبادل المعلومات التقنية[2]، التحقيقية، والقانونية، من خلال شبكات الاتصال 24/7 بين الدول الأطراف , كما طوّر الاتحاد الأوروبي آليات نوعية للتنسيق الأمني عبر جهاز الانتربول الذي يعد دوره فعالا في التنسيق الميداني وتسهيل عمليات تبادل الادلة الرقمية والبيانات الفنية بين الدول الاعضاء حيث يعتمد على آليات تشغيلية متطورة وفعالة مثل شبكات الإنذار المبكر، وفرق الاستجابة السريعة، ومراكز الاتصال المشتركة كشبكة (24/7-i) التي تعد قناة آمنة للاتصال بين الاجهزة الامنية في 194 دولة وهو ما مكن من مواجهة الحوادث السيبرانية في لحظتها، كما توصي بذلك وكالة الأمن السيبراني الأوروبية ، وايضا دور اليوروبول في مكافحة الجريمة السيبرانية بإعتماده وسائل وأدوات تقنية متطورة مثل مركز الجريمة السيبرانية (EC3) الذي يعمل كمحور تنسيق للعمليات الامنية السيبرانية التي تقوم بتأمين بين وحدات التحقيق عبر بروتوكولات موحدة .واقليميا أنشئت الاتفاقية العربية لمكافحة جرائم تقنية

[1]- القانون الجزائري 18-04 المؤرخ في 10 ماي2018 , المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 27، المادة 43 سنة2018.
[2]- اتفاقية بودابست 2001 . المواد 29 الى 33 مرجع سابق.

المعلومات (2010)، التي ألزمت الدول الأعضاء بتبادل المعلومات بين الأجهزة الأمنية والقضائية حول الجرائم الإلكترونية ومرتكبيها، كما جاء في المادة 12 وقد تمّ تأسيس مكتب الجريمة الإلكترونية التابع لمجلس وزراء الداخلية العرب لتنسيق هذا الدور[1].

وعلى المستوى الوطني، بادرت الجزائر إلى إنشاء هيئات أمنية مختصة مثل المركز الوطني للأدلة الرقمية التابع للدرك الوطني، إضافة إلى الخلية الوطنية للاستجابة لحوادث الحاسوبCERT ، التي تعمل على رصد الهجمات وتبادل التقارير مع الأجهزة الأمنية والجهات السيادية ذات الصلة، كما كرس القانون 18-04 لسنة 2018 هذه المنهجية من خلال التأكيد على ضرورة تبادل المعلومات بين الجهات المعنية بالتحقيق وحماية المعطيات.

وفي ذات السياق أن التعاون الأمني يواجه تحديات تتعلق بغياب شبكة اتصال سيبرانية بين مختلف الهيئات الأمنية، مما يتطلب اعتماد بنى تحتية مؤمنة وتكنولوجيات تشفير حديثة[2].

ثالثا: التعاون القضائي في تبادل المعلومات السيبرانية:

تعتبر اتفاقية بودابست (2001) المرجع الأبرز في هذا المجال، حيث تنص المادة 34 لتفعيل التعاون القضائي من خلال آلية شبكات نقاط الاتصال 24/7، التي تمكّن المدّعين والقضاة من التواصل الفوري وتبادل المعلومات حول الجناة، الأدلة، والمعلومات التقنية الخاصة بالجرائم المعلوماتية. وقد انضم إلى هذه الشبكة أكثر من 80 دولة، ما يجعلها من أكثر أدوات التعاون القضائي فعالية في مجال الجريمة السيبرانية.

ويشكل اليوروجست (Eurojust) وهو وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية". المحور القضائي لتنسيق تبادل المعلومات بين الجهات القضائية للدول الأعضاء، حيث يعمل على تنسيق مذكرات الاعتقال، أوامر الحصول على الأدلة، والإنابات القضائية ذات الصلة

[1]- مجلس وزراء الداخلية العرب، "التقرير العربي الموحد حول الجريمة السيبرانية"، تونس، 2021، ص. 25

[2]- سعيد شادي، آليات التعاون القضائي في مجال مكافحة الجرائم السيبرانية، رسالة دكتوراه، جامعة سطيف، 2021، ص. 180.

بالجرائم الإلكترونية. كما تدعمه مبادرة e-Evidence وهي مبادرة تشريعية من الاتحاد الأوروبي تهدف إلى تسهيل عملية جمع وتحليل الأدلة الإلكترونية في التحقيقات الجنائية عبر الحدود بين الدول الأوروبية.

وفي الإطار العربي، فقد تبنّت الدول العربية آلية الإنابات القضائية الإلكترونية ضمن توصيات الملتقيات القضائية لمجلس وزراء العدل العرب، كما ظهر في إعلان القاهرة 2018 حول العدالة الرقمية. وتُعدّ هذه المبادرات ترجمة لرغبة عربية في تطوير التعاون القضائي في ضوء التحديات التقنية الحديثة.

إن نجاح التعاون القضائي الدولي يتوقف على توحيد المساطر الإجرائية، واعتماد قنوات إلكترونية مخصصة للسلطات القضائية تسمح بتبادل الوثائق والأوامر القضائية إلكترونيا[1].

الفرع الثالث: اتفاقية تسليم المجرمين والتعاون في التحقيقات الجنائية.

في عالم يشهد تصاعدا لجرائم لا تعترف بالحدود، يبرز التعاون الدولي كركيزة لا غنى عنها لملاحقة الجناة وتحقيق العدالة. في هذا الفرع ثلاث فقرات اولا: الإطار القانوني لإجراء تسليم المجرمين ومعاييره الوطنية، ثم دور الاتفاقيات الدولية كمصادر لهذا الإجراء، وصولًا إلى آليات التحقيق الجنائي العابر للحدود في مواجهة الجريمة السيبرانية.

أولا: الطبيعة القانونية لإجراء تسليم المجرمين ومعيار تطبيقه في التشريعات الوطنية:

يُعد تسليم المجرمين إجراءً سيادياً تتخذه الدولة استجابةً لطلب دولة أجنبية تسعى لمحاكمة شخص متهم أو تنفيذ حكم صدر ضده، ويُمارَس هذا الإجراء ضمن ضوابط قانونية صارمة تنظمها الاتفاقيات الدولية والتشريعات الوطنية. ويعكس تسليم المجرمين مظهراً من مظاهر التعاون الدولي، إلا أنه في ذات الوقت يمسّ حقوق الأفراد وحرياتهم، ما يستدعي تحقيق توازن دقيق بين

[1]- أحسن بوصقيعة، الوجيز في قانون الإجراءات الجزائية، ديوان المطبوعات الجامعية، الجزائر، ط2020، ص96.

مقتضيات العدالة الجنائية وسيادة الدولة ، فأن إجراء التسليم ليس عملاً إدارياً محضاً، بل هو عمل قانوني يتقاطع فيه الجانب السيادي للدولة مع واجباتها الدولية في التعاون الجنائي[1].

وقد تبنّت أغلب التشريعات، مثل القانون الفرنسي والمغربي (قانون المسطرة الجنائية)، معايير تضمن شرعية التسليم، كوجود اتفاق مسبق، وتحقيق شرط ازدواجية التجريم، وضمانات المحاكمة العادلة[2]. وفي الجزائر، فقد نظم قانون الإجراءات الجزائية في تعديلاته المتعاقبة، خاصة في القانون رقم 06-22 لسنة 2006، شروط وإجراءات تسليم المجرمين بدقة، وأكّد في المادة 696 على مبدأ احترام حقوق الإنسان كشرط أساسي لتنفيذ التسليم[2], أن تسليم المجرمين لا يُنفذ إلا ضمن إطار قانوني دقيق، سواء عبر نصوص دستورية أو تنظيمات إجرائية خاصة.[3]

ثانيا: الاتفاقيات والمعاهدات الدولية كمصدر لإجراءات تسليم المجرمين:

أضحت الاتفاقيات الدولية المرجعية الأساسية لتنظيم عملية تسليم المجرمين، حيث تسدّ هذه الاتفاقيات الفراغ التشريعي وتُيسّر التعاون بين الدول ذات الأنظمة القانونية المختلفة و من أبرز هذه الاتفاقيات، نجد الاتفاقية الأوروبية لتسليم المجرمين (1957)، التي أرست قاعدة عامة للتعاون الجنائي بين دول المجلس الأوروبي، وحددت مبادئ مثل شرط ازدواجية التجريم، وعدم تسليم الجرائم السياسية[4]. أما على الصعيد العالمي، فقد جاءت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (باليرمو، 2000) لتؤسس اطار قانوني ملزم لتسليم المجرمين المرتبطين بالجريمة المنظمة، بما فيها الجريمة السيبرانية، وكرّست في مادتها 16 قواعد مُلزمة للدول الأطراف لتيسير إجراءات التسليم[5]. وتؤكد اتفاقية بودابست بشأن الجريمة السيبرانية (2001) على وجوب التعاون في التسليم عند الجرائم المتعلقة بالأنظمة والمحتوى المعلوماتي، وفقاً لما ورد في المادة 24

[1]- عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة، 1999، ص. 55

[2]- أحمد الخمليشي، شرح قانون المسطرة الجنائية المغربي، الجزء الثاني، دار المعرفة، الرباط، 2012، ص. 315.

[3]- القانون الجزائري رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدّل والمتمم للأمر 66-155 المتعلق بقانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، سنة 2006، المادة 695

[4]- إيهاب محمد يوسف، اتفاقيات تسليم المجرمين ودورها في تحقيق التعاون الدولي لمكافحة الإرهاب، القاهرة، 2003، ص. 32

[5]- مجلس أوروبا، الاتفاقية الأوروبية لتسليم المجرمين، باريس، 1957، المادة 2.

منها[1] هذه الاتفاقيات تُعد أساساً قانونياً متيناً يقلص من التعارضات التشريعية، ويُسهم في تعزيز مبدأ الأمن القانوني، خصوصاً حين يتعلق الأمر بجرائم دولية معقدة مثل الإرهاب أو الجرائم الإلكترونية[2] وهو ما يُلاحظ في اتفاقية الرياض العربية للتعاون القضائي لعام 1983، واتفاقيات الأمم المتحدة الخاصة بمكافحة الإرهاب.

ثالثا–آليات التعاون الدولي في مجال التحقيقات الجنائية:

إلى جانب تسليم المجرمين، تُعتبر التحقيقات المشتركة وتبادل المعلومات والمساعدة القانونية المتبادلة من أبرز صور التعاون الدولي في مجال مكافحة الجريمة، لاسيما الجرائم السيبرانية. وتُعد "فرق التحقيق المشتركة أداة فعالة في جمع الأدلة عبر الحدود، خصوصاً عندما يكون للجريمة طابع دولي. تدعم هذه الفرق هيئات إقليمية كهيئات قضائية تابعة للاتحاد الأوروبي، التي تضطلع بدور تنسيقي بين السلطات القضائية في الدول الأوروبية وتيسير التحقيقات في الجرائم المعقدة، من خلال تنظيم الاجتماعات المشتركة وتبادل الأدلة كما أن مبادرة e-Evidence" وتعني الأدلة الإلكترونية التي هدفت إلى تحسين التعاون في جمع البيانات الرقمية من مزوّدي الخدمة الأجانب، وقد جاءت لتتجاوز التعقيدات التي تواجهها الدول في تطبيق أوامر التفتيش التقليدية[3]. وتعتبر هذه الآليات ذات أهمية كبيرة في التحقيقات المتعلقة بالجرائم السيبرانية، التي تحتاج إلى تعاون فني وقانوني بين دول مختلفة في ظل سرية وتعقيد الأدلة الرقمية. من جهة أخرى، تتعاون الدول من خلال المبادرات الإقليمية والدولية، مثل إنتربول و اليوروبول، التي تلعب دورًا في تبادل المعلومات بين الأجهزة الأمنية والقضائية لمكافحة الجرائم السيبرانية عبر الحدود[4].

---

[1]- تنص المادة 24 على أن كل من الدول المتعاقدة تلتزم، وفقًا لأحكام هذه الاتفاقية، بتسليم أي شخص مطلوب من قبل دولة أخرى متعاقدة بسبب ارتكابه جريمة يعاقب عليها القانون في كل من الدولة الطالبة والدولة المطلوب منها التسليم.

[2]- المادة 24.تنص المادة 24 على التعاون في تسليم الأشخاص المتهمين بارتكاب جرائم منصوص عليها في الاتفاقية

[3]- المفوضية الأوروبية، "الأدلة الإلكترونية – العدالة الجنائية الرقمية"، https://ec.europa.eu/info/law/better-regulation
تم الاطلاع يوم: 2025/20/03، سا: 23:20.

[4]- مليكة عطوي، "الجريمة الإلكترونية"، مجلة حوليات، العدد 12، جوان 2012، ص. 9.

وفي الجزائر، ووفقًا لقانون الإجراءات الجزائية المعدّل، تم تعزيز أحكام التعاون القضائي، لا سيما المواد من 694 إلى 698، التي تنظم المساعدة القضائية وتسليم الوثائق والأدلة[1].

المطلب الثاني : التعاون بين القطاعين العام والخاص في مكافحة الجريمة السيبرانية.

أصبح التعاون بين القطاعين العام والخاص ضرورة حتمية في مواجهة التحديات المتنامية للجريمة السيبرانية، نظراً لتقاطع الأدوار بين الهيئات الحكومية والجهات التكنولوجية الفاعلة. ويتناول هذا المطلب ثلاثة أبعاد محورية:استراتيجية الشراكة بين الحكومات والشركات التكنولوجية، ودور المجتمع المدني والمنظمات غير الحكومية، ثم الجهود المبذولة لصياغة سياسة أمن سيبراني عالمية مشتركة.

الفرع الاول: الشراكة بين الحكومات والشركات التكنولوجية.

تعد الشراكة بين الحكومات والشركات التكنولوجية من المرتكزات الأساسية في مواجهة التهديدات السيبرانية المتزايدة، لما توفره من تكامل في الموارد والخبرات. ويتناول هذا الفرع : أولا الحاجة الاستراتيجية لهذه الشراكة، ثانياً، نماذج وآليات التعاون الدولي بين الجانبين، وثالثاً، الضوابط والتوازنات التي تحكم هذا التعاون.

أولا: الحاجة الاستراتيجية للشراكة بين القطاعين العام والخاص لمكافحة الجريمة السيبرانية:

أضحت الجريمة السيبرانية تهديداً شاملاً يتجاوز إمكانيات الحكومات وحدها، مما أوجب التحول نحو شراكة استراتيجية مع القطاع الخاص، ولاسيما الشركات التكنولوجية الكبرى، لكونها تملك البنية التحتية الرقمية والمعلومات اللازمة لرصد التهديدات والكشف عنها.

وقد اعتبرت اتفاقية بودابست لمكافحة الجريمة السيبرانية أن التعاون مع الجهات غير الحكومية، ومنها مزودو الخدمة، جزء أساسي من إنفاذ القانون عبر الحدود (المادة 35)[1] ، فتعزيز الشراكات

[1]- قانون الإجراءات الجزائية الجزائري، المواد 694–698، المعدل والمتمم، بموجب القانون رقم 18-04 لسنة 2018.

الأمنية السيبرانية بين القطاعين العام والخاص هو بمثابة درع ضد الهجمات الرقمية المعقّدة فالإنتربول يضطلع بدور محوري في بناء هذا النوع من الشراكات لأن مكافحة هذا النوع المعقّد والعابر للحدود من الجرائم لا يمكن أن يتم من طرف واحد، بل يتطلب جهداً تشاركياً متعدد الأطراف يجمع بين قدرات الحكومات السيادية وخبرات القطاع الخاص التكنولوجية، لاسيما الشركات المالكة للبنى التحتية السيبرانية وشبكات البيانات العالمية من خلال هذا نلاحظ ان هذه الشراكات لا تقتصر فقط على بيان أهمية التعاون، بل تؤطره ضمن نموذج مؤسسي دولي متقدّم يمثل الإنتربول أبرز معالمه، وهو ما يعكس تطور الفكر الجنائي من المقاربة الانعزالية إلى المقاربة التشاركية[2].

ومن منظور دولي فإشراك الشركات الخاصة أصبح ضرورة استراتيجية لبناء منظومة مرنة في مواجهة التهديدات الرقمية[3], فغياب التعاون بين مؤسسات الدولة من جهة، والشركات التكنولوجية من جهة أخرى، يؤدي إلى فجوات أمنية تستغل لتحقيق التهديدات السيبرانية فلتكامل المؤسسي بين القطاعين هو الركيزة الاستراتيجية الوطنية للأمن السيبراني العالمي.

ثانيا: نماذج وآليات الشراكة بين القطاعين في المجال السيبراني:

في ظل هيمنة القطاع الخاص على البنية التحتية الرقمية عالمياً قد اصبحت الشراكات بين القطاعين العام والخاص في المجال السيبراني امر ضروري و إحدى الركائز الأساسية للوقاية من الجريمة السيبرانية ومواجهتها، وقد تجسدت هذه الشراكة في عدد من المبادرات الدولية، أبرزها – المجمّع العالمي للابتكار للإنتربول –في سنغافورة والذي يشكل منصة تعاونية بين أجهزة إنفاذ القانون حول العالم والشركات التكنولوجية، بهدف تطوير قدرات مشتركة في رصد الجرائم

[1]- اتفاقية بودابست 2001. المادة 35, مرجع سابق.
[2]- أحمد عبد الله، الجريمة السيبرانية: التحديات القانونية والتقنية في العصر الرقمي، دار الفكر العربي، القاهرة 2020 ص91.
[3]- منظمة التعاون والتنمية الاقتصادية(OECD) ، "الشراكات بين القطاعين العام والخاص في مجال الأمن السيبراني: نظرة عامة"، 2012. مرجع سابق.

السيبرانية وتحليل بياناتها فلتعاون بين الشركاء من القطاعين العام والخاص يشكل أداةً حاسمة في التصدي للتحديات السيبرانية العابرة للحدود[1].

في السياق نفسه، تبرز مبادرة –تحالف التهديدات السيبرانية –2014 –CTA–وهي شبكة عالمية تضم عدداً من شركات الأمن السيبراني والحكومات[2]، تقوم على تقاسم معلومات التهديدات بشكل آني، ما يساهم في منع الهجمات واستباق آثارها قبل وقوعها. وتدل هذه المبادرات على انتقال التعاون من الإطار التقليدي إلى –الذكاء السيبراني المشترك –

أطلقت مبادرة "الشراكة العامة–الخاصة في مجال الأمن السيبراني– ضمن برنامج الأبحاث الأوروبي "هورايزن 2020"[3]، بهدف تطوير أدوات تكنولوجية دفاعية متقدمة، وتعزيز التنسيق بين المؤسسات الحكومية وشركات الأمن الرقمي، لا سيما لحماية البنى التحتية الحيوية

وعليه اصبح نقل الخبرة التقنية من القطاع الخاص إلى الجهات الرسمية هو أحد شروط النجاح في أي استراتيجية وطنية للأمن السيبراني[4].

وهكذا يتبين أن نماذج الشراكة الفاعلة لا تقوم فقط على تبادل الأدلة، بل على إنتاج استراتيجيات وقائية وتحليل مشترك للهجمات، ما يعزز الاستجابة الدولية المنسقة للجرائم الرقمية المتطورة.

[1] - الإنتربول، "المجمع العالمي للإبداع التابع للإنتربول"، https://www.interpol.int/en/Crimes/Cybercrime
تاريخ الاطلاع يوم: 23/03/2025، سا 23:05.

[2]- تحالف التهديدات السيبرانية، "من نحن"، CTA 2014. مرجع سابق، تم الاطلاع عليه يوم: 23/03/2025 سا 32:30.

[3]- المفوضية الأوروبية، "الشراكة بين القطاعين العام والخاص في مجال الأمن السيبراني"، مرجع سابق، تم الاطلاع عليه يوم: 24/03/2025، سا 21:00.

[4]- محمد زكريا، القانون الجنائي والتكنولوجيا الحديثة: دراسة في الجريمة السيبرانية، دار النهضة العربية، بيروت، 2019، ص 77.

ثالثا: ضوابط وتوازنات الشراكة بين القطاعين في المجال السيبراني:

رغم الأهمية المتزايدة للشراكة بين القطاعين العام والخاص في مواجهة التهديدات السيبرانية، إلا أن هذه الشراكة تثير إشكاليات تتعلق بضرورة إرساء توازنات دقيقة تضمن احترام السيادة القانونية، وحماية الخصوصية الرقمية، وتفادي استغلال النفوذ التكنولوجي. فالسلطات العمومية غالبًا ما تعتمد على قدرات الشركات الخاصة في مجالات مثل تحليل البيانات، واكتشاف الثغرات، ومراقبة الشبكات، وهو ما يفرض ضرورة وجود إطار قانوني ومؤسساتي صارم ينظم هذه العلاقة.

فتعد اتفاقية بودابست بشأن الجريمة السيبرانية لعام 2001، الإطار القانوني الدولي الأهم في تنظيم الجريمة السيبرانية وتحديد آليات التعاون بين الدول والقطاع الخاص، خاصة فيما يتعلق بضمان توازن دقيق بين مقتضيات الأمن السيبراني وضمانات الحقوق والحريات الأساسية. وقد أفردت الاتفاقية حيزاً خاصاً لمسألة الضوابط والتوازنات القانونية التي ينبغي احترامها في سياق الشراكة مع الشركات التكنولوجية، لا سيما عند جمع البيانات أو تسليمها.

ففي المادة 15، ألزمت الاتفاقية الدول الأطراف بأن تضمن في قوانينها الداخلية أن تُمارس سلطاتها المختصة صلاحيات التحري والتحقيق وفقاً لمبادئ الضرورة والتناسب دون تجاوز لحدود الخصوصية والحرية الشخصية، كما تنص الاتفاقية على وجوب توفير ضمانات قانونية فعالة لحماية البيانات والمراسلات الإلكترونية، حيث تؤكد المواد 14 و15 ان الشراكة بين القطاعين يجب ألا تتحول إلى أداة للمراقبة الشاملة، بل إلى قناة منظمة تُراعى فيها السيادة القانونية[1].

فخضوع الشراكات لقواعد المساءلة، وتحديد المسؤوليات بدقة، تُعد من العناصر الجوهرية لضمان نجاح هذه الشراكات في المجال السيبراني.

فأهمية التوازن بين الأمن الرقمي وحماية الحقوق الأساسية فتبادل المعلومات الاستخباراتية بين الشركات والحكومات يجب أن يتم ضمن ضوابط قانونية واضحة، وأن يُراعى فيه مبدأ الضرورة

[1]- اتفاقيت بودابست 2001 المواد 14و 15 مرجع سابق

والتناسب[1], فالتحديات الأخلاقية لهذه الشراكات، مثل إمكانية انتهاك الحياة الخاصة أو التضارب بين الأهداف الأمنية والربحية، تفرض إنشاء "هيئات رقابة مستقلة متعددة الأطراف"[2] ففي التشريعات الوطنية نجد في القانون الجزائري قانون حماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي (القانون 18-07 لسنة 2018)، يشكّل أحد الأسس القانونية لتنظيم العلاقات بين السلطات الأمنية والشركات المزودة للخدمات الرقمية، إذ ينص على ضرورة احترام سرية المعطيات وعدم الإفشاء بها إلا بأمر قضائي[3].

الفرع الثاني: دور المجتمع المدني والمنظمات غير حكومية.

يُعدّ المجتمع المدني والمنظمات غير الحكومية شريكًا فعالا في التصدي للجرائم السيبرانية، إذ يضطلعان بأدوار توعوية ورقابية وتكاملية مع الجهود الحكومية والدولية وتبرز أهمية هذا الدور من خلال ثلاث فقرات: أولًا، الإطار القانوني المنظم لعمل المجتمع المدني والمنظمات غير الحكومية، ثانيا دور المجتمع المدني في مكافحة الجريمة السيبرانية عبر التثقيف والمراقبة، وثالثًا، دور المنظمات غير الحكومية في تعزيز الأمن السيبراني على المستويين المحلي والدولي.

أولًا: الإطار القانوني للمجتمع المدني والمنظمات غير الحكومية:

شهد الإطار القانوني الدولي تطورًا ملحوظًا في الاعتراف بالدور المحوري الذي تؤديه المنظمات غير الحكومية ومكونات المجتمع المدني في مجال مكافحة الجريمة السيبرانية، وذلك ضمن مقاربة تشاركية تقوم على تعدد الفاعلين في مواجهة التهديد السيبراني. فقد نصت اتفاقية بودابست بشأن الجريمة السيبرانية لعام 2001 في ديباجتها[4]، على أهمية إشراك القطاع غير الحكومي في صياغة وتنفيذ السياسات العامة المتعلقة بالأمن الرقمي، وذلك إدراكًا للطبيعة العابرة للحدود لهذا النوع من الجرائم، وما تتطلبه من تنسيق متعدد المستويات.

---

[1]- تحالف التهديدات السيبرانية، مرجع سابق تاريخ وساعة الدخول: 22/03/2025، سا 02:25.
[2]- محمد زكريا، مرجع سابق ص. 189.
[3]- القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية الجزائرية، العدد 35.
[4]- مجلس أوروبا. "اتفاقية بودابست بشأن الجريمة السيبرانية". مرجع سابق.

فلا يمكن تحقيق استرتيجية فعالة للوصول الى الامن السيبراني الدولي الا بشراكة فعلية مع المجتمع المدني خاصة في مجالات التوعية ورصد الضحايا واحصاء للجرائم.

وقد أكد مجلس حقوق الإنسان التابع للأمم المتحدة (2021)[1] على دور المنظمات غير الحكومية في حماية الحقوق الرقمية والتوازن بين مكافحة الجرائم الإلكترونية واحترام الحريات الأساسية، ما عزز من شرعنة تدخل هذه الجهات ضمن الأطر القانونية الناظمة للعمل الدولي المشترك.

وعليه تكمن شمولية التعاون الذي يجعل المجتمع المدني عنصرا لا يقل أهمية عن الحكومات والقطاع الخاص في تحقيق الأمن السيبراني.

تأسيسًا على ذلك، أضحت العديد من الوثائق القانونية الدولية والإقليمية تستوعب مفهوم الحوكمة التشاركية للأمن السيبراني التي يُنظر فيها إلى المجتمع المدني والمنظمات غير الحكومية كشركاء قانونيين ومؤسسيين في بلورة السياسات وتقييم المخاطر، مما يمنح تدخلهم في هذا المجال شرعية قانونية متنامية، ويجعل من مساهماتهم ضرورة لا اختيارًا ضمن منظومة التعاون الدولي لمكافحة الجريمة السيبرانية.

ثانيا: دور المجتمع المدني في مكافحة الجريمة السيبرانية:

أ– مساهمة المجتمع المدني في الوقاية من الجريمة السيبراني:

[1]- مجلس حقوق الإنسان التابع للأمم المتحدة. "التعليق العام رقم 25 (2021) بشأن حقوق الأطفال في البيئة الرقمية."
الرابط: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
تاريخ وساعة الاطلاع: 11 ماي 2025، الساعة 17:00

يمثل المجتمع المدني جسرًا بين المواطن والدولة، ويقوم بدور محوري في نشر ثقافة الحذر الرقمي، والدفاع عن الحقوق الرقمية، وفضح الانتهاكات في الفضاء السيبراني[1].

1. التوعية المجتمعية: تنظم العديد من منظمات المجتمع المدني حملات توعوية حول مخاطر الإنترنت، مثل منظمة– مؤسسة الحدود الإلكترونية–

2. تدريب الفئات المستهدفة: تركز على تدريب الصحفيين، والناشطين، والطلبة، وأصحاب المؤسسات الصغيرة، على تقنيات الحماية الرقمية والتشفير، كأداة وقائية أساسية.

3. نشر أدوات الحماية المفتوحة: تُسهم منظمات مثل "Privacy International" و "Tor Project" في تطوير ونشر أدوات حماية الخصوصية، وتمكين الأفراد من التحكم في بياناتهم.

ب– أدوار منظمات المجتمع المدني في الاستجابة للجريمة السيبرانية:

1.الدعم القانوني والنفسي للضحايا: توفر منظمات مثل "Cyber Civil Rights Initiative" دعمًا نفسيًا وقانونيًا لضحايا الابتزاز الجنسي والجرائم الإلكترونية، بما في ذلك المساعدة في إزالة المحتوى غير المشروع.

2. **مراقبة السياسات والتشريعات:** تلعب المنظمات غير الحكومية دورًا رقابيًا في مراجعة التشريعات المتعلقة بالفضاء الرقمي، والتصدي لأي محاولات لتقييد الحريات العامة بحجة مكافحة الجريمة السيبرانية.

3.**التعاون مع الحكومات ومؤسسات الأمن:** في كثير من الدول، تُعد منظمات المجتمع المدني شريكًا في وضع استراتيجيات وطنية للأمن السيبراني، مثلما هو الحال في برامج "Cybersecurity Awareness Month" في أوروبا وأمريكا[2].

[1]- ناصري سميرة، بسمة ترغيني، دور المجتمع المدني في مكافحة الجريمة المنظمة، مداخلة، كلية الحقوق، جامعة خنشلة، 2014، ص 168-169.
[2] - مراد مشوش، مرجع سابق، ص711.

ج –نماذج وتجارب دولية ناجحة:

1. مبادرة "Keep It On" لمناهضة حجب الإنترنت: تضم هذه الحملة منظمات من أكثر من 100 دولة، وتهدف إلى فضح ومقاومة قرارات إغلاق الإنترنت التي تُتخذ غالبًا لتغطية الانتهاكات.

2.تجربة منظمة "APC" – Association for Progressive Communication:

تقدم APC الدعم للمدافعين عن حقوق الإنسان الرقمية في آسيا وأفريقيا، وتسهم في تعزيز القدرات القانونية والمؤسساتية.

3. شراكة المجتمع المدني في المنتدى العالمي لحوكمة الإنترنت:(IGF)

يعد IGF منصة تشاركية تضم المجتمع المدني، الحكومات، والشركات، مما يتيح صياغة سياسات متوازنة تراعي البعد الحقوقي في مواجهة الجريمة السيبرانية.

ثالثا : دور المنظمات الغير حكومية في مكافحة الجريمة السيبرانية:

تؤدي المنظمات غير الحكومية أدوارًا متعددة في مكافحة الجريمة السيبرانية، تشمل[1]:

1– رصد التهديدات الرقمية: تقوم هذه المنظمات بجمع وتحليل البيانات المتعلقة بالهجمات السيبرانية،[1] مما يساعد في فهم أنماط التهديدات وتطوير استراتيجيات لمواجهتها .

2– تقديم الدعم الفني والقانوني: توفر المنظمات غير الحكومية الدعم الفني للضحايا، مثل المساعدة في استعادة الحسابات المخترقة، وتقديم المشورة القانونية بشأن الإجراءات الممكنة.

3– التوعية وبناء القدرات: تنظم هذه المنظمات ورش عمل ودورات تدريبية لزيادة الوعي حول الأمن السيبراني وتعزيز القدرات التقنية للمجتمعات المستهدفة.

[1] - تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الفصل 7، آليات التعاون الدولي غير الرسمية، نشرت الترجمة العربية في: جويلية 2021.

4- المناصرة والتأثير على السياسات: تعمل المنظمات غير الحكومية على التأثير في السياسات العامة من خلال تقديم توصيات للهيئات الحكومية والدولية بشأن التشريعات المتعلقة بالجريمة السيبرانية.

هـ. نماذج لمنظمات غير حكومية ناشطة:

1- منظمة "أكسس ناو :(Access Now) "تقدم هذه المنظمة دعمًا فنيًا واستشاريًا للضحايا من خلال "خط المساعدة للأمن الرقمي"، وتدير منصة للمساعدة الأمنية الرقمية.

2- معهد السلام السيبراني :(CyberPeace Institute) يعمل هذا المعهد على رصد الهجمات السيبرانية ضد البنى التحتية الحيوية، ويعزز الشفافية السيبرانية من خلال تقاريره وتحليلاته.

3- **مؤسسة الجبهة الإلكترونية – Electronic Frontier Foundation)** (**EFF**:تركز هذه المؤسسة على القضايا الحقوقية المرتبطة بالإنترنت، وتدافع عن حرية التعبير، وتقدم مقترحات تشريعية متعلقة بالجريمة السيبرانية.

4- **مؤسسة الحقوق الرقمية (Digital Rights Foundation)** : تعمل هذه المؤسسة على تمكين النساء من الحماية من الابتزاز الإلكتروني، وتدير منصة لتوثيق الشكاوى الرقمية.

أثبت المجتمع المدني والمنظمات غير الحكومية أنها عنصر لا غنى عنه في مكافحة الجريمة السيبرانية، سواء من حيث الوقاية أو الاستجابة أو التأثير في السياسات. ومع ذلك، تبقى الحاجة ماسة إلى دعم هذه المنظمات، وبناء قدراتها لمواجهة التحديات المعقدة التي يفرضها الفضاء السيبراني[1].

[1] - مراد مشوش، مرجع سابق، ص711.

الفرع الثالث : تطوير سياسة أمن سيبرانية عالمية.

في ظل الطبيعة العالمية للتهديدات السيبرانية، بات من الضروري التفكير في صياغة سياسة أمن سيبرانية عالمية قادرة على توحيد الجهود الدولية، القانونية، والتقنية. ويقتضي هذا الفرع دراسة الإطار المفاهيمي والسياسي للأمن السيبراني العالمي، والركائز القانونية التي تحكمه، ثم بحث الآليات المؤسساتية الكفيلة بتنفيذه.

أولاً: الإطار المفاهيمي والسياسي للأمن السيبراني العالمي.

يمثل الأمن السيبراني أحد أوجه الأمن الجماعي في القرن الحادي والعشرين، إذ تجاوزت التهديدات الرقمية قدرة الدولة الوطنية على احتوائها بمفردها. فالهجمات السيبرانية لا تعترف بالحدود، وتستهدف البنى التحتية الحيوية والمؤسسات السيادية والأسواق العالمية في آنٍ واحد. ولذلك، ظهرت الحاجة إلى بناء فهم مشترك بين الدول حول ماهية الأمن السيبراني وتحديد مصادر التهديد، والأولويات، والمسؤوليات المشتركة.

أكدت دراسات وابحاث على أهمية هذا البعد المفاهيمي في بناء تعاون سيبراني عالمي، يوازن بين مقتضيات الأمن واحترام السيادة الرقمية للدول[1]. كما أبرزت دراسات أخرى أهمية إشراك الفاعلين من القطاع الخاص والمجتمع المدني في بناء تصور مشترك لمفاهيم مثل "الردع السيبراني" و"الحياد الرقمي"[2]. فا التفاهم المشترك حول القواعد الاساسية والتعاون الدولي في الفضاء الإلكتروني يشكل عنصراً أساسياً لمنع التصعيد والتنافس السيبراني بين القوى العالمية.

ثنياً: الركائز القانونية لتطوير سياسة سيبرانية عالمية مشتركة:

لا يمكن تصور سياسة سيبرانية فعالة دون وجود أساس قانوني دولي مشترك. فمن المبادئ العامة للقانون الدولي كاحترام سيادة الدول وعدم التدخل إلى الاتفاقيات المتخصصة كاتفاقية بودابست لعام 2001، تتضح الحاجة إلى إطار قانوني شامل ومنسّق.

[1] - التويجري، عبد الله بن عبد العزيز. التعاون الدولي في مكافحة الجرائم السيبرانية – دراسة في ضوء القانون الدولي العام. الرياض: مكتبة القانون والاقتصاد، 2020، ص. 49–52.

[2]- محمود، إيمان. "دور المنظمات الدولية في تعزيز الأمن السيبراني العالمي"، مجلة السياسة الدولية، العدد 121، 2020، ص. 92.

كما أظهرت دراسات أخرى التحديات المتعلقة بتضارب المصالح بين الدول الكبرى، وضعف التعاون القضائي في ملاحقة الجرائم العابرة للحدود[1] ومن هنا، برزت الحاجة إلى مرونة قانونية تشريعية تأخذ في الاعتبار الخصوصيات السيادية للدول، دون أن تُفرغ التعاون الدولي من مضمونه, فغياب إطار قانوني دولي موحّد هو أحد أبرز العوامل التي تعيق بناء بيئة رقمية آمنة عبر الحدود[2].

ثالثاً: الآليات المؤسساتية والتنسيقية لإنشاء سياسة أمن سيبراني مشتركة:

تتطلب السياسة السيبرانية العالمية مؤسسات قادرة على التنسيق بين الدول، ومتابعة تنفيذ الالتزامات، وتقييم المخاطر، واقتراح التدخلات السريعة عند وقوع حوادث كبرى , وفي هذا السياق، اقترحت الدراسات إمكانية إنشاء "هيئة دولية للأمن السيبراني" على غرار الوكالة الدولية للطاقة الذرية، تكون مختصة بمراقبة الأمن السيبراني العالمي، وتسهيل التعاون الفني وبناء القدرات لدى الدول النامية.[3] كما برزت دعوات لإدماج منظمات المجتمع المدني والجامعات ومراكز البحث في المنظومة التقريرية لهذه السياسات، بما يعزز الشفافية، ويضمن حماية الحقوق الرقمية.

فإنشاء هيئات مستقلة متعددة الأطراف في المجال السيبراني يشكّل أداة مركزية لتعزيز الثقة بين الدول وتعزيز بناء القدرات، خصوصاً في الدول النامية مع الاعتماد على مبادئ الشفافية والتمثيل المتعدد في صياغة سياسات الأمن السيبراني الدولية.

المبحث الثاني : تحديات التعاون الدولي لمكافحة الجريمة السيبرانية والحلول القائمة:

أضحى التعاون الدولي في مكافحة الجريمة السيبرانية ضرورة ملحة في ظل تصاعد التهديدات الرقمية العابرة للحدود، غير أن هذا التعاون يواجه تحديات سياسية واقتصادية تعيق تنسيقه الفعّال

[1] - جبري، فاطمة الزهراء. الركائز القانونية للأمن السيبراني في القانون الدولي العام. مذكرة ماستر، جامعة الجزائر 1، 2022، ص. 66.

[2] - عبد اللطيف، نسرين. التحديات القانونية في مواجهة الجريمة السيبرانية الدولية. مذكرة ماستر، جامعة وهران 2، 2019، ص. 73.

[3]- خليفة، محمد."أمن الفضاء السيبراني بين مقتضيات الحماية وحقوق الإنسان الرقمية"، مجلة الدراسات القانونية والسياسية، العدد 18، 2021، ص. 58.

بين الدول. وتبرز هذه التحديات من خلال تعارض المصالح السيادية، وتفاوت الإمكانيات التقنية والمالية. ضمن هذا السياق، يُعالج المطلب الأول "التحديات السياسية والاقتصادية للتعاون الدولي" أهم هذه العراقيل. بينما يتناول المطلب الثاني "سبل تعزيز التعاون الدولي في مكافحة الجريمة السيبرانية" أبرز المبادرات والآليات المقترحة لتجاوزها.

المطلب الأول : التحديات السياسية والاقتصادية والتقنية في مجال التعاون الدولي.

يُعد التعاون الدولي في مجال مكافحة الجريمة السيبرانية رهينًا بتقاطع جملة من العوامل الجيوسياسية والاقتصادية والتقنية، ما يُفضي إلى تعقيد جهود التنسيق بين الدول. وتبعًا لذلك، يتناول هذا المطلب أبرز التحديات الماثلة أمام هذا التعاون، وذلك عبر الفرع الأول الذي يعالج "تأثير العلاقات السياسية على التعاون الدولي في المجال السيبراني"، ثم الفرع الثاني المخصص لـ"العوائق الاقتصادية وتمويل مكافحة الجرائم السيبرانية"، وأخيرًا الفرع الثالث الذي يُناقش "التفاوت في القدرات التقنية" بين الدول.

الفرع الاول :تأثير العلاقات السياسية على التعاون الدولي في المجال السيبراني.

يمثل التداخل بين السياسة والأمن السيبراني أحد أبرز التحديات التي تُقوض إمكانيات التعاون الدولي الفعّال في مكافحة الجريمة السيبرانية، تناولنا في هذا الفرع: أولًا، التوترات الجيوسياسية كعائق أمام التعاون الدولي، ثانيًا، أثر التحالفات السياسية والاقتصادية على التعاون السيبراني، وثالثًا، التوظيف السياسي للأمن السيبراني في العلاقات الدولية.

أولا: التوترات الجيوسياسية كعائق أمام التعاون الدولي:

تشكّل التوترات الجيوسياسية بين القوى الكبرى أحد أبرز العوائق التي تحدّ من فاعلية التعاون الدولي في مجال مكافحة الجريمة السيبرانية. إذ أن حالة انعدام الثقة المتبادلة، خاصة بين الولايات المتحدة والصين وروسيا تُقوّض الجهود الرامية إلى تأسيس أطر قانونية عالمية موحّدة، وتُعيق التوافق حول المبادئ الحاكمة للأمن السيبراني.

فالصراعات السياسية والمصالح الاقتصادية المتعارضة تُفضي إلى تعطيل تبادل المعلومات الاستخباراتية المتعلقة بالهجمات السيبرانية، وإلى الامتناع عن توقيع اتفاقيات شاملة لمكافحة هذا النوع من الإجرام العابر للحدود، كما أن الانقسام السيبراني يعكس إلى حدّ كبير حالة الحرب الباردة الرقمية، حيث تستخدم الدول الكبرى الأمن السيبراني كوسيلة لتعزيز نفوذها العالمي، لا كأداة لحماية السلم الدولي[1],فهذه الانقسامات السياسية حالت دون التوصل إلى اتفاق دولي ملزم ينظم سلوك الدول في الفضاء السيبراني.

ثانيا: أثر التحالفات السياسية والاقتصادية على التعاون السيبراني:

تؤدي التحالفات الإقليمية والدولية دورًا مزدوجًا في التعاون السيبراني، فهي من جهة تسهم في تنسيق السياسات وتوحيد التشريعات بين أعضائها، ومن جهة أخرى قد تُعزز من الانقسام العالمي في إدارة الفضاء الإلكتروني. فالتحالفات مثل الاتحاد الأوروبي ومنظمة شنغهاي للتعاون عملت على إنشاء أطر سيبرانية متقدّمة، كما هو الحال في توجيه NIS الأوروبي الذي يسعى إلى تعزيز الأمن السيبراني بين الدول الأعضاء عبر تبادل المعلومات، وتحديث البنية التحتية للحماية الرقمية[2]. إلا أن هذه التحالفات قد تُقصي دولًا غير منضوية ضمنها، مما يؤدي إلى تشتت المبادرات العالمية، وغياب مقاربة شاملة لمواجهة التهديدات السيبرانية.

كما أن التباين في مستوى القدرات التقنية والسياسية بين الدول يُؤثر سلبًا على مستوى التنسيق المشترك، وهو ما حول الفجوة الرقمية بين الدول,وعلى المستوى الاقليمي فغياب تكتل عربي موحد في المجال الرقمي يضعف من قدرة الدول العربية على الدخول في مفاوضات دولية متكافئة[3].

[1]- غجاتي سهيلة، راهم أميرة، مرجع سابق، ص68.

[2]- لامية طالة، تهديدات الجرائم السيبرانية، مجلة معالم للدراسات القانونية والسياسية، 2020، مج2، ع2، ص62.

[3]- بوصقيعة، أحسن. التحديات القانونية للتعاون الدولي في مكافحة الجريمة السيبرانية. مجلة دفاتر السياسة والقانون، العدد 20، 2019. ص 33.

ثالثا: التوظيف السياسي للأمن السيبراني في العلاقات الدولية:

لا يخفى أن بعض الدول توظّف خطاب "مكافحة الجريمة السيبرانية" لخدمة أهداف سياسية واستراتيجية، وذلك من خلال فرض قيود أو عقوبات على دول أخرى بذريعة التصدي للهجمات الإلكترونية.

هذا التسييس للمجال السيبراني يُعدّ من أبرز الإشكاليات المعاصرة، حيث يُستخدم الأمن الرقمي كأداة جيوسياسية لتبرير التدخل أو فرض السيطرة التقنية والاقتصادية. وحسب الدراسات فالإفراط في تسييس الأمن السيبراني يُقوّض من فعالية التعاون الدولي ويهدد مبادئ الشفافية والعدالة الرقمية ، كما يُسجّل أن بعض الدول ترفض الانضمام إلى اتفاقيات دولية مثل اتفاقية بودابست، بسبب مخاوفها من أن تُستغل بنودها لأغراض استخباراتية أو لفرض معايير قانونية لا تراعي الخصوصيات السيادية[3], وفي الإطار الاقليمي فعدداً من الدول العربية ما زالت مترددة في تبني تعاون دولي موسّع في المجال السيبراني، خشية فقدان السيطرة الوطنية على بياناتها أو التعرض لضغوط سياسية من قبل القوى الكبرى[1].

الفرع الثاني: العوائق الاقتصادية وتمويل مكافحة الجرائم السيبرانية.

يشكل الجانب الاقتصادي أحد الأعمدة الأساسية في بناء قدرات فعّالة لمواجهة الجريمة السيبرانية، إذ تعاني العديد من الدول من صعوبات مالية تحد من تطوير بنيتها التحتية الرقمية. وفي هذا السياق، يناقش هذا الفرع ثلاث إشكالات رئيسية: أولًا، ضعف الموارد المالية كعائق أمام البنية التحتية السيبرانية، ثانيًا، التفاوت الاقتصادي بين الدول وأثره على التعاون الدولي، وثالثًا، محدودية التمويل الدولي وبرامج المساعدة التقنية.

[1]- بوصقيعة، أحسن. المرجع نفسه.

أولا : ضعف الموارد المالية كعائق أمام البنية التحتية السيبرانية:

تُعد محدودية الموارد المالية في العديد من الدول، خاصة النامية منها، من أبرز المعوقات في بناء بنية تحتية سيبرانية قوية. فالقدرات التقنية والمؤسساتية في هذه الدول غالبًا ما تتسم بالضعف بسبب نقص التمويل، مما يُعوق تطوير نظم الدفاع السيبراني، وتوظيف الكفاءات المتخصصة، واقتناء الوسائل التكنولوجية الضرورية للكشف عن الجرائم السيبرانية والرد عليها.

"البلدان النامية غالبًا ما تفتقر إلى نظم حوكمة رقمية، والمهارات التقنية، والتمويل اللازم لتنفيذ تدابير الأمن السيبراني الأساسية"[1]. هذه التحديات الهيكلية تجعل من بيئة الأمن الرقمي فيها هشّة، وتزيد من قابليتها للاستهداف من قبل الجماعات الإجرامية العابرة للحدود.

ثانيا : التفاوت الاقتصادي بين الدول وأثره على التعاون الدولي:

إنّ التفاوت الكبير في الإمكانيات الاقتصادية بين الدول يُفضي إلى فجوة رقمية عالمية تُقوّض إمكانيات التعاون الدولي المتوازن في مكافحة الجريمة السيبرانية .

فالدول ذات الاقتصاديات المتقدمة تتمتع بقدرات مالية وتقنية تسمح لها بإنشاء هياكل أمنية متطورة، بينما تعاني الدول الأقل نمواً من صعوبات في الوفاء بالحد الأدنى من متطلبات الأمن السيبراني. فهذا التفاوت يؤدي إلى انخفاض ثقة المستثمرين في الأسواق الناشئة، ويُضعف استراتيجيات التنمية الرقمية فيها.

كما يضعف هذا التفاوت إمكانيات الانخراط في الاتفاقيات الدولية بسبب الالتزامات التقنية والمالية التي تُرهق كاهل الدول الضعيفة.

ثالثا : محدودية التمويل الدولي وبرامج المساعدة التقنية:

[1]- البنك الدولي. (2005-01-20). تعزيز القدرة على الصمود السيبراني في البلدان النامية .تم الاطلاع عليه بتاريخ 2025/03/04، سا 11:18، من الموقع:
https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries

رغم تزايد التهديدات الإلكترونية، لا تزال برامج الدعم الدولية لمكافحة الجريمة السيبرانية غير كافية، وتواجه العديد من العراقيل. فبحسب التقارير والدراسات السابقة فإن "الموارد المالية المخصصة لتعزيز الأمن السيبراني في البلدان المنخفضة والمتوسطة الدخل ضئيلة مقارنة بالحاجيات الواقعية"[1]. كما أن بعض برامج الدعم تخضع لاشتراطات سياسية أو أولويات جيوسياسية للدول المانحة، مما يعيق إيصال التمويل إلى الدول الأكثر تضرراً وفي ذات السياق وفي مجال التعاون الدولي فغياب استراتيجية تمويل إقليمية لمواجهة الجريمة السيبرانية في الأقاليم العربية والأفريقية يُعد من أبرز نقاط الضعف التي تُعيق التنسيق بين هذه الدول في هذا المجال.

الفرع الثالث : التفاوت في القدرات التقنية.

يُعد التفاوت في القدرات التقنية بين الدول من أبرز العقبات التي تعيق بناء تعاون سيبراني فعّال، حيث تكشف هذه الفجوة عن اختلال عميق في إمكانيات الدول على الصعيدين الفني والمؤسساتي. ويتناول هذا الفرع ثلاثة محاور أساسية: أولًا، الفجوة الرقمية العالمية كعائق للتعاون السيبراني، ثانيًا، اختلال التوازن في القدرة على المشاركة في الأطر القانونية، وثالثًا، التمكين السيبراني كضرورة لبناء قدرات الدول ومواكب.

أولا: الفجوة الرقمية العالمية كعائق للتعاون السيبراني:

إن التفاوت التقني بين الدول من أبرز العراقيل التي تعيق بناء منظومة شاملة لمكافحة الجريمة السيبرانية، حيث يؤدي غياب البنى التحتية الرقمية المتطورة في العديد من البلدان النامية إلى جعلها مناطق هشّة من الناحية السيبرانية، لا تملك القدرة على رصد الهجمات أو تعقب الفاعلين, فحسب تقرير مكتب الأمم المتحدة أن الجماعات الإجرامية المنظمة تستغل هذا الضعف المؤسسي في الدول الأقل تقدماً للقيام بعمليات عابرة للحدود، مستفيدة من غياب وسائل التحقيق الجنائي الرقمي[2]. وفي السياق ذاته، يرى الباحثان McGuire و Dowling أن

[1]- بوصقيعة، أحسن مرجع سابق ص 79
[2]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) مرجع سابق.

الفجوة التقنية لا تقتصر على الوسائل، بل تمتد إلى مفاهيم الأمن السيبراني، ما يؤدي إلى ضعف التنسيق بين الدول في مواجهة الجرائم الرقمية.

فلا يقتصر التعاون الدولي على المساعدة القضائية المتبادلة، بل يشمل أيضا المساعدة الفنية وتبادل الخبرات بين الدول.

ثانيا: اختلال التوازن في القدرة على المشاركة في الأطر القانونية:

إن التفاوت في الموارد التقنية والبشرية ينعكس مباشرة على قدرة الدول على الاندماج في الأطر القانونية الدولية المنظمة لمكافحة الجريمة السيبرانية. فالدول التي تفتقر إلى القدرات التكنولوجية الكافية تُستبعد عملياً من صياغة أو تنفيذ المبادرات التقنية المتقدمة، مثل تلك المتبناة من قبل الاتحاد الأوروبي أو عبر اتفاقية بودابست، فالدول المتطورة تكنولوجيا تفرض من خلال تقدمها رقميا توجهاً عالمياً لا يتماشى مع واقع وقدرات الدول النامية ما يجعل التعاون مستبعد. هذا الخلل يؤدي إلى تفكك الاستجابة العالمية، وظهور فجوات في آليات التعاون الجنائي الدولي.

ثالثا :التمكين السيبراني كضرورة لبناء قدرات الدول:

إن تقليص الفجوة التقنية لا يمكن أن يتحقق دون دعم ممنهج للدول التي تعاني من ضعف القدرات السيبرانية، فلا بد من إتاحة فرص للدول النامية في مجال التمكين السيبراني، والذي يشمل تقديم الدعم المالي والتقني للدول غير القادرة، وتوفير فرص التدريب، وتعزيز الكفاءات المحلية، أما في السياق العربي، فقد نصّت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على ضرورة تعزيز القدرات الفنية للدول الأعضاء، من خلال تبادل الخبرات والتعاون في مجالات التحقيق والتجريم الرقمي[1].

إن بناء منظومة أمن سيبراني متوازنة وشاملة يمر عبر الاعتراف بالتفاوت في القدرات، وتوفير آليات تعاون مبنية على التضامن الرقمي، وليس على التفوق التقني.

[1]- جامعة الدول العربية (2010). مرجع سابق.

المطلب الثاني:سبل تعزيز التعاون الدولي لمكافحة الجريمة السيبرانية.

أمام تصاعد وتيرة التهديدات السيبرانية العابرة للحدود، بات من الضروري إرساء بنية قانونية دولية فعالة، تستند إلى اتفاقيات دولية موحدة وتشريعات وطنية متجانسة، في إطار مقاربة تشاركية شاملة. في هذا المطلب سنتطرق إلى أهمية تعزيز الاتفاقيات الدولية ثم إلى آفاق إنشاء مركز دولي موحد للأمن السيبراني ثم إلى المساعي لتطوير برامج دولية وإرساء ثقافة الوعي السيبراني، لبناء رد قانوني ومؤسساتي قادر على التصدي للتحديات الرقمية المعقدة

الفرع الاول: تعزيز الاتفاقيات الدولية وتطوير تشريعات وطنية متوافقة.

يُعد التعاون الدولي في مكافحة الجريمة السيبرانية ضرورة حتمية في ظل الطابع العابر للحدود لهذا النوع من الجرائم. وفي هذا السياق، تتجلى أهمية الاتفاقيات الدولية كمرجعية قانونية، تليها ضرورة مواءمة التشريعات الوطنية، واعتماد مقاربات تشاركية شاملة في صياغة السياسات السيبرانية.

أولًا: الاتفاقيات الدولية كإطار مرجعي في مكافحة الجريمة السيبرانية:

تُعد الاتفاقيات الدولية من الركائز الأساسية التي يرتكز عليها التعاون الدولي في مجال مكافحة الجريمة السيبرانية، حيث تشكل مرجعية قانونية لتنظيم التعاون العابر للحدود. وتُعد اتفاقية بودابست لسنة 2001 أبرز مثال على ذلك، إذ أرست أحكامًا واضحة لتجريم الأفعال السيبرانية، وسنّت آليات لتبادل المعلومات والأدلة، والتعاون القضائي الفوري بين الدول الأطراف[1] وفي هذا السياق، صرّحت المديرة التنفيذية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة، غادة والي، بأن اعتماد اتفاقية دولية جديدة سيشكّل "خطوة مفصلية نحو بناء استجابة موحدة

[1]- مجلس أوروبا. (2001). اتفاقية بودابست لمكافحة الجريمة السيبرانية، المادة 23. مرجع سابق.

ومتكاملة ضد الجرائم السيبرانية المتنامية"[1] وعليه، فإن وجود اتفاقيات دولية فعالة لا يُعد ترفًا قانونيًا، بل ضرورة عملية لتعزيز الحوكمة السيبرانية العالمية.

ثانيًا: مواءمة التشريعات الوطنية مع الأطر الدولية كشرط للتعاون القضائي:

تُواجه الدول تحديات ملموسة في مجال مكافحة الجريمة السيبرانية بسبب التفاوت البنيوي في تشريعاتها الداخلية، وهو ما يعوق فعالية التعاون الدولي، خصوصًا في ما يتعلق بتنفيذ مذكرات التوقيف وتبادل الأدلة الرقمية.

فعدم انسجام التشريعات الوطنية مع الاتفاقيات الدولية يؤدي إلى ثغرات قانونية تُستغل من قبل المجرمين مما يتطلب إعادة هيكلة المنظومات القانونية لتتوافق مع المعايير المعتمدة عالميًا [2] لأجل تعاون دولي في مجال السيبرانية فأهمية ملاءمة الإطار القانوني الوطني مع المعايير الدولية يعتبر كخطوة حاسمة نحو تفعيل دور الدولة في إطار تعاوني دولي لمكافحة التهديدات الرقمية العابرة للحدود[3], ويُستنتج من ذلك أن مواءمة التشريعات لم تعد خيارًا بل ضرورة استراتيجية لتعزيز السيادة الرقمية الوطنية.

ثالثًا: اعتماد مقاربات تشاركية في صياغة السياسات السيبرانية:

إن النجاح في بناء منظومات تشريعية رقمية فاعلة رهينٌ باعتماد مقاربات تشاركية تشمل كافة الفاعلين المعنيين، من مؤسسات رسمية، ومنظمات دولية، وخبراء قانونيين وتقنيين، فضلًا عن المجتمع المدني. وقد أكدت الدراسات السابقة أن الانفراد في صناعة القرار القانوني يؤدي إلى نصوص معزولة لا تستجيب لواقع التهديدات المتغيرة[4]، فإرساء امن سيبراني دولي يتطلب منسوبًا

[1]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة. (2024). تصريح غادة والي خلال جلسة الجمعية العامة للأمم المتحدة، 24 ديسمبر 2024. مرجع سابق

[2]- زكرياء، محمد. (2022). المواءمة التشريعية في مكافحة الجريمة السيبرانية. مجلة البحوث القانونية، جامعة الجزائر، العدد 14، ص. 89.

[3]- العازمي، فهد عبد الله عبيد. (2021). دور الاتفاقيات الدولية في مكافحة الجريمة السيبرانية. ورقة بحثية، جامعة الكويت، ص. 76.

[4]- عطوي، مليكة. (2020). نحو مقاربة تشاركية في صياغة السياسات السيبرانية العربية. مجلة الأمن والحكم الراشد، جامعة نايف العربية للعلوم الأمنية، ص. 105.

عاليًا من التعاون المؤسسي وتبادل الخبرات بين الدولية[1]، من ثم فإن المقاربة التشاركية تُعد أداةً إستراتيجية في بناء تشريعات قابلة للتنفيذ في بيئة رقمية عالمية مترابطة.

الفرع الثاني : انشاء مركز دولي موحد في مكافحة الجريمة السيبرانية.

أمام تصاعد التهديد السيبراني بات من الضروري توحيد الجهود الدولية ضمن كيان مؤسسي دولي قادر على التنسيق وتبادل المعلومات وتقديم الدعم للدول الأضعف. ويتناول هذا الفرع اربع نقاط أولًا: أهمية إنشاء مركز دولي موحد لمكافحة الجرائم السيبرانية ثانيا :دور المركز الدولي في توحيد جهود التعاون الدولي ثالثا: آفاق المركز الدولي وتطوير البنى التحتية الإلكترونية الهشة في الدول النامية،رابعا: التحديات والفرص المرتبطة بإنشاء مركز دولي موحد.

أولًا: أهمية إنشاء مركز دولي موحد لمكافحة الجرائم السيبرانية:

في سياق التزايد المستمر للتهديدات السيبرانية العابرة للحدود، تبرز الحاجة الملحة إلى إنشاء مركز دولي موحد يتبنى مهمة التنسيق بين الدول في مواجهة هذه الجرائم. تعتبر اتفاقية بودابست لعام 2001 أول معاهدة دولية في هذا المجال، حيث نصت المادة 23 على "ضرورة التعاون بين الأطراف في التحقيقات والملاحقات القضائية المتعلقة بالجرائم السيبرانية"[2] مما يعكس أهمية توفير منصة دولية لتبادل المعلومات والموارد بين الدول المعنية، من خلال هذه المعاهدة، تعزز الدول قدرتها على مواجهة التهديدات السيبرانية عبر الآليات الدولية المتفق عليها، والتي يمكن أن يتولى المركز الدولي تسهيل تطبيقها بشكل أكثر فعالية.

ويدعم مكتب الأمم المتحدة، هذا التوجه عبر التأكيد على أهمية التعاون الدولي في مكافحة الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات. في هذا السياق صرحت المديرة التنفيذية للمكتب، أن "الاتفاقيات الدولية، بما في ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة

[1]- سراج، إيهاب عبد الفتاح ويوسف، إيهاب محمد. (2019). نحو تشريعات سيبرانية عربية موحدة. المؤتمر العربي للأمن المعلوماتي، جامعة نايف العربية للعلوم الأمنية، ص. 54.
[2]- اتفاقية بودابست . المادة 23 , مرجع سابق.

السيبرانية، تساهم بشكل كبير في تعزيز الجهود العالمية لمكافحة الجريمة السيبرانية"[1] من خلال ذلك، يتضح أن إنشاء مركز دولي موحد يمثل خطوة حيوية نحو ضمان استجابة منسقة وفعالة لهذه الجرائم على مستوى عالمي.

ثانيا :دور المركز الدولي في توحيد جهود التعاون الدولي لمكافحة الجريمة السيبرانية:

إن التنسيق الدولي هو عنصر أساسي لمكافحة الجريمة السيبرانية، وهو ما تسعى اتفاقية بودابست إلى تحقيقه من خلال شبكة الاتصال التي تعمل على مدار الساعة التي تتيح التعاون السريع بين الدول في جمع الأدلة والتحقيق في الجرائم السيبرانية. يمثل المركز الدولي دورًا حيويًا في هذا الإطار، حيث وجوده يكون بمثابة محور للتواصل الفوري بين الدول، مما يعزز كفاءة التحقيقات عبر الحدود ويزيد من قدرة السلطات على تنفيذ الإجراءات اللازمة في أسرع وقت.

وتعكس الاتفاقيات الإقليمية والدولية، مثل الاتفاقية العربية لمكافحة الجرائم الإلكترونية واتفاقيات الاتحاد الأوروبي والاتحاد الإفريقي، التوجه ذاته في تعزيز التعاون الدولي لمكافحة الجرائم السيبرانية. وتؤكد الاتفاقية العربية[2] على ضرورة تبادل المعلومات والخبرات بين الدول العربية وتوحيد التشريعات لمكافحة الجريمة السيبرانية، مما يتطلب من الدول أعضاء المركز الدولي أن تعمل على تطوير استراتيجيات مشتركة للحد من هذه الجرائم العالمية.

ثالثا : آفاق المركز الدولي وتطوير البنى التحتية الإلكترونية الهشة في الدول النامية:

من أبرز التحديات التي تواجه الدول النامية في مكافحة الجرائم السيبرانية هو الهشاشة في البنى التحتية الإلكترونية، وهي مشكلة تؤثر بشكل كبير على قدرتها على مواجهة التهديدات السيبرانية. في هذا السياق، يمثل المركز الدولي دورًا محوريًا في دعم هذه الدول من خلال توفير المساعدة التقنية والفنية لبناء قدراتها الإلكترونية. فالدول النامية تفتقر إلى البنية التحتية التقنية

[1]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة. تقرير حول الجريمة السيبرانية، 2024. مرجع سابق.
[2]- الاتفاقية العربية لمكافحة الجرائم الإلكترونية. جامعة الدول العربية، 2023. مرجع سابق.

المتطورة التي تُمكنها من التصدي للجرائم السيبرانية بشكل فعال، مما يبرز الحاجة إلى تدخل من المركز الدولي لتوفير الدعم الفني.

أكدت تقارير للأمم المتحدة على ضرورة توفير الدعم التقني والتدريب للدول ذات البنى التحتية الهشة، حيث قالت غادة والي، المديرة التنفيذية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة ان بناء القدرات الوطنية والإقليمية في مجال الأمن السيبراني يعد من أولويات الأمم المتحدة لمكافحة الجرائم الإلكترونية[1] لذلك سيكون للمركز الدولي دور كبير في توجيه الجهود العالمية نحو بناء البنية التحتية الإلكترونية التي تلبي احتياجات الدول النامية وتساعدها على مواجهة التهديدات السيبرانية المتزايدة.

رابعا: التحديات والفرص المرتبطة بإنشاء مركز دولي موحد لمكافحة الجرائم السيبرانية:

على الرغم من أن إنشاء مركز دولي لمكافحة الجرائم السيبرانية يعكس خطوة مهمة نحو تعزيز التعاون الدولي، إلا أن هناك العديد من التحديات التي قد تعيق إنشاءه ، تشير الدراسات إلى أن التحديات القانونية والتقنية التي تواجه التعاون الدولي في مجال الأمن السيبراني يتطلب آليات أكثر تطورًا ومرونة لتسهيل هذا التعاون[2], لذا فإن المركز الدولي يجب أن يتعامل مع قضايا تخص التنسيق بين الأنظمة القانونية المختلفة، التي تختلف من دولة إلى أخرى، وضمان التوافق بين التشريعات الوطنية والدولية.

وبالرغم من هذه التحديات، فإن الفرص التي يتيحها المركز الدولي في تطوير البنى التحتية التقنية للدول النامية، وتعزيز التنسيق بين الدول المتقدمة، تمثل محركًا رئيسيًا للحد من الجرائم السيبرانية. فإن المركز سيتيح للدول النامية الوصول إلى التدريب والموارد التقنية اللازمة لتعزيز أمنها السيبراني، مما يفتح المجال لتعاون أوسع وفعال في هذا المجال فمن خلال الاتفاقيات الدولية والإقليمية، مثل اتفاقية بودابست واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، والاتفاقيات الإقليمية تظهر

[1]- تصريح غادة والي، المديرة التنفيذية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة، "دور الأمم المتحدة في تعزيز الأمن السيبراني"، 2023. مرجع سابق

[2]- فهد عبد الله عبيد العازمي , ص 76 .مرجع سابق.

أهمية التعاون الدولي في مواجهة هذه التهديدات. وبالرغم من التحديات القانونية والفنية التي قد تواجه المركز الدولي، فإن الدور الذي سيلعبه في تطوير البنى التحتية الإلكترونية الهشة للدول النامية يشكل فرصة كبيرة لتعزيز الاستجابة العالمية لهذه الجرائم.

الفرع الثالث : تطوير برامج دولية وإرساء ثقافات عالمية حول الأمن السيبراني.

مع تصاعد التهديدات السيبرانية على المستويين الوطني والدولي، برزت الحاجة الملحّة إلى ترسيخ ثقافة أمنية رقمية تقوم على الوعي والتربية الوقائية يتناول هذا الفرع المبادرات الدولية ثم ضرورة التعليم والاعلام في الوقاية ثم دور التشريعات الوطنية في مجال الوعي الرقمي.

أولًا: المبادرات الدولية في تعزيز الثقافة السيبرانية:

دعت الاتفاقيات الدولية والإقليمية و المنظمات العالمية على تسليط الضوء على ضرورة تطوير مقاربات شاملة لمكافحة الجريمة السيبرانية، ليس فقط من خلال التعاون القضائي والأمني، بل كذلك من خلال نشر الوعي المجتمعي والثقافة السيبرانية، وذلك باعتبارها خط الدفاع الأول ضد التهديدات الرقمية وقد أبرزت تقارير صادر عن وكالات أوروبية[1] أن السلوكيات البشرية تشكل في كثير من الأحيان الثغرات الأخطر في أنظمة الأمن المعلوماتي، ما يتطلب استهداف الأفراد ببرامج توعوية منهجية ودائمة.

ثانيًا: ضرورة التعليم والإعلام في الوقاية من الجريمة السيبرانية:

وحسب الدراسات حول خسائر الاقتصاد العالمي الناجمة عن الجريمة السيبرانية بلغت مستويات غير مسبوقة[2]، فهو ما حوّل التوعية من خيار إلى ضرورة إستراتيجية فإدماج مفاهيم الأمن السيبراني في البرامج الدراسية وتكثيف التكوين المهني، يعدّ أحد المداخل الأساسية لتقوية مناعة

[1]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق.
[2]- لوكالة الأوروبية للأمن السيبراني(ENISA) ، "إرشادات الثقافة السيبرانية: الجوانب السلوكية للأمن السيبراني"، 2019. تم الاطلاع يوم : 12/04/2025، سا 19:50 رابط الوثيقة:
: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

المجتمعات تجاه التهديدات الرقمية فا الثقافات الرقمية الراسخة تمثل شرطا أساسيا لتحقيق التنمية المستدامة والأمن العالمي الشامل.

ثالثًا: دور التشريعات الوطنية في نشر الوعي الرقمي:

لعبت بعض التشريعات الوطنية، دورا هاما في مجال مكافحة الجريمة السيبرانية ومن المبادرات الرائدة في هذا المجال، اعتماد بعض الدول العربية—كالمغرب وتونس والإمارات—لبرامج مدرسية وجامعية تتضمن حصصًا في "الثقافة السيبرانية."

والقانون الجزائري رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي[1]، دورًا تأسيسيًا في ترسيخ مبادئ الخصوصية والأمن السيبراني من خلال فرض ضوابط على الجهات الفاعلة وتوجيه المجتمع نحو التعامل الآمن مع الفضاء الرقمي ,كما تضمنت السياسات التعليمية الرسمية توجهًا لإدماج الثقافة الرقمية والسلامة السيبرانية في المناهج الدراسية عبر برامج مدرسية وجامعية، بالإضافة إلى حملات تحسيسية تستهدف فئات المجتمع المختلفة، خاصةً النساء والأطفال الذين يمثلون الفئات الهشة.

رابعًا: أفق التنسيق الدولي والتثقيف العابر للحدود:

تُعتبر اتفاقية بودابست مرجعًا قانونيًا مهمًا في مجال التعاون الدولي السيبراني، إلا أنها، كما تشير المادة 23 منها، لا تكتفي بالتجريم والتعاون الفني، بل تدعو ضمنيا إلى تقوية القدرات المؤسساتية والتثقيفية للدول الأعضاء[2], وهو ما يدفع نحو التفكير في وضع برنامج تثقيفي عالمي موحّد بإشراف مركز دولي مختص، يُعنى بتوحيد الرسائل التوعوية وتبادل أفضل الممارسات في هذا المجال، خاصة في الدول النامية التي تعاني من هشاشة في البنية التحتية الإلكترونية والتعليم الرقمي.

[1]- الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.
[2]- مجلس أوروبا، اتفاقية بودابست , المادة 23، مرجع سابق

خلاصة الفصل الثاني:

إنّ الجريمة السيبرانية، بطابعها اللامرئي والعابر للحدود، فرضت على المجتمع الدولي واقعًا جديدًا يستدعي تجاوز الأطر التقليدية للتعاون. وقد بيّن هذا الفصل أن مكافحة هذا التهديد لا يمكن أن تتم إلا عبر ميثاق عالمي مشترك تُصهر فيه الإرادات السياسية، والتقنيات الأمنية، والشراكات بين مختلف الفاعلين، من مؤسسات دولية، وأجهزة أمنية، وشركات تكنولوجية، ومجتمع مدني. كما أظهر أن غياب توازن تقني وتشريعي بين الدول يُقوّض جهود المكافحة، ويُكرّس الفجوة بين شمال متقدّم وجنوب هشّ. لكن، وبرغم هذه العوائق، فإن الأمل يظل معقودًا على بناء منظومة تضامن إلكتروني عالمي، تقوم على الثقة، والشفافية، وتوحيد الجهود، لصون السيادة الرقمية، وحماية الأمن والسلم الدوليين من عبث هذا الخطر غير التقليدي.

خاتمة

في عالم يتقاطع فيه الفضاء الرقمي مع كل مناحي الحياة، ويتحوّل فيه التطور التكنولوجي من وسيلة تمكين إلى ساحة صراع وتهديد، برزت الجريمة السيبرانية كأحد أعقد التحديات التي تواجه المجتمع الدولي، لا من حيث تعقيدها التقني فحسب، بل من حيث اتساع نطاقها وتعدد أبعادها القانونية والأمنية والإنسانية. وقد أظهرت هذه الدراسة أن مكافحة هذا النمط الجديد من الإجرام لم تعد رهينة التشريعات الوطنية أو المساعي المنعزلة، بل باتت تتطلب منظومة تعاون دولي متماسكة، قائمة على التنسيق القانوني، وتبادل المعلومات، وتوحيد الجهود الوقائية والردعية.

لقد كشفت فصول هذه المذكرة من خلال تحليل الآليات الدولية متعددة الأطراف، أن المجتمع الدولي قد خطى خطوات معتبرة في سبيل بلورة إطار قانوني عابر للحدود، كما هو الحال مع اتفاقية بودابست، واتفاقية الأمم المتحدة لعام 2024، والجهود الحثيثة لمكتب الأمم المتحدة المعني بالمخدرات والجريمة، غير أن هذه المبادرات، ورغم أهميتها، ما زالت تواجه تحديات في التفعيل والتنفيذ، لا سيما في ظل التفاوت الرقمي، وهشاشة البنى التحتية، وضعف التنسيق بين النظم القانونية الوطنية.

كما أبان البحث أن أفق المواجهة الفعالة للجريمة السيبرانية لا يقف عند حدود التجريم والعقاب، بل يمتد إلى ترسيخ ثقافة رقمية عالمية قائمة على التوعية، والتعليم، والوقاية، وذلك عبر تطوير برامج تربوية، وإدماج مفاهيم الأمن السيبراني في المدارس والجامعات، فضلاً عن تفعيل دور التشريعات الوطنية في بناء مواطن رقمي واعٍ ومحصّن. وقد برزت الحاجة الملحّة إلى إنشاء مركز دولي موحّد لتنسيق الجهود، وتطوير البنى السيبرانية، وتقديم الدعم الفني والتقني للدول النامية، بما يعزز العدالة الرقمية ويقلّص فجوات المواجهة.

وعليه فإن الرهان الأكبر في مواجهة هذا التحدي المتسارع لا يكمن في تطويق الجريمة السيبرانية فحسب، بل في صياغة نموذج عالمي مشترك للأمن الرقمي، قائم على قيم التضامن، والعدالة، والابتكار. وهو ما يجعل من هذه المذكرة، رغم محدودية إطارها الزمني والبحثي، دعوةً مفتوحةً

لإعادة التفكير في المقاربة الجنائية المعتمدة حيال الجريمة السيبرانية، والانخراط في مشروع إنساني عالمي يضمن أمن الفضاء الرقمي وعدالته لجميع الشعوب، دون إقصاء أو تمييز.

إن تعقيد الجريمة السيبرانية وامتدادها عبر الحدود يجعل من التعاون الدولي ضرورة لا غنى عنها لمواجهتها بفعالية، فغياب توحيد قانوني عالمي يؤدي إلى التفاوت في تعريفات الجريمة السيبرانية وأساليب مكافحتها بين الدول، فرغم أن اتفاقية بودابست 2001 تمثل الإطار القانوني الدولي الأبرز، إلّا أنها لا تغطي كافة أوجه الجريمة السيبرانية وتحتاج لتطوير مستمر.

كما أن الأدوار الحيوية للمنظمات الدولية مثل الأمم المتحدة، الإنتربول، واليوروبول، كان لها الدور الأبرز في تعزيز التعاون القضائي والأمني بين الدول من خلال تبادل المعلومات الفوري والموثوق بين الأجهزة الأمنية والقضائية قصد إنجاح وسائل مكافحة الجرائم السيبرانية.

وسيرا نحو تفعيل الشراكات فكان لابد من إحداث قرابة بين القطاعين العام والخاص، خاصة فيما تعلّق بإحداث تقارب بين شركات التكنولوجيا، لما لها من أدوار بارزة في تعزيز من قدرات الدول في رصد ومنع الهجمات السيبرانية، كما أن للمجتمع المدني والمنظمات غير الحكومية أهمية كبرى في توعية ودعم الأطر القانونية والتقنية.

ومما يعيق بناء تعاون موحد ومستدام نجد تلك التحديات السياسية مثل التوترات الجيوسياسية واختلاف المصالح الوطنية كلها تقف حائلا دون إنشاء مركز دولي موحد –لمكافحة الجريمة السيبرانية– يعزز التنسيق وتبادل الخبرات والموارد بشكل مركز وفعال، ويطرح برامج دولية وتوعوية عالمية لترسيخ ثقافة أمن سيبراني مشتركة والتقليل من مخاطر الجريمة السيبرانية على الأمن والسلم الدوليين.

وللعوائق الاقتصادية ونقص التمويل دور في الحد من قدرات الدول على تطوير بنية تحتية قوية لمكافحة الجرائم السيبرانية، يتبعها التفاوت في القدرات التقنية والفجوة الرقمية العالمية مما أدى إلى عدم توازن في مشاركة الدول ضمن الأطر الدولية.

ومنه يمكننا إراد جملة من الاقتراحات التي من شأنها أن تساهم في تعزيز المخرجات القانونية والتنظيمية للمنظمات غير الحكومية والدول، مثل: تطوير إطار قانوني دولي شامل ومتكامل يحدّد بوضوح تعريفات الجرائم السيبرانية ويواكب التطورات التقنية الحديثة، وذلك بإنشاء مركز دولي موحد متخصص في التنسيق بين الدول لتبادل المعلومات والخبرات وإدارة الأزمات السيبرانية بسرعة وكفاءة.

تعزيز الشراكة بين القطاعين العام والخاص من خلال وضع أطر تعاون رسمية مع شركات التكنولوجيا والاتصالات لتبادل المعلومات الأمنية والدعم التقني، وتطوير آليات تمويل دولية مخصصة لدعم مشاريع وبنية تحتية أمنية في الدول ذات القدرات الضعيفة، وتوفير برامج تدريبية وتمكين تقني للدول النامية لسد الفجوة الرقمية وتعزيز القدرات المحلية في مواجهة التهديدات السيبرانية.

تبني إستراتيجية توعية عالمية مستمرة تستهدف الحكومات، المؤسسات، والمواطنين لرفع مستوى الثقافة الأمنية للحد من الجرائم الإلكتروني، وتعزيز التعاون القضائي الدولي عبر تبسيط إجراءات تسليم المجرمين والتعاون في التحقيقات والملاحقات القضائية.

وفي المجالين الأكاديمي والاجتماعي يمكن دعم البحث والتطوير في مجال الأمن السيبراني لتعزيز الأدوات والتقنيات الحديثة لمكافحة الجرائم السيبرانية بفعالية، وتشجيع دور المجتمع المدني والمنظمات غير الحكومية في تقديم الدعم القانوني والتقني والتوعوي لتعزيز جهود مكافحة الجريمة السيبرانية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

1- المصادر:

أ- القوانين :

- قانون الاجراءات الجزائية الجزائري، المواد 694 -698 المعدل و المتمم بموجب القانون رقم 18/04 سنة 2018

ب- الاتفاقيات الدولية :

- اتفاقية بودابست ، مجلس اوروبا بشأن الجريمة السيبرانية 2001/11/23 رقم المعاهدة 185

- جامعة الدول العربية ، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010

- الجمعية العامة للامم المتحدة ، القرار 247/74 بشان مكافحة استخدام تكنولوجياا المعلومات و الاتصال لاغراض اجرامية 2019

- الامم المتحدة ، اعلان الدوحة بشان منع الجريمة و العدالية الجنائية ، المؤتمر 13 الدوحة 2015 .

- الاتحاد الافريقي ، الاتفاقية بشأن الامن السيبراني و حماية البيانات الشخصية (اتفاقية مالابو2014)

- مجلس وزراء الداخلية العرب ، التقرير العربي الموحد حول الجريمة السيبرانية تونس 2021

- مجلس اوروبا ، الاتفاقية الاوروبية لتسليم المجرمين باريس ، 1957

- مجلس حقوق الانسان التابع للامم المتحدة ، التعليق العام رقم 25 /2021 بشأن حقوق الاطفال

ج- القوانين العادية :

- القانون الجزائري رقم 18/04 المؤرخ في 10 ماي 2018 ، الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، ج.ر.ج.ج العدد27 – المادة 43 - 2018

-القانون رقم 07/18 المؤرخ في 10 جوان 2018 المتضمن حماية الاشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي ج . ر .ج.ج عدد 35 -2018

-القانون رقم 04/18 المؤرخ بتاريخ 10 ماي 2018 المتضمن حماية الاشخاص من الجرائم المتعلقة بتكنولوجيا الاعلام و الاتصال ج .ر .ج .ج العدد 27 المادة 43 لسنة 2018

- القانون رقم 22/06 المؤرخ في تاريخ 20 ديسمبر 2006 المعدل و المتمم للامر 66/115 النمتعلق بقانون الاجراءات الجزائية ج.ر.ج.ج العدد84 سنة 2006

د- القوانين الاجنبية باللغة العربية :

-القانون المصري رقم 2018-175 الباب الاول الاحكام العامة، التعريفات المادة 15 المتضمن قانون مكافحة جرائم تقنية المعلومات ج.ر.ج.م 2018

- القانون الاردني رقم 17 سنة 2015 الخاص بالجرائم الالكترونية ج.ر.م.أ بتاريخ 12 اوت 2023

-توجيه البرلمان الاوروبي و المجلس رقم 2016 /1148 جوان 2016 المتضمن تدابير تحقيق مستوى عالي من امن الشبكات و نظم المعلومات في الاتحاد

هـ– المعاجم :

– المعجم الوسيط ، معجم اللغة العربية ، ط04 ، دار الدعوة القاهرة ، 2004

– مجمع اللغة العربية ، القاهرة ، معجم المصطلحات التقنية ، اصدر المنظمة العربية للترجمة ، بيروت 2015

– جامعة الدول العر بية ، الامانة العامة ، المعجم القانوني الموحد للمصطلحات الالكترونية ، القاهرة 2017

2– المراجع العامة :

– زكريا محمد ، الموائمة التشريعية في مكافحة الجريمة السيبرانية ، مجلة البحوث القانونية ، جامعة الجزائر ،ع2022 14 ص 89

– العازمي فهد عبدالله عبيد ، دور الاتفاقيات الدولية في مكافحة الجريمة السيبرانية ورقة بحثية جامعة الكويت ص76

– بوثلجة سمير ، الجريمة المعلوماتية ، دراسة في القانون الجزائرية و المقارن ، دار هومة ، الجزائر 2013

– محمد نجيب حسني ، شرح قانون العقوبات ، القسم العام ، دار النهضة العربية ، القاهرة ط05 ، 1998

– احسن بوصقيعة ، الوجيز في القانون الجنائي العام ، دار هومة ، الجزائر ط07 ،2013

– احسن بوصقيعة ، الوجيز في القانون الجنائي العام ، دار هومة ، الجزائر ط05 ،2018

– نهلة عبدالقادر المومني ، الجرائم المعلوماتية ، دتار الثقافة و التوزيع الاردن ،ط01 ، 2008

– عبدالله منصور ، الجرائم الالكترونية في القانون الجنائي ، دار الفكر الجامعي ، الاسكندرية 2020

– محمد زكي ابو عامر ، علي عبدالقادر القهوجي ، قانون العقوبات ، القسم الخاص، د.ط دار النهضة العربية ، القاهرة 1993

– بن عزوز عبدالعلي ، الجرائم الالكترونية و التحديات الامنية في الفضاء السيبراني ، دار المعرفة ، الرباط 2021

– خلف حسين ، الجريمة المنظمة في العصر الرقمي ، دراسة تحليلية ، دار السنهوري بغداد 2021

–الدجنى أسامة ، السيادة الرقمية في فلسطين و مخاطر الاحتلال السيبراني ، المرطز الفلسطيني لابحاث السياسات ، رام الله 2021

– عبدالفتاح محمد سراج ، النظرية العامة لتسليم المجرمين ، دار النهضة العربية ، القاهرة 1999

– احمد الخمليشي ، شرح قانون المسطرة الجنائية المغربي ، ج02 دار المعرفة الرباط2012

– ايهاب محمد يوسف ، اتفاقية تسليم المجرمين و دورها في تحقيق التعالون الدولي لمكافحة الارهاب ، القاهرة 2003

–اجمد عبدالله ، الجريمة السيبرانية ، التحديات القانونية و التقنية في العصر الرقمي ، دار الفكر العربي القاهرة 2020

– محمد زكريا ، القانون الجنائي و التكنولوجي الحديث ، دراسة في الجريمة السيبرانية ، دار النهصة العربية بيروت2019

– تويجري عبدالله عبدالعزيز، التعاون الدولي في مكافحة الجرائم السيبرانية ، دراسة في ضوء القانون الدولي العام ، الرياض مكتبة القانون و الاقتصاد 2014

3– المراجع المتخصصة :

– مركز الابحاث الفلسطيني ، العدوان على غزة ، عزل رقمي ضمن عدوان عسكري ، غزة 2023

- مكتب الامم المتحدة المعني بالمخدرات و الجريمة لعام 2013

- التقرير التفسيري لاتفاقية بودابست ، اتفاقية الجريمة السيبرانية ، المعاهدة رقم 185 ، 2001

- المفوضية الاوروبية ، استراتيجية الاتحاد الاوروبي للامن السيبراني ، فضاء الكتروني امن و مضمون ، بروكسل 2013

- منظمة التعاون الاقتصادي و التنمية (OFCD) اطار سياسات الامن الرقمي 2022

- تقرير المعهد الدولي للسلام عن الجريمة السيبرانية العابرة للحدود و الاستخبارات القانونية العالمية 2021

- المنظمة الدولية للشرطة الجنائية (INTERPOL) النظام الاساسي 2016

- وكالة الاتحاد الاوروبي للتعاون في انفاذ القانون (اليوروبول) اللائحة رقم 794 – 2016 معلومات حول النظام SIENA

- تحالف التهديدات السيبرانية – من نحن – CTA 2014

4– الأطروحات و المذكرات:

أ– الأطروحات.

- لخضر دهيمي ، النظام القانوني لعمل الشرطة في الجزائر ، اطروحة دكتوراه في الحقوق جامعة البليدة 2 ،2015

- سعيد شادي ، اليات التعاون القضائي في مجال مكافحة الجريمة السيبرانية ، رسالة دكتوراه ، جامعة سطيف ،2021.

ب– المذكرات:

- سامية عبدالوهاب ،الجريمة الالكترونتية أو السيبرانية ، مذكرة ماستر ، جامعة القاهرة ، 2016 /2017

- الطالبة عبير علي محمد النجار ، تحت اشراف الدكتولر مازن اسماعيل هنية ، جرائم الحاسب الالي في الفقه الاسلامي ، مقدمة لنيل درجة الماجستير ، كلية الشريعة و القانون بالجامعة الاسلامية بغزة سنة 2009

- بولنوار حنان ، الارهاب السيبراني كتهديد للامن القومي ، مذكرة ماستر ، جامعة الجزائر 02 قسم الحقوق و العلوم السياسية 2021/2020

- نجاتي سهيلة ، راهم اميرة ، الهجمات السيبرانية و اثرها على تهديد السلم و الامن الدوليين ، مذمكرة لنيل شهادة ماستر في تالقانون جامعة ورقلة ، 2024/2023

- عبد المنعم محمد مجدي خليفة ، التغلب على تضارب الاختصاص في الجرائم الالكترونية ، رسالة ماجستير ، الجامعة الامريكية ، القاهرة 2021/2020

- جيري فاطمة ، الركائز القانوني للامن السيبراني في القانون الدولي العام ، مذكرة ماستر، جامعة الجزائر 01 2022/2021

- عبداللطيف نسرين ، التحديات القانونية لمواجهة الجريمة السيبرانية الدولية ، مذكرة ماستر ، جامعة وهران 02،2019

5- **المقالات العلمية :**

- زكريا محمد ، الموائمة التشريعية في مكافحة الجريمة السيبرانية ، مجلة البحوث القانونية ، جامعة الجزائر ،ع2022 14 ص 89

- العازمي فهد عبدالله عبيد ، دور الاتفاقيات الدولية في مكافحة الجريمة السيبرانية ورقة بحثية جامعة الكويت ص76

- خليفة محمد ، امن افلفضاء السيبراني بين مقتضيات الحماية و حقوق الانسان الرقمية، مجلة الدراسات القانونية و السياسية ، ع 18 ، 2021

- رضا مهدي ، الجرائم السيبرانية و اليات مكافحتها ، مجلة لنيل البحوث و الدراسات ، مج 06 ، ع 02 ،2021

- واجعوط سعاد ، مكافحة الجريمة السيبرانية على المستوى الوطني ، مجلة البحوث العلمية، المركز الجامعي بتيبازة مج12,ع 02 ،2018

- سي حمدي عبدالمومن ، قيرة سعاد ، الجريمة الالكترونية و اليات التصدي لها في البقانون الجزائري ، مجلة البنيان للدراسات القانونية و السياسية مج 07، ع 01 ،2021

- لامية طالة ، المخذرات الرقمية ، الادمان الجديد في تالفضاء السيبراني ، مجلة الرسالة للدراسات الاعلامية ، مج06، ع01 ،2020

-حسام أحمد كيلاني علي ، الدليل الرقمي و معوقات اثبات الجريمة الالكترونية ، مجلة البحوث الفقهية و القانونية ، جامعة الازهر، كلية الشريعة و القانون ، ع 47 ، 2024

- الطاهر باكر ، مكافحة الجريمة الالكترونية بين التشريعات الوطنية و الاتفاقيات الدولية ، مجلة الصدى للدراسات القانونية و السياسية مج04، ع 04، 2022

- قطاف سليمان بوقرين عبدالحليم ، مواجهة الجرائم السيبرانية في ضور الاتفاقيات الدولية ، مجلة البحوث القانونية و الاقتصادية ، مج 05 ،ع02 ، 2022

- عواد محمد ، الجهود القانونية لمكافحة الجريمة السيبرانية بين الطموح و التنفيذ ، مجلة دراسات الجريمة السبرانتية ، مج 02 ،ع 01 ،2018

دراسة حول الاطار القانوني للامن السيبراني في دول مجلس التعاون الخليجي ، مجلة دراسات الخليج و الجزيرة العربية ، ع 113 ، 2018

- مليكة عطوي ، الجريمة الالكترونية ، مجلة حوليات ، ع12 ، جوان2012

- محمود ايمان ، دور المنظمات الدولية في تعزيز الامن السيبراني العالمي ، مجلة السياسة الدولية ، ع 121 سنة 2020

6- المداخلات علمية :

- ناصري سميرة ، بسمة ترغيني ، دور المجتمع المدني في مكافحة الجريمة المنظمة ، مداخلة علمية بكلية الحقوق جامعة خنشلة 2014.

7- المواقع الالكترونية :

https://ar.m.wikipidia.org/wiki

https://www.europol.eu/ioctu.2022

المفوضية الاوروبية pa.eu.2020https://eur.lex/euro

توجيه البرلمان الاوروبي https://eur.europa/eu/eli/dit2016

الاتحاد الافريقي https://au.int/enltreaties/african-union

المكتب الاتحادي لامن المعلومات المانيا https://wwweuro.pardct.com

امن المعلومات الفرنسي comhttps://www.diplomatie.gouv.f

قانون الامن السيبراني- الصين https://www.youm7.com

منظمة التعاون الاقتصادي و التنمية https://www.oecd.org.2022

المعهد الدولي للسلام https://www.ipnst.org

انتربول https://www.interpol/int

النظام الاساسي االيوروبول

https://eur-lex.europa.eureur-lex

المجمع العالمي للابداع الانتربول https://www.interpol.int/en/crime

تحالف التهديدات اسيبرانية https://www.cyberthreatalliance.org/about

فهرس المحتويات

-فهرس المحتويات-

ملخص المذكرة:

مع تسارع العصر الرقمي وتغلغل التكنولوجيا في كل مناحي الحياة، باتت الجريمة السيبرانية تهديداً حقيقياً للأمن والسلم الدوليين، نظراً لعبورها للحدود وتعقيدها الفائق. تكشف هذه الدراسة أن التصدي لهذا التحدي يستلزم تعاوناً دولياً متكاملاً في إطار قانوني مرن يواكب التطورات التقنية، يجمع بين الحكومات والمنظمات والقطاع الخاص. ورغم الجهود المبذولة، يظل غياب إطار قانوني موحد واختلاف قدرات الدول الفنية والسياسية من أبرز المعوقات. لذلك، تتطلب مكافحة الجريمة السيبرانية بناء منظومة دولية قوية تُعزز التعاون القضائي، وتبادل المعلومات، وترسيخ الوعي العالمي بخطورتها. إن التصدي لهذا الخطر يستوجب إرادة سياسية مشتركة وتضامناً دولياً لحماية الاستقرار العالمي في زمن الرقمنة المتسارع.

In the accelerating digital era, with technology permeating all aspects of life, cybercrime has become a real threat to international peace and security due to its cross-border nature and high complexity. This study reveals that addressing this challenge requires integrated international cooperation within a flexible legal framework that keeps pace with technological advances, uniting governments, organizations, and the private sector. Despite ongoing efforts, the lack of a unified legal framework and disparities in states' technical and political capabilities remain major obstacles. Hence, combating cybercrime demands building a strong international system that enhances judicial cooperation, information exchange, and global awareness of its dangers. Confronting this threat requires shared political will and international solidarity to protect global stability in a rapidly digitizing world.