الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة عبد الرحمان ميرة –بجاية–

كلية الحقوق والعلوم السياسية

قسم القانون العام

آليات مكافحة الجرائم السيبرانية في إطار القانون الدولي

مذكرة لنيل شهادة الماستر في القانون العام

تخصص القانون الدولي العام

من إعداد الطالب:

وشان عبد الله

تحت إشراف الأستاذ:

د. قدوم محمد

أعضاء لجنة المناقشة

الأستاذ: د. منعة جمال ..... أستاذ محاضر "أ" ..... رئيسا

الأستاذ: د. قدوم محمد ..... أستاذ محاضر "أ" ..... مشرفا ومقررا

الأستاذ: د. بوخلو مسعود ..... أستاذ محاضر "أ" ..... ممتحنا

السنة الجامعية: 2024-2025

« La Cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires. »

Colin Rose

شكر و تقدير

الحمد لله الذي وفقني في إنجاز هذه المذكرة المتواضع

والصلاة والسلام على سيدنا محمد خاتم الأنبياء والمرسلين.

أما بعد

أتقدم بالشكر الجزيل والامتنان للأستاذ الفاضل "**د. قدوم محمد**" على إشرافه في إنجاز هذه المذكرة من خلال المتابعة الدائمة بالنصائح والتوجيهات.

كما أتقدم بالشكر الجزيل لكل الأساتذة الأفاضل في كلية الحقوق والعلوم السياسية، خاصة الأستاذ "**معيفي لعزيز**" الذي له الفضل في عودتي للدراسة بعد فترة فراغ مررت بها أدت لتركي الدراسة، حيث آمن بقدرتي على إكمال المسار الدراسي، هذا ما حدث الحمد لله.

أخيرا أتقدم بالشكر الجزيل لكل العائلة الكريمة والأصدقاء على صبرهم معي في فترة إعداد هذه المذكرة، ولكل من ساعدني ولو بكلمة طيبة أو ابتسامة.

وشان عبد الله

إهداء

أهدي ثمرة جهدي المتواضع إلى من كانت دعواتهم سر عطائي، وابتسامتهم نور دربي.. إلى أغلى الناس **أمي الحبيبة** و**أبي العزيز**، من علمني معنى الحياة، وغرس في قلبي قيم الصبر والاجتهاد.

إلى **جدتي** الغالية.

إلى من وهبني الله نعمة وجودهم في حياتي إلى العقد المتين من كانوا عونا لي **إخوتي**، وإلى أبناء أخي وأختي.

إلى كل أفراد عائلتي الكريمة.

إلى أصدقائي الأوفياء داخل الوطن وخارجه.

إلى زملائي من تقاسمنا معا رحلة العلم والمعرفة، وعشنا لحظات الجد والاجتهاد، أتمنى أن تدوم صداقتنا رغم انتهاء مشوارنا الدراسي، حقا كانت أوقات جميلة.

إليكم جميعا، أهدي ثمرة هذا العمل عربون وفاء واعتراف بجميل لا ينسى.

وشان عبد الله

قائمة المختصرات

أولا: باللغة العربية

الأفريبول: منظمة الشرطة الجنائية الإفريقية.

الإنتربول: المنظمة الدولية للشرطة الجنائية.

ج.ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

د.ب.ن: دون بلد النشر.

د.س.ن: دون سنة النشر.

ص ص: من الصفحة إلى الصفحة.

ص: الصفحة.

ع: العدد.

م: المجلد.

ثانيا: باللغة الفرنسية

p: page.

p.**p**: page à page.

s.**l**: sans lieu

s.**d**: sans date

مقدمة

تعد الجريمة ظاهرة قديمة ارتبطت بوجود الإنسان، وتطورت بتطور الوسائل والأساليب التي يستخدمها، وظلت كذلك الى غاية عصر التنظيم الدولي حيث عمد المجتمع الدولي إلى وضع قانون دولي يسعى لتحقيق السلم والأمن الدوليين من خلال العمل على مكافحة الجرائم الدولية ومعاقبة مرتكبيها، خاصة مع بروز القانون الدولي الجنائي وتطوره بوضع نظام روما للمحكمة الجنائية الدولية.

غير أن الوضع تغير مع التطور التكنولوجي الذي عرفه العالم، فقد ظهر نوع جديد من الجرائم تسمى بالجرائم الالكترونية أو كما تسمى أيضا بالجرائم السيبرانية[1]، كان أول ظهور للجرائم السيبرانية مع بداية بروز الثورة الصناعية وبداية صناعة الحواسيب، حيث تم تسويق أول جهاز كمبيوتر في الخمسينيات القرن الماضي، ومع بداية استعماله التجاري ظهرت جرائم الحاسوب، ولكن كانت جرائم بسيطة تقتصر على إساءة استخدام الحاسوب على البعد الأخلاقي، وتم تسجيل أول جريمة إلكترونية في الولايات المتحدة الأمريكية سنة1957[2].

شاع استخدام الحاسوب في الستينات وسبعينات القرن الماضي وازدادت إساءة استخدامه، أما في فترة الثمانينات فقد ظهرت أنشطة الفيروسات الإلكترونية التي تقوم بتدمير

[1] **Rosé (P)**, la criminalité informatique, QSJ, Paris, s.d, p125.

[2] **عفاف بعون، نسيمة أولاد سالم،** "الجريمة الالكترونية–قراءة سوسيوتاريخية في النشأة والأثار–"، مجلة القبس للدراسات النفسية والإجتماعية، م 05، ع20، 2023، ص72.

الملفات والبرامج مثلما حدث في قضية مورس[1]، كما أطلق اسم "**الهاكرز**" على مرتكبي الجرائم السيبرانية[2].

غير أنه ابتداء من فترة التسعينات إلى يومنا هذا تطورت الجرائم السيبرانية بشكل رهيب خاصة مع ظهور الانترنت وانتشاره السريع على مستوى الدولي حيث جعل العالم على شكل قرية صغيرة، مما سهل تفشي هذه الجرائم وصعب من متابعتها.

تعد الجرائم السيبرانية من الجرائم المستحدثة مقارنة بالجرائم التقليدية، وذلك بسبب ارتباطها بأجهزة الحاسوب والأنترنت، ويختلف مرتكبي الجرائم السيبرانية عن غيرهم من مرتكبي الجرائم التقليدية في احترافهم ومهارتهم في استخدام أجهزة الكمبيوتر والإنترنت.

ولأجل احتواء الجرائم السيبرانية كان من الأولى ضبط تعريفه حتى لا يختلط بمفاهيم أخرى ذات الصلة رغم صعوبة ذلك[3]، وقد وضعت تعريفات عدة لهذا المفهوم من خلال الاتجاهات القانونية والفقهية التي تراوحت بين التضييق والتوسيع، وقد عرفها مؤتمر الأمم

---

[1] تعد حادثة "**دودة مورس**" من أوائل الهجمات الخطيرة التي استهدفت أجهزة الحاسوب، في شهر نوفمبر سنة 1988 قام طالب يدعى روبرت مورس يبلغ من العمر 23 سنة بإطلاق فيروس عبر الإنترنت يعرف بدودة مورس، وقد تسبب هذا الفيروس في إصابة حوالي 6000 جهاز كمبيوتر متصل بحوالي 60 ألف نظام عبر الشبكة ومن بينها أجهزة تابعة لجهات حكومية، حيث بلغت الخسائر الناتجة عن إصلاح الأنظمة المتضررة وكذا تشغيل المواقع المتوقفة بسبب الفيروس حوالي 100 مليون دولار وخسائر غير مباشرة بسبب تعطل الأنظمة، بعد القبض على مورس حكم عليه بالسجن لمدة 3 سنوات مع غرامة مالية قدرها 10 آلاف دولار. راجع: **شريف حسين محمد محمد**، الجرائم الإلكترومعلوماتية "مفهوم جديد في جرائم الوسط الجيوسيبراني"، دار النهضة العربية، د.ب.ن، 2022، ص139.

[2] الهاكرز: هو الشخص الذي يمتلك مهارة عالية في البرمجة وأنظمة الحاسوب، ويستخدمون مهاراتهم لاختراق الأنظمة والتلاعب بها، نجد منهم من يستخدم مهاراته لأغراض غير مشروعة، كما يمكن أن يمكن استخدامها للأغراض مشروعة منها التصدي للهاكرز الغير مشروع، راجع: **ربيعي حسين**، "المجرم المعلوماتي–شخصيته وأصنافه–"، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، م15، ع01، 2015، ص 296.

[3] **Chawki (M)**, Essai sur la nation de cybercriminalité, IEHEI, s.l, 2006, P06.

المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المقام في فيينا عام 2000، على أنها "أي جريمة ترتكب باستخدام نظام حاسوبي أو شبكة إلكترونية، ويشمل هذا التعريف جميع الجرائم التي يمكن تنفيذها في بيئة رقمية"[1].

أما على المستوى الفقهي فهناك من يرى أن الجريمة السيبرانية هي "مجموعة من الأفعال غير المشروعة التي يجرمها القانون، وتكون مرتبطة بالمعالجة الإلكترونية للمعلومات أو نقلها، كما نشير إلى أن الجرائم السيبرانية قد تكون أي سلوك غير قانوني يتم باستخدام الحاسوب وغرضه تحقيق أهداف غير مشروعة"[2].

عموما تشمل الجريمة السيبرانية أي سلوك ضار يقوم به الفرد عبر استعمال جهاز الكمبيوتر والشبكة العالمية (الإنترنت)، بحيث يشكل هذا السلوك جريمة في حالة استخدام الحاسوب كأداة أساسية لارتكاب فعل غير مشروع.

بعد التطرق إلى مختلف التعريفات الخاصة بالجريمة السيبرانية، ونظرا للطبيعة المتميزة لهذه الجرائم فهي تتوفر على خصائص مميزة تميزها عن الجرائم التقليدية، لاسيما أنها ترتكب بواسطة الأجهزة الإلكترونية خاصة أجهزة الحاسوب حيث لا يمكن ارتكاب الجريمة السيبرانية دون استخدام أحد الأجهزة الالكترونية، لا يمكن ارتكاب هذا النوع من الجرائم دون توفر الانترنت، حيث تعتبر الوسيلة الرئيسية التي تسمح لارتكاب الجريمة السيبرانية.

تتميز الجرائم السيبرانية من حيث خصوصية مرتكبيها اذ يعتبر شخص غير عادي بسبب ذكائه ومهاراته في استخدام الأجهزة الالكترونية خاصة الحاسوب، لهذا أطلق عليه

---

[1] **بوقرين عبد الحليم، قطاف سليمان،** "مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية"، مجلة البحوث القانونية والاقتصادية، م05، ع02، 2022، ص 69.

[2] **حسين عباس حميد،** نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية، دار النهضة العربية للنشر والتوزيع، القاهرة، 2021، ص 23.

اسم الهاكرز، فهي سريعة التنفيذ بحيث يمكن ارتكابها في ثواني معدودة وحتى جزء من الثانية.

تتميز الجريمة السيبرانية أنها من الجرائم المرتكبة عن بعد، أي من مسافات بعيدة يمكن أن تكون من دولة أخرى أو قارة أخرى، هذا ما يجعلها تصبح جرائم عابرة للحدود وذلك لعدم اعترافها بالحدود الجغرافية للدول هذا بسبب الشبكة العنكبوتية، كما أن من ميزاتها أنها صعبة الإثبات ويكمن ذلك في أن اكتشافها لا يكون في الوقت المناسب ولا يمكن حصرها في مكان محدد ولا تترك أثرا ماديا، مما يصعب متابعة مرتكبي هذه الجرائم.

مما سبق تبرز أهمية البحث في اعتبار الجرائم السيبرانية من الجرائم الحديثة لارتباطها بالتكنولوجيا هذا ما يسهل تزايد التهديدات السيبرانية عالميا، ذلك بسبب غياب تشريعات موحدة خاصة بمكافحة هذا النوع من الجرائم.

لقد حاول القانون الدولي أن يتصدى للجريمة السيبرانية من خلال وضع نصوص قانونية دولية لتجريم هذا الفعل ومعاقبة مرتكبيه، كما أنشأ في سبيل ذلك جملة من الآليات أو الميكانيزمات قصد ضمان تفعيل وتكريس هذه النصوص عمليا، غير أن الإشكالية المطروحة لا ترتبط أساسا في الاهتمام بوضع القوانين والأجهزة المرافقة لها بقدر ما يتعلق الأمر بالبحث عن نجاعتها وتحقيقها للأهداف المرجوة منها وهذا ما يدفعنا لطرح الإشكالية التالية:

ما مدى فعالية آليات مكافحة الجرائم السيبرانية في إطار القانون الدولي؟

من أجل دراسة مستفيضة لهذا الموضوع اعتمدنا في دراستنا على المنهج الوصفي والتحليلي من خلال وصف الجريمة السيبرانية وتبيان مدى خطورتها، وتحليل النصوص التي جاءت بها الاتفاقيات الدولية والإقليمية التي لها صلة بهذه الجرائم، علاوة على المنهج الاستقرائي وذلك بدعم الدراسة بشواهد ونماذج عملية توثق لنسبية ومتغيرات هذا المنهج.

وقد قسمنا هذه الدراسة إلى فصلين، تطرقنا في الفصل الأول إلى الآليات القانونية والمؤسساتية لمكافحة الجرائم السيبرانية، أما الفصل الثاني فقد تناولنا مسألة فعالية هذه الآليات في مكافحة هذا النمط من الجرائم.

الفصل الأول

الآليات القانونية والمؤسساتية لمكافحة الجرائم السيبرانية

لا شك أن تكريس الآليات الخاصة لمكافحة الجرائم السيبرانية يقتضي أولا وضع النصوص القانونية الدولية منها الإجرائية والموضوعية، علاوة على ضرورة إنشاء أجهزة وآليات دولية تسهر على تطبيق هذه النصوص القانونية، وعليه فإن مكافحة الجرائم السيبرانية يعتمد على وثائق قانونية دولية وأخرى إقليمية، تأتي في مقدمة الآليات الدولية اتفاقية بودابيست التي تجمع الدول الأوروبية خاصة وباقي الدول من القارات المختلفة، أما الاتفاقيات الإقليمية فمن أهمها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات واتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية البيانات الشخصية **(المبحث الأول)**.

أما على المستوى الإجرائي فقد تبنى القانون الدولي مجموعة من الأجهزة الدولية التي تجعل من النصوص القانونية الموضوعية حيز التطبيق وكذا تفعيلها من ناحية الوقاية والمتابعة في آن واحد، وقد كان لهيئة الأمم المتحدة دور في التصدي لهذه الجرائم وذلك من خلال الجمعية العامة ومختلف الأجهزة المتخصصة التابعة لها مثل الإتحاد الدولي للاتصالات، كما سعت المنظمة الدولية للشرطة الجنائية على التصدي لمختلف الجرائم العابرة للحدود من بينها الجرائم السيبرانية وبفضل التعاون الأمني بين مختلف الأجهزة الشرطية مثل الإتحاد الإفريقي للتعاون الشرطي والتعاون الدولي في مختلف المجالات كالتدريب والمساعدة القضائية و أهم شيء وهو تسليم المجرمين **(المبحث الثاني)**.

المبحث الأول: الآليات القانونية لمكافحة الجرائم السيبرانية

إن انتشار الجرائم السيبرانية بشكل واسع وعدم اقتصارها على نطاق جغرافي محدد بل تجاوزت الحدود الوطنية وأصبحت تشكل تهديدا عالميا على الأفراد والدول، ومع تزايد خطورتها وتعقيد أساليبها برزت الحاجة الملحة إلى وضع أطر قانونية فعالة وشاملة لمواجهتها على المستويين الدولي والإقليمي، وقد عملت الدول الأوروبية على وضع نظام قانوني لمكافحة هذا النوع من الجرائم من خلال وصفها لأحكام قانونية دولية ملزمة تسهل التعاون الدولي وكانت اتفاقية بودابست أول اتفاقية لمكافحة هذا النوع من الجرائم **(المطلب الأول)**.

سعت العديد من المنظمات الإقليمية سواء في إفريقيا أو الوطن العربي إلى تبني اتفاقيات وقوانين لمجابهة التحديات المتنامية للجرائم السيبرانية، وكانت اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية البيانات الشخصية المعروفة باتفاقية مالابو أول اتفاقية يصدرها الإتحاد الإفريقي لمكافحة هذه الجرائم، أما على المستوى الوطن العربي فقد تم اعتماد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، كل هذا سيتم التطرق إليه في **(المطلب الثاني)**.

المطلب الأول: اتفاقية بودابست آلية قانونية دولية لمكافحة الجرائم السيبرانية.

تعتبر اتفاقية بودابست أول اتفاقية دولية تهدف إلى التصدي للجرائم السيبرانية، حيث وضعت اطارا قانونيا مشتركا لمواجهة التحديات المتزايدة الناجمة عن الجرائم الإلكترونية، وذلك من خلال وضع قواعد موحدة وتعزيز التعاون الدولي، وعليه فمن الأهمية استعراض ظروف نشأة اتفاقية بودابست وأبرز الأحكام التي جاءت بها اتفاقية بودابست لمكافحة الجرائم السيبرانية **(الفرع الأول)**، ثم يليه دراسة الإطار القانوني لمكافحة الجرائم السيبرانية الذي جاءت به اتفاقية بودابست **(الفرع الثاني)**.

الفرع الأول: الأحكام العامة لاتفاقية بودابست بين ظروف النشأة والمضمون

ترتبط الأحكام العامة لاتفاقية بودابست بين ظروف النشأة باعتبارها أول وثيقة دولية متخصصة متعلقة بالجرائم الإلكترونية **(أولا)**، وكذا المضمون هذه لاتفاقية في جانبها الخاص بالتدابير القانونية التي جاءت بها **(ثانيا)**.

أولا: ظروف نشأة اتفاقية بودابست

تعد اتفاقية بودابست الخاصة بمكافحة الجرائم الإلكترونية استجابة جماعية من الدول الأوروبية وبعض الدول غير الأعضاء لمواجهة التحديات الناجمة عن الجرائم الإلكترونية،

حيث تعتبر هذه الاتفاقية أول معاهدة ملزمة دوليا خاصة بمكافحة هذا النوع من الجرائم، وقد كانت حصاد من الجهود التي بذلتها لجنة الخبراء[1].

بدأ مجلس أوروبا العمل على هذه القضية منذ أواخر الثمانينات، حيث قدم المجلس عام 1989 مبادئ توجيهية للهيئات التشريعية الوطنية، تزامنا مع تقرير اللجنة الأوروبية للجريمة الذي اعتمد ضرورة سن تشريعات جنائية متخصصة في الجرائم

السيبرانية، واستنادا إلى هذه التوصيات بدأ تطوير اتفاقية تتعلق بجرائم الإنترنت بإشراف من لجنة الخبراء حول الجريمة في الفضاء السيبراني[2].

بعدما أنشأت اللجنة الأوروبية المعنية بمشكلات الإجرام لجنة خبراء للتعامل مع الجريمة السيبرانية، عملت اللجنة على مشروع الاتفاقية بين العامين 1997 و2000 إلى أن تم اعتمادها في الدورة 109 المنعقدة من طرف اللجنة الوزارية لمجلس أوروبا وذلك بتاريخ 8 نوفمبر 2001، وكانت الاتفاقية تحت مسمى الاتفاقية الأوروبية للجريمة الإلكترونية[3].

تعد الاتفاقية الأوروبية للجريمة الإلكترونية الأولى من نوعها التي تهدف إلى تحقيق التنسيق بين القوانين الوطنية للدول لمكافحة الجريمة الإلكترونية، حيث تم التوقيع عليها في مؤتمر دولي عقد في العاصمة المجرية بودابيست في 23 نوفمبر 2001، وقد تم التوقيع

---

[1] أنظر: **الاتفاقية المتعلقة بالجريمة الالكترونية**، المعتمدة بموجب القرار رقم 185، الصادر عن مجلس أوروبا، بودابست، المؤرخ في 23 نوفمبر 2001، متوفر على الموقع: https://rm.coe.int/budapest-convention-in-arabic/1680739173 ، تم الاطلاع عليه بتاريخ 2025/04/16، على الساعة 22:00.

[2] **بوقرين عبد الحليم، قطاف سليمان**، "الأليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، مجلة الأكاديمية للبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، م 06، ع01، 2022، ص337.

[3] **هالة أحمد الرشيدي**، الإرهاب السيبراني –ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية–، دار النهضة العربية للنشر والتوزيع، القاهرة، 2021، ص 183.

عليها من طرف 30 دولة منها 26 دولة من الدول الأعضاء في مجلس أوروبا وأربعة دول واقعة خارج مجلس أوروبا، وذلك عملا بالمادة 37 من الاتفاقية التي تسمح بانضمام دول غير الأعضاء في المجلس أوروبا إليها، وهي الولايات المتحدة الأمريكية، كندا، اليابان، جنوب إفريقيا[1].

ثانيا: مضمون اتفاقية بودابست

تعتبر اتفاقية بودابست المعروفة بالاتفاقية الدولية لمكافحة الجرائم السيبرانية من أهم الاتفاقيات، حيث جاءت بديباجة و48 مادة تتضمن أهم التدابير الإجرائية والموضوعية والتعاون الدولي لمواجهة هذا النط من الجرائم، أما الديباجة فتتضمن تشجيع الدول وترغيبها للمشاركة في إعداد الاتفاقية من أجل التعاون الدولي بشأن مكافحة الجريمة السيبرانية، من خلال تفعيل سياسة جنائية مشتركة لحماية الدول من خطر هذه الجريمة بسبب انتشار التكنولوجيا[2].

أما محتوى الاتفاقية فيرتكز على ثلاث عناصر أساسية من خلال تشديدها على ضرورة اتخاذ تدابير تشريعية موضوعية وإجرائية لمكافحة الجرائم الإلكترونية، مؤكدة على أهمية التعاون بين الدول الأعضاء، لاسيما تصنيفها للمؤسسات التي تعمل على مكافحة الجرائم الإلكترونية،[3]

ففيما يتعلق بالعنصر الأول الخاص بالتدابير التشريعية الموضوعية فيشمل إدراج نصوص قانونية تحدد أنواع الجرائم الإلكترونية، أما العنصر الثاني فيكمن في التدابير

---

[1] **هالة أحمد الرشيدي**، المرجع السابق، ص 183.

[2] **نفس المرجع**، ص 184.

[3] **بوقرين عبد الحليم، قطاف سليمان**، "الأليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المرجع السابق، ص 339.

الإجرائية التي تتعلق بضرورة تحديث التشريعات الوطنية لتتماشى مع طبيعة الجرائم الإلكترونية، وأخيرا يتعلق العنصر الثالث في التعاون الدولي والإقليمي الذي يرتكز على أهمية تبادل المعلومات والتنسيق بين الدول في مكافحة الجرائم السيبرانية، كما تتكون الاتفاقية الأوروبية بشأن الجريمة السيبرانية من ديباجة وأربعة فصول.

تتطرق الاتفاقية الدولية إلى تعريف المصطلحات الأساسية[1]، ثم استعرض التدابير الواجب اتخاذها على الصعيد الوطني الذي ينقسم بدوره إلى ثلاث أقسام وهي القانون الجنائي الموضوعية[2]، الثاني خاص بالقانون الإجرائي[3]، أما القسم الثالث فهو خاص بالولاية القضائية[4]، بعدها جاء كل ما يتعلق بالتعاون الدولي[5]، وأخيرا تضمنت الأحكام الختامية[6].

الفرع الثاني: الأحكام الخاصة لاتفاقية بودابيست: أنواع الجرائم السيبرانية والتدابير القانونية الخاصة بها

للتعرف على الإطار القانوني لمكافحة الجرائم السيبرانية وفقا للاتفاقية يجب معرفة أهم الجرائم التي تتضمنها الاتفاقية **(أولا)** ثم التدابير التي تضمنتها اتفاقية بودابست **(ثانيا)**.

أولا: أنواع الجرائم السيبرانية في اتفاقية بودابست

تنقسم الجرائم السيبرانية في اتفاقية بودابيست إلى أربع فئات رئيسية، تتضمن الفئة الأولى الجرائم التي تمس خصوصية الأفراد وسلامة البيانات مثل الدخول الغير المشروع

---

[1] أنظر: المادة 01 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[2] أنظر: المواد 2-13 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[3] أنظر: المواد 14-21 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[4] أنظر: المادة 22 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[5] أنظر: المواد 23-35 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[6] أنظر: المواد 36-48 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

للأنظمة، الاعتراض غير القانوني للبيانات وتشويهها أو التأثير على سلامة الأنظمة، أما الفئة الثانية فقد شملت جرائم التزوير والاحتيال المعلوماتي، بينما تتطرق الفئة الثالثة إلى الجرائم المتعلقة بالمحتوى غير المشروع مثل نشر وتوزيع مواد إباحية خاصة بالأطفال، في حين تناولت الفئة الرابعة الاعتداءات على حقوق الملكية الفكرية والحقوق المجاورة[1].

ولقد نصت اتفاقية بودابيست على الجرائم السيبرانية في المواد (من 2 إلى 10) وهي مفصلة كمايلي:

1. **جريمة الدخول الغير قانوني المتعمد:** يقصد به الدخول المتعمد إلى أي نظام يخص الكمبيوتر أو جزء منه دون حق أو إذن سواء كان بنية انتهاك وسائل الأمن أو الحصول على معطيات الكمبيوتر أو لأي نية غير مشروعة.[2]
2. **جريمة الاعتراض الغير قانوني المتعمد:** الاعتراض الغير قانوني المتعمد ودون حق يتم بواسطة وسائل التكنولوجية للبيانات المرسلة غير عامة من أو إلى نظام كمبيوتر، كذلك اعتراض الاشعاعات الكهرومغناطيسية المنبعثة من نظام كمبيوتر تحمل مثل هذه المعطيات[3].
3. **جريمة التدخل المتعمد في المعطيات لتدميرها:** تتم هذه الجريمة كلما حدث تغيير في المعطيات بتدميرها أو حذفها أو تشويهها أو إفسادها أو تبديلها أو تغييرها أو تعديلها أو تعطيلها أو كبتها أو اخمادها، وأن يكون مقصود[4].

---

[1] أنظر: الاتفاقية المتعلقة بالجريمة الإلكترونية.

[2] أنظر: المادة 02، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[3] أنظر: المادة03، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[4] أنظر: المادة 04، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

4. **جريمة التدخل المتعمد في الأنظمة:** هي ارتكاب نفس الأفعال الذكورة في المادة السابقة (المادة04)، ويضاف إليها البث أو الإرسال[1].
5. **جريمة إساءة استخدام الأجهزة:** تشمل هذه الجريمة طائفتين من الأفعال الأولى منصوص عليها في الفقرة الأولى من المادة السادسة وتشمل عملية الإنتاج أو البيع أو الشراء بغرض الاستخدام، أو الاستيراد أو التوزيع بهدف ارتكاب أي فعل غير مشروع من الأفعال المنصوص عليها سابقا، كما تشمل هذه الجريمة وفقا للفقرة الثانية من المادة السابقة حيازة وتملك أي عنصر مما ورد ذكره في الفقرة الأولى بنية ارتكاب أي فعل غير مشروع من الأفعال الواردة في المواد 02-05 من اتفاقية بودابست[2].
6. **جريمة التزوير المتعمد باستخدام الكمبيوتر:** تتمثل هذه الجريمة في القيام عمدا باستخدام الحاسوب لإدخال أو تعديل أو حذف بيانات رقمية بطريقة تظهر معلومات غير صحيحة على أنها صحيحة ومقبولة قانونا كأنها بيانات رسمية، ويمكن أن تكون مقروءة أو غير ذلك ويحق للدولة أن تشترط توفر النية أو القصد للاحتيال لقيام المسؤولية الجنائية.[3]
7. **جريمة الاحتيال المتعمد باستخدام الكمبيوتر:** تتحقق هذه الجريمة من خلال استخدام الحاسوب بشكل متعمد بهدف الاحتيال، وذلك دون وجه حق وبقصد إلحاق الضرر بممتلكات الغير ويشمل ذلك إدخال أو تعديل أو حذف بيانات رقمية

[1] أنظر: المادة 05، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[2] أنظر: المادة 06، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[3] أنظر: المادة 07، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

أو التدخل في أنظمة الحاسوب أو برامجه بهدف تحقيق مكاسب مادية غير مشروعة.[1]

8. **الجرائم المرتبطة بدعارة الأطفال:** يقصد بها تلك التي تتم عبر الوسائط الالكترونية، بحيث يجب على الدول الأطراف اتخاذ تدابير تشريعية تجرم كل أشكال إنتاج أو توزيع أو عرض أو نقل المواد الإباحية التي يكون ضحاياها أطفال خاصة تلك التي تتم بواسطة الحاسوب.[2]
9. **الجرائم المرتبطة بحق المؤلف:** جاءت المادة بفقرتين الأولى خاصة بحق المؤلف والثانية بالحقوق المجاورة، أوجبت على الدول الأعضاء اتخاذ تدابير تشريعية تجرم الاخلال أو الاعتداء على حق المؤلف أو الحقوق المجاورة وفقا لما تحدده القوانين الوطنية، على أن تكون هذه الأفعال ارتكبت عمدا وبغرض تجاري وباستخدام الكمبيوتر[3].

تجدر الإشارة أن اتفاقية بودابيست تلزم الدول الأعضاء باتخاذ تدابير تشريعية واضحة لتجريم ومكافحة الأفعال الإجرامية المرتبطة باستخدام تكنولوجيا المعلومات، وتشمل أنواع متعددة من الجرائم الإلكترونية أبرزها الجرائم الاقتصادية التكنولوجية وجرائم انتهاك الملكية الفكرية المتعلقة بالمحتوى الرقمي بالإضافة إلى جرائم المحتوى الغير مشروع، رغم أن الاتفاقية تطرقت إلى ثلاث مراحل تشريعية رئيسية في مجال مكافحة الجريمة السيبرانية إلا أنه يلاحظ

[1] أنظر: المادة 08، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[2] أنظر: المادة 09، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

[3] أنظر: المادة 10، من الاتفاقية المتعلقة بالجريمة الإلكترونية.

عدم تناول بعض الموضوعات مثل انتهاك الخصوصية والبيانات الشخصية، يعود السبب إلى وجود تشريعات أوروبية مستقلة تهدف لحماية البيانات الشخصية[1].

ثانيا: التدابير القانونية التي تضمنتها اتفاقية بودابيست

من جملة التدابير والعقوبات المقررة في الاتفاقية أنها تلزم الدول الأطراف باتخاذ إجراءات قانونية فعالة ضد مرتكبي هذه الجرائم خاصة تلك التي تمثل تهديدا خطيرا، يجب أن تكون فعالة ومتناسبة ورادعة سواء للأشخاص الطبيعية أو الاعتبارية[2].

كما تنص الاتفاقية على القواعد العامة المتعلقة بمسؤولية الأفراد عن المساهمة في ارتكاب الجرائم الدولية، وألزمت الدول الأعضاء بوضع تشريعات تجرم الأفعال المرتبطة بالتحريض والمساعدة والتدخل في ارتكاب هذه الجرائم، كما يمكن أن يحاسب الشخص المعنوي جنائيا إذا تصرف لصالحه شخص طبيعي بناء على سلطة قانونية أو تمثيل رسمي أو بسبب غياب الرقابة عليه من طرف أشخاص طبيعيين[3].

المطلب الثاني: مكافحة الجرائم السيبرانية على المستوى الإقليمي

أصبحت الجرائم السيبرانية تشكل تهديدا متزايد للأمن والسلم على المستوى الاقليمي والوطني، حيث يتم استغلال الفضاء الرقمي لارتكاب أفعال خطيرة تمس الخصوصية والسيادة والاستقرار الاقتصادي والسياسي للدول، وفي هذا السياق برزت جهود إقليمية في مجال

---

[1] **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والأنترنت (الجرائم الالكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، لبنان، 2007، ص136.

[2] **بوقرينة عبد الحليم، قطاف سليمان**، "الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المرجع السابق، ص343.

[3] **عبد الله عبد الكريم عبد الله**، المرجع السابق، ص136.

مكافحة الجرائم السيبرانية من خلال اعتماد جامعة الدول العربية اتفاقية عربية لمكافحة جرائم تقنية المعلومات **(الفرع الأول)**، كما تم اعتماد اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية البيانات الشخصية **(الفرع الثاني)**.

الفرع الأول: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

للتعرف أكثر على هذه الاتفاقية يجب التطرق إلى ظروف نشأة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات **(أولا)**، ثم إلى أهم الجرائم المنصوص عليها في الاتفاقية **(ثانيا)**.

أولا: ظروف نشأة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تسعى الدول العربية إلى تكثيف جهودها للحد من الجرائم الإلكترونية لأنها تسبب مخاطر جسيمة بالأفراد والمؤسسات من خلال الخسائر المادية أو المعنوية، هذا ما دفع جامعة الدول العربية عبر أمانتها العامة ومجلس وزراء الداخلية العرب إلى العمل على مكافحة هذا النوع من الجرائم وذلك بإبرام على اتفاقيات وإصدار تشريعات قانونية تهدف إلى الحد من هذه الجرائم والوقاية منها[1].

ولأجل تحقيق هذا المسعى في إطار الجهود المبذولة من طرف الدول العربية لمكافحة الجرائم الإلكترونية، اجتمع مجلسي وزراء الداخلية والعدل العرب في مقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21 ديسمبر 2010 وأقر الاتفاقية العربية لمكافحة جرائم

[1] **عماد حسين محمد الفريحات**،" الجهود العربية والإفريقية لمواجهة الجرائم الإلكترونية في الفترة 2010-2023"، مجلة ابن خلدون للدراسات والأبحاث، م03، ع05، 2023، ص 194. متوفر على الموقع: https://www.benkjournal.com/article/view/323/298 تم الاطلاع عليه بتاريخ: 2025/04/11 على الساعة 23:04.

تقنية المعلومات، وقد دخلت حيز النفاذ بتاريخ 07 فيفري 2014 بعد استكمال النصاب القانوني المتعلق بإيداع وثائق التصديق من سبع دول[1].

ثانيا: مضمون الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تتكون الاتفاقية من 43 مادة منقسمة إلى الديباجة وخمسة فصول وقد تضمن في بدايته جملة من الأحكام العامة حيث نجد فيه أهداف الاتفاقية والتعريف ببعض المصطلحات المستخدمة وكذا مجالات تطبيق الاتفاقية[2].

تستعرض الاتفاقية أهم الأفعال المجرمة التي تلزم الدول الأطراف على تجريمها ونذكر منها جرائم الدخول غير مشروع، جرائم الاعتراض الغير مشروع، جرائم الاعتداء على سلامة البيانات، جرائم إساءة استخدام وسائل تقنية المعلومات، جرائم التزوير والاحتيال، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، كما جرمت الاتفاقية الشروع والاشتراك العمدي في ارتكاب أي من الجرائم المذكورة سابقا[3].

أما ما يتعلق بالأحكام الإجرائية التي لها صلة بتطبيق الاتفاقية وتحديد ما يجب على الدول الأطراف اتخاذه تشريعيا وجنائيا وتقنيا وأمنيا لضمان مكافحة فعالة لهذه الجرائم، وقد خصص الفصل الرابع بتبيان مجالات التعاون القانوني والقضائي بين الدول الأطراف من

---

[1] **هالة أحمد الرشيدي**، المرجع السابق، ص188.

[2] أنظر: **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21 ،صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 2014/09/08، ج.ر.ج.ج عدد 57، المؤرخ في 2014/09/28 متوفر على الموقع: https://esttf.motrans.gov.iq/wp-content/uploads/2016/04/الاتفاقية-العربية-لمكافحة-جرائم-تقنية-المعلومات. تم الاطلاع عليه بتاريخ 2025/04/12 على الساعة 23:05.

[3] أنظر: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

حيث مد الاختصاص الاقليمي وكذا التعاون في مجال تسليم المجرمين والمساعدة المتبادلة، وأخيرا تم التطرق إلى الأحكام الختامية في الفصل الخامس[1].

الفرع الثاني: اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو)

تعد اتفاقية مالابو من أهم المواثيق الإقليمية التي وضعها الإتحاد الإفريقي قصد مكافحة الجريمة السيبرانية، وللوقوف عند أهم بنود هذه الاتفاقية يقتضي الأمر الحديث عن تداعيات ابرام الاتفاقية **(أولا)**، ثم عن مضمون الاتفاقية **(ثانيا)**.

أولا: تداعيات إبرام اتفاقية مالابو لسنة 2014

تعرف القارة الإفريقية انتشارا واسعا للجريمة السيبرانية كغيرها من القارات في العالم، لهذا كان ولابد على الدول أن تصدر قوانين وتشريعات لمكافحة هذا النوع من الجرائم، فبعد اتفاقية بودابيست التي صدرت في أوروبا، عمل الإتحاد الإفريقي بدوره على إصدار تشريع اقليمي خاص بالدول الأعضاء في الإتحاد الإفريقي.

بعد عدة محاولات من الإتحاد الإفريقي لتبني آلية قانونية في مجالات الإلكترونية ومع تزايد الاهتمام بالمجال السيبراني، صدرت عدة قرارات في هذا المجال منها القرار بشأن تكنولوجيا المعلومات والاتصال في إفريقيا "التحديات والأفاق"2010، وإعلان أديس أبابا بشأن تنسيق قوانين الأنترنت في إفريقيا 2012[2].

---

[1] **هالة أحمد الرشيدي**، المرجع السابق، ص190.

[2] **لوكل مريم**،" قراءة في اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات طابع الشخصي لسنة 2014"، مجلة الدراسات القانونية والاقتصادية، المجلد03، العدد 03، 2021، ص 659.

غير أن أول مشروع للاتفاقية كان سنة 2013، وباسم اتفاقية الإتحاد الإفريقي حول الثقة والأمن في الفضاء الرقمي، والذي جاء لثمرة التعاون بين مفوضية الاتحاد الإتحاد الإفريقي ولجنة الأمم المتحدة للاقتصاد الإفريقي، خلال الدورة العادية رقم23 لمؤتمر الاتحاد الإفريقي في مالابو بغينيا الاستوائية تم اعتماد الاتفاقية من قبل رؤساء الدول والحكومات يومي26 و27 جوان 2014، وبهذا أصبحت الاتفاقية مفتوحة للمصادقة من قبل الدول وبعدها تم تعديل تسميتها لتصبح اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي[1].

لم تدخل الاتفاقية حيز التنفيذ إلى غاية 8 جوان 2023، حيث بلغت النصاب لدخولها حيز النفاذ وصادقت عليها سوى 15 دولة من أصل 55 دولة في الإتحاد الإفريقي، علما أن الجزائر لم تصادق على هذه الاتفاقية.

ثانيا: محتوى اتفاقية مالابو لسنة 2014

تتكون الإتفاقية من ديباجة تتضمن أهداف وأسباب التي تجعل من رؤساء الدول والحكومات للتصديق والاعتماد على نص الاتفاقية إلى جانب 38 مادة مركزة على أربعة محاور وهي:

تطرقت الإتفاقية إلى المعاملات الإلكترونية[2]، حيث ركزت على كل ما يتعلق بالمعاملات الإلكترونية من نطاق تطبيق التجارة الإلكترونية ثم المسؤولية التعاقدية لمقدم

---

[1] **لوكل مريم**، المرجع السابق، ص660.

[2] أنظر: المواد 2-7 من **اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصية**، متوفر على الموقع: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection، تم الاطلاع عليه بتاريخ 2025/04/16، على الساعة 10:01.

السلع والخدمات بالوسائل الإلكترونية وأن يتم الإعلان بالوسائل الإلكترونية، الاهتمام بالعقود الإلكترونية والكتابة بشكل إلكتروني أخيرا ضمان أمن المعاملات الإلكترونية[1].

تركز الاتفاقية أيضا على حماية البيانات الشخصية[2]، حيث تبين القواعد التي لا يمكن تجاوزها من طرف القائم على عملية المعالجة وهي مبدأ التراضي ومشروعية المعالجة الآلية للمعطيات ذات الطابع الشخصي، مبدأ الحياد ونزاهة المعالجات الآلية للمعطيات ذات الطابع الشخصي، مبدأ معالجة المعطيات، مبدأ دقة المعطيات وتحديد مدة حفظ المعطيات[3].

قصد تعزيز الأمن السيبراني ومكافحة الجريمة السيبرانية داخل الدول لم تغفل الإتفاقية من التنصيص على ضرورة تعاون الدول الأعضاء لوضع تشريعات وطنية خاصة بالأمن السيبرانية بالإضافة إلى توعية المجتمع بالتهديدات المرتبطة باستخدام أجهزة الكمبيوتر، وكذا تكوين الأفراد لضمان الاستخدام الآمن للفضاء الإلكتروني[4].

أما الأحكام الختامية فجاءت لتوضيح جملة من الأمور الخاصة بالانضمام والانسحاب، كما بينت أنه في حالة نشوء نزاع عن تطبيق الاتفاقية يتم تسويته وديا من خلال الوسائل السلمية لحل النزاعات الدولية، فيما يخص نفاذ الاتفاقية في القوانين الوطنية للدول يكون ذلك حسب قانون كل دولة[5].

---

[1] أنظر: اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

[2] أنظر: المواد 8-23 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

[3] **مريم لوكال**، المرجع السابق، ص ص 662-663.

[4] أنظر: اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

[5] **مريم لوكال**، المرجع السابق، ص 665.

المبحث الثاني: الآليات المؤسساتية في مكافحة الجرائم السيبرانية

نظرا للطبيعة التي تتميز بها الجرائم السيبرانية أي أنها عابرة للحدود وتعقيداتها التقنية والقانونية، أصبح التعاون الدولي أمرا لابد منه لتعزيز الجهود المبذولة في مكافحة هذه الجرائم والتصدي لها، وفي هذا السياق تنوعت مجالات التعاون الدولي في مكافحتها، لتشمل التعاون الأمني والتدريبي الذي يهدف إلى تبادل الخبرات والمعلومات ورفع من كفاءة المتخصصين في متابعة هذه الجرائم، كما برز التعاون في مجال المساعدة القضائية وتسليم المجرمين لضمان ملاحقة المجرمين **(المطلب الأول)**.

برزت الآليات المؤسساتية كأدوات فعالة لمكافحة الجرائم السيبرانية، سواء من خلال دور المنظمات الدولية في تبني اتفاقيات ومعايير قانونية وإجراءات تنسيقية أو من خلال تطوير مجالات التعاون الأمني والتقني بين الدول، كل هذا قصد مجابهة التطور التكنولوجي السلبي الذي أفرز تحديات أمنية خطرة كالجرائم السيبرانية، التي باتت تشكل تهديدا للأفراد والدول بسبب طبيعتها العابرة للحدود وصعوبة تتبع مرتكبيها مما يستدعي ضرورة تبني إستراتيجية مؤسسية لمواجهتها **(المطلب الثاني)**.

المطلب الأول: مجالات التعاون الدولي في مجال مكافحة الجرائم السيبرانية

تعتبر الجرائم السيبرانية من الظواهر الإجرامية العابرة للحدود التي تشكل تهديد على المستوى الوطني والدولي مما يستلزم تكاثف الجهود الدولية لمكافحتها، يبرز التعاون الدولي في عدة مجالات منها التعاون الأمني والتدريبي **(الفرع الأول)**، بالإضافة إلى التعاون القضائي الذي يشمل المساعدة القضائية وتسليم المجرمين **(الفرع الثاني)**.

الفرع الأول: التعاون الأمني والتدريبي

يعتبر التعاون الدولي من ركائز مكافحة الجرائم السيبرانية ومن بين المجالات التي يجب التعاون فيها نذكر التعاون الدولي في المجال الأمني **(أولا)**، والتعاون الدولي في المجال التدريبي **(ثانيا)**.

أولا: التعاون الدولي في المجال الأمني

يشكل التعاون الأمني لمكافحة الجرائم السيبرانية ركيزة أساسية في مواجهة التحديات الناتجة عن الجرائم الرقمية العابرة للحدود، ويتجسد هذا التعاون في تبادل الخبرات والمعلومات بين الدول هذا ما يعزز القدرات الأمنية ويسمح بمواجهة التهديدات السيبرانية بأكثر فعالية كما يشمل التنسيق المشترك في مجال التحقيق والرقابة، يساهم التكامل الأمني الدولي في بناء بيئة رقمية آمنة ومستقرة ويحد من تأثير الجرائم السيبرانية على الأمن الوطني والإقليمي والدولي[1].

نظرا لطبيعة الجرائم السيبرانية العابرة للحدود، أصبح من الضروري تفعيل التعاون الدولي لمكافحتها لأنه لم تعد جهود الدول المنفردة كافية للتصدي لها خاصة مع التطور

[1] **بركات رياض، محمد الصغير مسيكة**، "تسليم الجرمين كآلية لتفعيل التعاون الدولي لمكافحة الجرائم المعلوماتية"، مجلة الدراسات الحقوقية، م11، ع01، 2024، ص134.

التكنولوجي وظهور الشبكة المعلوماتية، لهذا لوجب تعزيز التنسيق بين أجهزة الشرطة في مختلف الدول من خلال إنشاء مكاتب متخصصة لتبادل المعلومات حول مرتكبي هذه الجرائم[1].

يتجسد التعاون الأمني في مختلف المنظمات الدولية المتخصصة التي تم إنشاءها والتي تم التطرق إليها سابقا على سبيل المثال في الفرع الثاني من المطلب الأول.

ثانيا: التعاون الدولي في مجال التدريب

يعاني رجال الضبط القضائي وأجهزة العدالة الجنائية من صعوبة في التعامل مع الجرائم السيبرانية، بسبب نقص الخبرة والمعرفة التقنية خاصة فيما يتعلق في آلية التعامل مع الأدلة الرقمية، حيث أن بعض رجال الشرطة قد يتسببون عن غير قصد في إتلاف الأدلة وعرقلة التحقيقات نتيجة جهلهم بطبيعة هذه الجرائم، لهذا يجب اكتساب مهارة فنية وتقنية مناسبة من خلال تطوير قدراتهم ومهاراتهم في مواجهة الجرائم السيبرانية[2].

يعتبر التدريب ضروري في ظل التطور التكنولوجي المتسارع خاصة في مجال مكافحة الجرائم السيبرانية، حيث لم يعد التدريب التقليدي كافيا بل يجب أن يكون متخصص في المجال الفني والتقني للتعامل مع هذا النوع من الجرائم، ويشمل فهم طبيعة التهديدات والاختراقات الإلكترونية والتعرف على أنواع الجرائم المعلوماتية بالإضافة إلى الجوانب

---

[1] **جمال محمد خلفان محمد النقبي**، سلطان محمد سالم عوض هيسان المصعبي، " التعاون الوطني والدولي في الجرائم الإلكترونية "المشكلات والحلول" "، مجلة المعهد العالي للدراسات النوعية، المجلد03، العدد16، 2023، ص5473. متوفر على الموقع: https://hiss.journals.ekb.eg/article_342134.html ، تم الاطلاع عليه بتاريخ: 2025/04/20، على الساعة 22:25.

[2] **محمد عادل علي عبد السلام**، الأحكام الإجرائية في جريمة السرقة السيبرانية–دراسة مقارنة–، دار النهضة العربية للنشر والتوزيع، القاهرة، 2023، ص215.

الإجرائية، ينبغي أن تتنوع أساليب التدريب بين الدراسة والتحليل والتفاعل الميداني[1]، كما يتم عقد ندوات و مؤتمرات متخصصة في سبل مكافحة الجرائم السيبرانية عن طريق مختصين في المجال لتبادل الخبرات والمكتسبات[2].

الفرع الثاني: التعاون في مجال المساعدة القضائية وتسليم المجرمين

تعتبر متابعة مرتكبي الجرائم السيبرانية من بين الصعوبات التي تواجه الدول لذلك وجب التعاون الدولي في مجال المساعدة القضائية **(أولا)**، وتسليم المجرمين **(ثانيا)**.

أولا: التعاون الدولي في مجال المساعدة القضائية

تعرف المساعدة القضائية الدولية بأنها: "**كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم**"[3]، كما تعد أحد الإجراءات التي تلجأ إليها الدولة الطالبة في إطار الدعوى الجنائية حيث تتقدم بطلب إلى دولة أخرى للقيام بإجراء قضائي يتعذر عليها تنفيذه ضمن إقليمها، وتكمن أهمية هذا التعاون في تعزيز فعالية التحقيقات الجنائية وتمكين الدول من ملاحقة المتهمين وتقديمهم للمحاكمة، بالإضافة إلى سعي الدول إلى إبرام اتفاقيات دولية تهدف لتسريع آليات التعاون القضائي من خلال السماح بالتواصل المباشر بين السلطات المختصة في كلا الدولتين[4].

---

[1] **بدري فيصل**، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون عام، كلية الحقوق، جامعة الجزائر1–بن يوسف بن خدة–، الجزائر، 2018، ص84.

[2] **محمد عادل علي عبد السلام**، المرجع سابق، ص221.

[3] **عميمر عبد القادر**، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراه علوم في القانون الدولي، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1–بن يوسف بن خدة–، الجزائر، 2020، ص357.

[4] **محمد عادل علي عبد السلام**، المرجع السابق، ص238.

تتخذ المساعدة القضائية في المجال الجنائي أشكال عدة نذكر منها:

التبادل المعلوماتي بين الدول يتمثل في تزويد الجهات القضائية أو الأمنية الأجنبية بالوثائق والمعلومات المطلوبة[1]، ونقل الإجراءات الجنائية الذي يقصد به تولي دولة ما بناء على اتفاقية باتخاذ إجراءات قانونية بخصوص جريمة حدثت في دولة أخرى ولمصلحة هذه الدولة بشرط توفر مجموع من الشروط منها التجريم المزدوج وشرعية الإجراءات[2].

ثانيا: التعاون الدولي في مجال تسليم المجرمين

تعتبر آلية تسليم المجرمين من أبرز وسائل التعاون الدولي في مواجهة الجرائم السيبرانية والحد من انتشارها، وقد تم تنظيمها بموجب عدد من الاتفاقيات الدولية والتشريعات الوطنية، وهو إجراء قانوني دولي يتمثل في نقل شخص متهم أو مدان بارتكاب جريمة من دولة يتواجد فيها إلى دولة أخرى تطالب به إما لمحاكمته أو لتنفيذ العقوبة الصادرة في حق، ويتم هذا الإجراء وفقا لاتفاقية بين الطرفين أو بمبدأ المعاملة بالمثل[3].

المطلب الثاني: دور المنظمات الدولية في مكافحة الجرائم السيبرانية

تلعب المنظمات الدولية دورا أساسيا في تنسيق الجهود الدولية وتوحيد المعايير القانونية لمكافحة هذا النوع من الجرائم، من أبرز هذه المنظمات نجد هيئة الأمم المتحدة ووكالاتها المتخصصة **(الفرع الأول)**، بالإضافة إلى المنظمات الدولية الأخرى على غرار منظمة الأمم المتحدة في مجال مكافحة الجرائم السيبرانية **(الفرع الثاني)**.

---

[1] **فريد ناشف**، "آليات التعاون الدولي في مكافحة الجرائم الإلكترونية"، مجلة البحوث في الحقوق والعلوم السياسية، م08، ع01، 2022، ص440.

[2] **محمد عادل علي عبد السلام**، المرجع السابق، ص240.

[3] **بركات رياض، محمد الصغير مسيكة**، المرجع السابق، ص137.

الفرع الأول: مكافحة الجرائم السيبرانية في إطار منظمة الأمم المتحدة

تساهم المنظمات الدولية في مكافحة الجرائم السيبرانية ومن بين أهم هذه المنظمات نستعرض دور الجمعية العامة في مكافحة هذه الجرائم **(أولا)**، ومن بين الوكالات المتخصصة التابعة لها نذكر جهود الإتحاد الدولي للاتصالات في مجال مكافحة الجرائم السيبرانية **(ثانيا)**.

أولا: دور الجمعية العامة في مكافحة الجرائم السيبرانية

تسعى الأمم المتحدة إلى تحقيق السلم والأمن الدوليين،[1]بما أنه أصبحت تستعمل الجرائم السيبرانية في التهديد بالسلم والأمن الدوليين وجب على الأمم المتحدة التصدي

لهذه الجرائم من خلال تعزيز التعاون بين الدول الأعضاء لمجابهة التهديدات الناتجة عن التطور التكنولوجي وتنظيم المؤتمرات مثل مؤتمر منع الجريمة ومعاملة المجرمين[2].

تؤدي الجمعية العامة للأمم المتحدة دور فعال في مكافحة الجرائم الدولية ومناقشة القضايا التي تهم المجتمع الدولي منها الجرائم السيبرانية ذلك بتقريب وجهات النظر بين الدول الأعضاء حول طريقة مكافحة استخدام الأنترنت لأغراض غير مشروعة، لهذا أصدرت العديد من التوصيات في مجال مكافحة الإرهاب السيبرانية تحث من خلالها الدول على الاستخدام المشروع لتكنولوجية المعلومات وتعزيز التعاون الدولي في هذا المجال.[3]

---

[1] المادة01 الفقرة 01 من **ميثاق منظمة الأمم المتحدة**، الموقع من طرف مندوبي حكومات الأمم المتحدة، بتاريخ 26جوان1945، دخل حيز التنفيذ في 24أكتوبر1945، انضمت الجزائر إلى هيئة الأمم المتحدة في 04أكتوبر1962 بموجب قرار الجمعية العامة للأمم المتحدة رقم 176 {د-17}، الصادر بتاريخ 04أكتوبر1962 في جلستها رقم 1020.

[2] **عمر يوسف عبد الله**، الإطار القانوني والمؤسساتي لمكافحة التقليد والقرصنة الإلكترونية، أطروحة للحصول على شهادة الدكتوراه في العلوم، القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة وهران 02، وهران، 2022، ص 268.

[3] **هالة أحمد الرشيدي**، المرجع السابق، ص ص152-153.

في هذا السياق من بين الجهود المبذولة على مستوى الأمم المتحدة إصدار عدة قرارات دولية خاصة بمكافحة هذا النوع من الجرائم منها:[1]

- قرار الأمم المتحدة الصادر في 2000/12/14، المتعلق بمكافحة إساءة استعمال تكنولوجية المعلومات لأغراض إجرامية.
- قرار الأمم المتحدة الصادر في 2001/12/19، الخاص بتعزيز التعاون الدولي في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

ثانيا: جهود الإتحاد الدولي للاتصالات في مجال مكافحة الجرائم السيبرانية

يعتبر الاتحاد الدولي للاتصالات من الأجهزة الفعالة في مجال مكافحة الجرائم السيبرانية على المستوى العالم، بحث كان له الفضل بعقد أول اجتماع حول موضوع المجتمع المعلوماتي في جنيف من 10 إلى 12 ديسمبر 2003، لما يشهده العالم من تطور في مجال الالكتروني لكن لم يسفر عن أي نتائج[2]، وكان يهدف إلى تعزيز التعاون بين الدول الأعضاء من خلال الاتفاق على قواعد ومعايير موحدة تتعلق بتكنولوجية المعلومات والبنية التحتية للاتصالات، كما يعمل على وضع خطط إستراتيجية لتعزيز الأمن السيبرانية الدولي أسفر عن سبعة أهداف رئيسية، نذكر منها:[3]

- وضع إستراتيجيات وطنية ودولية مناسبة لمواجهة التهديدات الإلكترونية، مع الأخذ بعين الاعتبار السياسات المختلفة للدول.

---

[1] **حسين طاهري**، الجرائم الإلكترونية، دار الخلدونية للنشر والتوزيع، الجزائر، 2022، ص548.

[2] **Romain Boos**, La Lutte Contre La Cybercriminalité au Regard de l'action des états, thèse de Doctorat en Droit privé et Sciences Criminelles, Faculté de Droit Sciences Économiques et Gestion, Université de Lorraine, Français, 2016, P 211.

[3] هالة أحمد الرشيدي، المرجع السابق، ص ص165-166.

- وضع معايير أمنية مشتركة لتسهيل التعاون بين الدول، بالإضافة إلى وضع أنظمة فعالة للمراقبة والإنذار المبكر بهدف التصدي للهجمات السيبرانية.
- تطوير آليات لتبادل المعلومات بين الدول والمنظمات بهدف تعزيز الأمن السيبراني، كما يضع توصيات لإنشاء هياكل تنظيمية تساعد الدول على مواجهة الجرائم الإلكترونية.

الفرع الثاني: أهم المنظمات الدولية المتخصصة في مجال مكافحة الجرائم السيبرانية

من بين أهم المنظمات الدولية المتخصصة في مجال مكافحة الجرائم السيبرانية نجد المنظمة الدولية للشرطة الجنائية "الإنتربول" **(أولا)**، والإتحاد الإفريقي للتعاون الشرطي "الأفريبول" **(ثانيا)**.

أولا: جهود المنظمة الدولية للشرطة الجنائية (الإنتربول)

تعتبر المنظمة الدولية للشرطة الجنائية منظمة دولية حكومية تضم 196 دولة عضو، أنشأت سنة 1923، كانت تختص في المساعدة أجهزة الشرطة في مختلف أنحاء العالم في مواجهة الجرائم التقليدية في ذلك الوقت، مع التطور التكنولوجي ظهرت جرائم جديدة مثل الجرائم السيبرانية فتطور العمل الشرطي تماشيا مع التطور التكنولوجي.[1]

تهدف الإنتربول إلى تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء من أجل مكافحة الجريمة، من خلال جمع وتبادل المعلومات المتعلقة بالمجرمين والجرائم عبر المراكز المنتشرة في الدول الأعضاء، كما يساهم في تنسيق الجهود بين الأجهزة الأمنية في الجرائم العابرة للحدود مثل الجرائم السيبرانية وذلك بتوفير المعلومات الازمة.[2]

---

[1] **المنظمة الدولية للشرطة الجنائية**، متوفر على الموقع: https://www.interpol.int/ar/3/12 تم الاطلاع عليه بتاريخ:2025/04/16، على الساعة: 12:03.

[2] **عمر يوسف عبدالله**، المرجع السابق، ص273.

تهدف المنظمة الدولية للشرطة الجنائية إلى تنمية التعاون بين أجهزة الشرطة الجنائية في مختلف الدول، وذلك في إطار احترام القوانين الوطنية ومبادئ الإعلان العالمي لحقوق الإنسان، كما تعمل على دعم وتطوير المؤسسات التي تساهم في الوقاية من الجرائم ومكافحتها، علما أن عمل المنظمة يقتصر على الجوانب الأمنية والجنائية فقط أي أنها لا تتدخل في القضايا ذات الطابع السياسي أو العسكري أو الديني أو العنصري حسب ما ينص نظامها الأساسي[1].

ثانيا: فعالية آلية الإتحاد الإفريقي للتعاون الشرطي(الأفريبول)

ظهرت فكرة تأسيس منظمة الشرطة الجنائية الإفريقية **(أفريبول)** خلال أشغال المؤتمر الإقليمي الإفريقي الثامن والعشرون، الذي انعقد بمدينة وهران–الجزائر– في الفترة الممتدة من 10 إلى 12 سبتمبر 2013، بمشاركة قادة أجهزة الشرطة من 41 دولة إفريقية الذين أجمعوا على أهمية التعاون الأمني في مواجهة التحديات المشتركة[2].

تعد آلية الاتحاد الإفريقي للتعاون الشرطي المعروفة ب "الأفريبول" هيئة تقنية تابعة للاتحاد الإفريقي، أنشئت بهدف تعزيز فعالية وكفاءة أجهزة الشرطة في الدول الإفريقية ذلك بدعم التعاون بينها من خلال تبادل المعلومات الأمنية وتعزيز التنسيق العملياتي بينها، يقع مقرها في الجزائر العاصمة[3].

يعتبر تأسيس هذه الآلية هو نتيجة لتزايد التهديدات الأمنية العابرة للحدود على القارة الإفريقية ومن بينها الجرائم السيبرانية، ولمواجهة هذه التحديات نصت الاتفاقية على ضرورة تطوير إستراتيجية إفريقية موحدة تهدف إلى مكافحة الجريمة المنظمة والجرائم السيبرانية لتعزيز

---

[1] **بدري فيصل**، المرجع السابق، ص 66.

[2] **طاهري حسين**، جرائم القرصنة الإلكترونية، دار الخلدونية للنشر والتوزيع، الجزائر، 2023، ص248.

[3] **لزعر عبد العزيز، زياني رشيد**، "آليات الإتحاد الإفريقي للتعاون الشرطي(الأفريبول) ودورها في مكافحة الجريمة الإلكترونية"، مجلة متون، جامعة مولاي الطاهر سعيدة، م14، ع03، 2021، ص 254.

الأمن والسلم في القارة الإفريقية، كما تسعى إلى تعزيز التعاون بين أجهزة الشرطة وتطوير قدراتها من خلال التدريب وتبادل خبراتها وتدعم التنسيق بين الجهات الشرطية[1].

لتعزيز الجهود الدولية لمكافحة الجرائم السيبرانية برز التعاون بين منظمة الأفريبول والإنتربول لتنسيق الجهود وتبادل المعلومات والأدلة الرقمية بين الجهازين وذلك استجابة للتحديات المتزايدة في الفضاء السيبراني على المستويين الإقليمي والدولي[2].

[1] **ودرار أمين**، "الشرطة الجنائية الإفريقية "الأفريبول" "، حوليات جامعة الجزائر1، جامعة بن يوسف بن خدة، م34، ع01، 2020، ص139.

[2] **لزعر عبد العزيز، زياني رشيد**، المرجع السابق، ص259.

الفصل الثاني

فعالية آليات مكافحة الجرائم السيبرانية

يعتبر التعاون الدولي في مجال مكافحة الجرائم السيبرانية ركيزة أساسية في التصدي لهذه الجرائم المستحدثة، وذلك من خلال تفعيل جملة من الآليات القانونية والمؤسساتية التي تهدف إلى الحد من انتشار هذه الجرائم والوقاية منها، وقد تجسد دور هذه الآليات من خلال ما حققته من إنجازات على المستويين الوطني والدولي خاصة عبر النماذج العملية والتجارب الواقعية التي أظهرت قدرة المجتمع الدولي على التصدي لهذا النوع من الجرائم، لكن رغم النتائج الإيجابية المحققة غير أنها واجهت مجموعة من الإخفاقات والتحديات المتمثلة في تهديد سيادة الدول والمساس بحقوق الإنسان الأساسية **(المبحث الأول)**.

يشهد التعاون الدولي في مجال مكافحة الجرائم السيبرانية مجموعة من التحديات والإشكالات التي تحد من فعاليته وتعرقل الجهود الساعية إلى التصدي لهذه الجرائم، وتتنوع هذه الإشكالات بين الصعوبات القانونية المتمثلة في اختلاف التشريعات الوطنية وعدم ملاءمتها مع طبيعة هذه الجرائم العابرة للحدود، وصعوبات تتعلق بمحدودية آليات التعاون الدولي وذلك بغياب إطار قانوني موحد يضمن التنسيق بين الدول، لهذا يجب البحث عن السبل والآليات التي تسهر على تجاوز هذه الصعوبات على المستويين الوطني والدولي من خلال تطوير القوانين الخاصة بمكافحة هذا النوع من الجرائم وتعزيز التنسيق والتعاون الدولي بما يتناسب مع خصوصية و تعقيدات الجرائم السيبرانية **(المبحث الثاني)**.

المبحث الأول: تقييم دور آليات مكافحة الجرائم السيبرانية

يساهم التعاون الدولي في مجال مكافحة الجرائم السيبرانية من خلال الآليات القانونية والمؤسساتية التي تسعى بدورها للحد والتصدي لهذه الجرائم، ويظهر دورها من خلال تقييمها في الواقع عن الإنجازات التي تم تحقيقها على المستوى الوطني أو الدولي والتي تبرز خصوصا في النماذج العملية التي تم من خلالها على التصدي للجرائم السيبرانية **(المطلب الأول)**.

على الرغم من الفعالية التي حققتها الآليات القانونية والمؤسساتية في مكافحة الجرائم السيبرانية على المستويين الوطني والدولي في الحد من انتشار الجرائم السيبرانية والوقاية منها إلا أنها لم تسلم من الإخفاقات التي كانت سبب في استمرار هذا النوع من الجرائم، وقد مست هذه الإخفاقات عدة مجالات كزيادة اختراقها لسيادة الدول التي تعتبر أهم عنصر لقيام الدولة وكذا انتهاكها لأهم حقوق الإنسان الأساسية **(المطلب الثاني)**.

المطلب الأول: إنجازات الآليات الدولية في مجال مكافحة الجرائم السيبرانية

تطبيقا للآليات مكافحة الجرائم السيبرانية تنوعت التجارب الوطنية والدولية في التصدي لهذه الجرائم، حيث سنستعرض بعض من نماذج مكافحة الجرائم السيبرانية منها على المستوى الوطني **(الفرع الأول)**، وبعض من نماذج التعاون الدولي في مكافحة الجرائم السيبرانية **(الفرع الثاني)**.

الفرع الأول: الإنجازات المحققة في المجالين التشريعي والتكويني

تعددت الإنجازات المحققة في مكافحة الجرائم السيبرانية لاسيما في الجانب التشريعي، ونأخذ على سبيل المثال لا الحصر التشريع الجزائري في هذا المجال **(أولا)**، إضافة إلى التكوين والتدريب الذي تباشره المنظمات الدولية خاصة خلال النزاعات المسلحة لقمع الجرائم السيبرانية ومن أمثلته الدور الذي لعبته هذه الأخيرة خلال النزاع بين روسيا وأوكرانيا **(ثانيا)**.

أولا: وضع تشريعات داخلية خاصة بمكافحة الجرائم السيبرانية: الجزائر نموذجا

تعتبر الجزائر من بين الدول الأكثر تعرضا للهجمات السيبرانية حيث سجلت في السنوات الأخيرة حوالي 95 ألف هجمة إلكترونية[1]، وقد شهدت أول جريمة سيبرانية سنة 2003 بعدما تعرض البنك التجاري للاستثمار لعملية احتيال إلكتروني، بدأت العملية بقيام أحد الزبائن بفتح حساب في البنك وإيداع مبلغ مالي وبعد أيام قليلة تقدم لسحب مبلغ ضخم يفوق رصيده، هذا ما جعل الموظفة تشك وأخبرت إدارة البنك، التحقيقات الأولية

[1] **كاوجة محمد الصغير**، "الهجمات السيبرانية بين الواقع وسبل المواجهة"، مجلة الرسالة للدراسات الإعلامية، جامعة العربي التبسي، م06، ع03، 2022، ص115.

وجهت أصابع الاتهام نحو مهندس صيانة الحواسيب غير أن تدخل خبير في الإعلام الآلي تابع للشرطة العلمية كشف وجود اختراق جزئي للنظام المعلوماتي للبنك وتم التلاعب بالحسابات البنكية[1].

بعد هذه الحادثة سارع المشرع الجزائري إلى تعديل الإطار التشريعي لمواجهة الجرائم المعلوماتية، حيث تم تجريم الأفعال الماسة بالنظم المعلوماتية في قانون العقوبات سنة 2004 وبعدها أصدر قانون خاص حول الوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها سنة 2009.

ثانيا: نجاعة البرامج التكوينية في الحد من الجرائم السيبرانية: الحرب الروسية الأوكرانية نموذجا

شهدت الحرب الروسية على أوكرانيا هجمات سيبرانية بين الطرفين في البداية ثم تحولت إلى مواجهة بين روسيا والدول الأوروبية بشكل عام، وقد انطلقت بتاريخ2 مارس 2022 حينما شنت أوكرانيا هجمات إلكترونية استهدفت شبكات الطاقة الروسية وخطوط السكة الحديدية، في المقابل قامت روسيا بتاريخ 16 أوت 2022 بشن هجوم إلكتروني ضد أوكرانيا حيث استهدفت شركة الطاقة النووية الأوكرانية "إينرغوأتوم"[2].

أصبحت الهجمات السيبرانية تشكل تهديدات حقيقية على العلاقات الدولية، لأنها بمثابة سلاح يستعمل في الحروب الحديثة ولها قدرته بإحداث أضرار كبيرة بالأنظمة الأمنية والمعلوماتية للدول، حيث يمكن أن يصل تأثير الهجوم السيبراني إلى القضاء على الدول لهذا

---

[1] **زكري محمد**، نشأة الجريمة المعلوماتية من بداية الستينات إلى القرن ال21 "التحقيقات الجنائية في مجال مكافحة الجريمة المعلوماتية"، مجلة الشرطة العلمية والتقنية، ع04، ص08.

[2] **سامر نمر سالم الجاروشة**، الجرائم السيبرانية وحقوق الإنسان في القوانين الدولية والوطنية، دار النهضة العربية للنشر والتوزيع، القاهرة، 2023، ص20.

وجب التعاون الدولي في مجال مكافحة الجرائم السيبرانية، وقد تدخلت منظمة الحلف الأطلسي والإتحاد الأوروبي لمساعدة أوكرانية للتصدي للهجمات السيبرانية وذلك بتقديم التدريب الازم للمختصين في مجال مكافحة الجرائم السيبرانية.

الفرع الثاني: أمثلة عن التعاون الدولي في مكافحة الجرائم السيبرانية

يعتبر التعاون الدولي من أهم سبل مكافحة الجرائم السيبرانية لما له من أهمية عملية، لهذا نستعرض النجاح النسبي للتعاون الدولي في مكافحة الجرائم السيبرانية **(أولا)**، بالإضافة إلى التنسيق بين الإنتربول الأفريبول في مواجهة هذه الجرائم **(ثانيا)**.

أولا: فعالية التعاون الدولي في مكافحة الجرائم السيبرانية

تتجسد فعالية التعاون الدولي في مكافحة الجرائم الإلكترونية في عدة عمليات تمت بمساعدة بين أجهزة مختلفة من عدة دول، ونذكر منها عملية "falcon" التي نفذت في شهر أفريل من سنة 2005 بالتعاون بين مكتب التحقيقات الفيدرالي الأمريكي (FBI) والإنتربول والشرطة الفرنسية، حيث تمكنت من تفكيك منظمة إجرامية تعمل في عدة دول أوروبية، إضافة إلى عملية "محطم الجليد" التي تمت من طرف الشرطة الأوروبية "يوروبول" بتاريخ 14 جوان2005 حيث قامت بمداهمات وتفتيشات في 13دولة أوروبية، وتم توقيف عدة مشتبه فيهم[1].

ثانيا: التنسيق بين الإنتربول الأفريبول في مواجهة الجرائم السيبرانية

قامت منظمة الإنتربول بالتنسيق مع منظمة الأفريبول بإطلاق عملية واسعة النطاق تحت اسم(**Africa Cyber Surge 2**) استهدفت 25دولة إفريقية وذلك في إطار الجهود الدولية في مكافحة الجريمة السيبرانية، حيث جاءت هذه العملية بهدف الكشف وتعطيل

[1] **شنتير خضرة**، المرجع السابق، ص238.

الشبكات الإجرامية الإلكترونية في إفريقيا، تعزيز التعاون بين أجهزة القانون في الدول الإفريقية وغيرها، وقد حققت هذه العملية التي استمرت لمدة أربعة أشهر وذلك منذ أفريل2023 إلى الكشف عن 67420 شبكة سيبرية مشبوهة وعن 14134 ضحية تعرضت بياناتها للسرقة، هذا ما أدى إلى اعتقال 14 شخص متورط وغلق 615 موقع إلكتروني ضار في كينيا و185 في غامبيا وموقعين في الكاميرون[1].

تعتمد العملية على دعم تقني من شركات عالمية مختصة في الأمن السيبرانية، هذا ما أثبت أن الشراكة بين أجهزة القانون والقطاع الخاص ضروري لمكافحة الجرائم السيبرانية، كما يجب تطوير الآليات الأمنية للتصدي لهذه الجرائم.

المطلب الثاني: مظاهر إخفاق الآليات الدولية في مكافحة الجرائم السيبرانية

رغم الجهود الدولية المبذولة في مكافحة الجرائم السيبرانية سواء على المستوى الوطني أو الإقليمي أو الدولي، خاصة التعاون الدولي في مجال التصدي لهذه الجرائم والنتائج المحققة في هذا المجال، إلا أن الآليات الدولية لمكافحة الجرائم السيبرانية لا تزال تعاني من إخفاقات عديدة وذلك يعود لعدة أسباب، ويظهر هذا الإخفاق في عدة مجالات نذكر منها العجز عن وقف اختراق الجرائم السيبرانية لسيادة الدول **(الفرع الأول)**، وكذا عدم السيطرة على الجرائم السيبرانية في انتهاكها لحقوق الإنسان **(الفرع الثاني)**.

[1] **المنظمة الدولية للشرطة الجنائية**، متوفر على الموقع:https://www.interpol.int/ar/1/1/2023/14-Africa، تم الاطلاع عليه بتاريخ: 2025/05/14، على الساعة 12:14.

الفرع الأول: العجز عن وقف اختراق الجرائم السيبرانية لسيادة الدول

تعتبر السيادة أساس قيام الدولة حيث لا يمكن أن تقوم دولة دون أن تتمتع بالسيادة ولا يمكن تصور سيادة بدون دولة[1]، لطالما شكلت السيادة أصل قيام الدولة ومصدر قوتها، حيث سعت الدول إلى حماية سيادتها الداخلية من خلال احتكار ممارسة السلطة على مواطنيها دون تدخل أي جهة في أخرى في ممارسة هذا الحق، كما تحرص على الحفاظ على سيادتها الخارجية من خلال ترسيخ حدودها لإقليمية واعتبارها غير قابلة للتنازع، غير أن التغيرات الدولية شهدت ظهور تهديدات جديدة التي بدورها فرضت تحديات جديدة على سيادة الدول[2]، لأجل ذلك يفترض أن يمارس الفضاء السيبرانية داخل حدود الدولة فحسب[3].

تعد الجرائم السيبرانية في العصر الحديث من أبرز التحديات التي تواجه سيادة الدول، حيث أصبحت تشكل تهديد حقيقي للسيادة الوطنية خاصة عند استهداف الأنظمة الحكومية أو البنى التحتية الحيوية أو التدخل في الشؤون الداخلية للدول، ويزداد هذا التحدي مقارنة بالمبادئ الأساسية للقانون الدولي خاصة مبدأ عدم التدخل وعدم استخدام القوة، لأنهما يعتبران أساس العلاقات الدولية[4].

---

[1] **بن قطاط خديجة**، "تداعيات الحروب السيبرانية على السيادة الرقمية"، مجلة القانون العام الجزائري والمقارن، م10، ع02، 2024، ص 287.

[2] **شرقي عبد الغاني**، "التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة لسيادة واستقالية"، مجلة السياسة العالمية، م07، ع02، 2023، ص278.

[3] **Maupeou S**, Cybercriminalité, cyberconflits, Revue Défense nationale et sécurité collective, 2009, p127.

[4] **محمد محمود زيتون**، "العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني"، مجلة وميض الفكر، ع25، 2025، ص195، متوفر على الموقع: https://wameedalfikr.com/?p=2522 ، تم الاطلاع عيه بتاريخ:2025/05/19 على الساعة: 21:55.

تعد الهجمات السيبرانية التي تستهدف المنشآت الحيوية للدول انتهاكا صريحا لسيادتها، ومن أمثلة ذلك الهجوم بفيروس شمعون الذي تعرضت له شركة النفط السعودية عام 2012، بحيث تسبب في تعطيل آلاف الأقراص الصلبة وأدى إلى فقدان وظائف المعدات والأنظمة المعتمدة في البنية التحتية المستهدف، كما يتم استخدام الهجمات السيبرانية للتأثير على العمليات الانتخابية حيث تعرضت الانتخابات البريطانية لسنة2016، لهجمات إلكترونية، كما عرفت الانتخابات الأمريكية لسنة2021، عدة هجمات سيبرانية التي وصفها وزير الخارجية الأمريكي بأنها اجتياح رقمي يمس سيادة الولايات الأمريكية[1].

تعرضت إستونيا سنة2007 لهجمات سيبرانية تعتبر الأكبر استهدفت البنية التحتية الإلكترونية للدولة من مؤسسات حكومية، مصارف، شركات الاتصال، وقد استمرت لعدة أسابيع وسببت بشلل على مستوى الدولة، ويعتبر مثال عن استهداف سيادة الدولة لأنه تسبب بعزل إستونيا عن العالم الخارجي رقميا[2].

الفرع الثاني: عدم السيطرة على الجرائم السيبرانية في انتهاكها لحقوق الإنسان

ساهمت الجرائم السيبرانية في عدة انتهاكات تمس حقوق الإنسان، ومن بين هذه الحقوق التي تنتهك عن طريق هذه الجرائم نذكر على سبيل المثال الحق في الخصوصية **(أولا)**، وتضييق في الحق في حرية التعبير **(ثانيا)**.

---

[1] محمد محمود زيتون، **المرجع السابق**، ص ص196-197.

[2] **محمد عباس محسن**، الهجمات السيبرانية ومنطقة الفراغ التشريعي دراسة في ميثاق الأمم المتحدة والقانون الدولي، منشورات ألفا للوثائق، قسنطينة، 2021، ص88.

أولا: عدم القدرة على ضبط الجرائم السيبرانية الماسة بالحق في الخصوصية

تعد عمليات اختراق حسابات الأفراد وبياناتهم الشخصية من بين الجرائم السيبرانية التي تنتهك حقوق الإنسان، حيث يتم الدخول إلى الحسابات الخاصة بالأفراد بطرق غير مشروعة، معتمدين على مهاراتهم التقنية في مجال الأنترنت وبهدف المساس بسرية المعلومات حيث يشهد هذا النوع انتشار واسع على المستوى الدولي[1].

وفي هذا السياق تتنوع أشكال الجريمة السيبرانية التي تحدث عبر الأنترنت والتي تمس بخصوصية الأفراد، نجد تلك التي تتم عبر منصات التواصل الاجتماعي حيث يتم الاحتيال على عدد كبير من المستخدمين عن طريق الروابط الاحتيالية من أجل الحصول على معلوماتهم الشخصية وبياناتهم السرية أو اختراق حساباتهم[2].

مع تزايد استخدام مواقع التواصل الاجتماعي، أصبح الحفاظ على الخصوصية أمرا صعبا لأن هذه المنصات لديها جميع بيانات مستخدميها دون علمهم، هذا ما يعرضهم لمختلف الجرائم السيبرانية مثل الاختراق، التجسس وغيرها التي تمس بشكل مباشر حقوق الإنسان خاصة الحق في حماية الحياة الخاصة، لهذا لم يعد هناك خصوصية مطلقة في العالم الرقمي.

ثانيا: الجرائم السيبرانية والتضييق على حرية التعبير

سنتطرق إلى العلاقة بين الجرائم السيبرانية والحقوق الرقمية خاصة ما يتعلق بحرية التعبير عبر الأنترنت، بسبب الاستعمال السيء لمواقع التواصل والمنصات الرقمية ظهرت

---

[1] **عمتون كمال، قدوس خديجة**، "انتهاك حقوق الإنسان في ظل انتشار الجريمة الإلكترونية"، مجلة التدوين، م12، ع02، 2020، ص136.

[2] **علوش كهينة**، "مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي بين اختراق الخصوصية وآليات المواجهة"، مجلة الدراسات، م11، ع02، 2022، ص93.

عدة جرائم إلكترونية منها جريمة التويج لخطاب الكراهية بنشر رسائل تتضمن السب والتمييز العنصري وشائعات تهدف لنشر العداوة بين الأفراد، هذا ما يمثل انتهاك لحقوق الإنسان لأنه يسبب العنف الجسدي واللفظي والمعنوي ضد فئة معينة من السكان[1].

يظهر أن خطاب الكراهية يتعارض مع حرية التعبير حيث الأول يكون بهدف الإساءة والتحريض بينما الثاني يهدف إلى نشر الأفكار والمساهمة في استقرار المجتمع، في هذا السياق حدد مقرر الأمم المتحدة الخاص بحماية حرية التعبير أربعة أنواع من التعبير المحظور قانونا ومن بينها التويج للكراهية القومية أو العنصرية أو الدينية أي التحريض على العنف[2].

رغم أن هذه القوانين التي تقيد حرية التعبير خاصة بالجرائم السيبرانية، إلا أنه هناك من الدول من تستغل هذه القوانين في تقييد حرية التعبير للأفراد والصحافة وكل من يقوم بمعارضة السلطة، هذا ما يشكل انتهاك لحقوق الإنسان المكفولة في العهد الدولي الخاص بالحقوق المدنية والسياسية.

[1] **سامر نمر سالم الجاروشة**، المرجع السابق، ص166.

[2] **عمتون كمال، قدوس خديجة**، المرجع السابق، ص138.

المبحث الثاني: إشكالات التعاون الدولي في مكافحة الجرائم السيبرانية وسبل تجاوزها

رغم التعاون الدولي في مجال مكافحة الجرائم السيبرانية إلا أنه ما زالت تعترضها مجموعة من الإشكالات التي تحد من فعاليتها وتقف عائق أمام التصدي لهذه الجرائم، تتنوع هذه الإشكالات بين الصعوبات القانونية متمثلة في تباين القوانين الوطنية وعدم ملاءمتها مع طبيعة الجرائم السيبرانية، بالإضافة للصعوبات في التعاون الدولي.

انطلاقا من هذا سيتم دراسة إشكالات التعاون الدولي في مكافحة الجرائم السيبرانية وسبل تجاوزها، وذلك بالتطرق إلى الصعوبات التي تواجه التعاون الدولي في مجال مكافحة الجرائم السيبرانية على المستوى الوطني والدولي **(المطلب الأول)**، وسبل التغلب على الصعوبات التي تواجه التعاون الدولي في مجال مكافحة الجرائم السيبرانية على المستوى الوطني والدولي **(المطلب الثاني)**.

المطلب الأول: الصعوبات التي تواجه التعاون الدولي في مجال مكافحة الجرائم السيبرانية

يعتبر التعاون الدولي من بين الركائز الأساسية في مجال مكافحة الجرائم السيبرانية، نظرا للطبيعة الخاصة لهذا النوع من الجرائم العابرة للحدود، إلا أنه يواجه العديد من الصعوبات العملية والقانونية التي تقلل من فعاليته وتعيق تحقيق أهدافه، ومن بينها عدم قدرة التشريعات الوطنية في مواكبة تطور الجرائم السيبرانية **(الفرع الأول)**، وصعوبات التعاون الدولي على المستوى الدولي **(الفرع الثاني)**.

الفرع الأول: عدم قدرة التشريعات الوطنية على مواكبة تطور الجرائم السيبرانية

يعد التعاون الدولي في مجال مكافحة الجرائم السيبرانية من أهم الوسائل للتصدي لهذه الجرائم، إلا أنه هناك عدة صعوبات أمام هذا التعاون خاصة على المستوى الوطني حيث تتمثل هذه الصعوبات في عدم كفاية وملائمة القوانين الخاصة بمكافحة الجرائم السيبرانية **(أولا)**، بالإضافة إلى صعوبة الإثبات والتحقيق في هذه الجرائم **(ثانيا)**.

أولا: عدم كفاية وملائمة القوانين الخاصة بمكافحة الجرائم السيبرانية

يؤدى الانتشار الواسع للتكنولوجيا الحديثة واعتماد المجتمع على الأنترنت في مختلف مجالات الحياة إلى ظهور جرائم سيبرانية متنوعة ومعقدة، في حين لم تواكب التشريعات الوطنية هذا التطور بالشكل الكافي حيث أن النصوص القانونية لا تزال تقليدية وتعجز عن تنظيم بعض أنواع الجرائم السيبرانية[1].

[1] **لرقط عزيزة**، "التعاون الدولي في مكافحة الجرائم المعلوماتي (إشكالاتها وآليات التغلب عليها)"، مجلة التواصل في الاقتصاد والإدارة والقانون، م25، ع04، 2018، ص03.

رغم أن الكثير من الدول أصدرت قوانين خاصة بالجرائم السيبرانية ووقعت اتفاقيات دولية لمواجهتها، إلا أن هذه التشريعات لا زالت غير كافية للتصدي لهذه الجرائم التي تقع عبر الإنترنت، كما أن القوانين التقليدية الموجودة في معظم الدول تتضمن قواعد عامة للجرائم التقليدية وهذا لا يتناسب مع الجرائم السيبرانية بسبب اختلافها من حيث الطبيعة والخصائص، مما يصعب متابعة مرتكبي هذه الجرائم والتصدي لها[1].

ثانيا: صعوبة الإثبات والتحقيق في الجرائم السيبرانية

تعد الجرائم السيبرانية من الجرائم المستحدثة التي تتميز بخصوصية في التنفيذ والإثبات، الأصل أن الجريمة ترتكب في نفس مكان وقوع الفعل غير أن الجريمة السيبرانية عادة ما تنفذ في مكان ويكتشف آثارها في مكان آخر، مما يعيق تدخل الأجهزة الأمنية في الوقت المناسب كونها مختلفة عن الجرائم التقليدية والتي ترتكب في بيئة افتراضية[2].

تتميز الجرائم السيبرانية أن آثارها المادية غير موجودة، فلا توجد أدلة ملموسة أو أقوال شهود أو حالات تلبس فالأدلة تكون عبارة عن بيانات إلكترونية لذا يجب على المحقق أن يكون متمكن بشكل جيد في التعامل مع أنظمة الكمبيوتر حتى يستطيع التعامل مع الأدلة الرقمية والحفاظ عليها بشكل صحيح، لأن الجاني يحاول دائما إخفاء الأدلة وتعقيد الوصول إليها من خلال عدة وسائل بعد ارتكاب الجريمة[3].

---

[1] **عادل عبد العالي إبراهيم خراشي**، "إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها"، مجلة كلية الشريعة والقانون، د.س.ن، ص 229. متوفر على الموقع: https://jfslt.journals.ekb.eg/article_14124_9940c95e1f087a055130abff802ddbd8.pdf تم الاطلاع عليه بتاريخ: 2025/04/29، على الساعة: 13:26.

[2] **لرقط عزيزة**، المرجع السابق، ص ص03-04.

[3] **عادل عبد العالي إبراهيم خراشي**، المرجع السابق، ص230.

الفرع الثاني: صعوبات التعاون الدولي في مكافحة الجرائم السيبرانية على المستوى الدولي

إضافة إلى الصعوبات التي تواجه التعاون الدولي على المستوى الوطني نجد أن هناك عدة عوائق على المستوى الدولي، منها ما تعلق باختلاف في تحديد الأفعال المجرمة والنظم الإجرائية **(أولا)**، ومنها ما يخص التجريم المزدوج وعدم وجود قنوات اتصال **(ثانيا)**، وأشدها تلك التي تتعلق بالصعوبات القضائية **(ثالثا)**.

أولا: اختلاف في تحديد الأفعال المجرمة والنظم القانونية الإجرائية

ترتبط صعوبة التعاون الدولي في مجال مكافحة الجرائم السيبرانية في الاختلاف في تحديد الأفعال المجرمة من جهة **(1)**، وكذا اختلاف النظم القانونية الإجرائية **(2)**.

1/ اختلاف في تحديد الأفعال المجرمة

يتضح من القوانين المعمول بها في الكثير من الدول لمواجهة الجرائم السيبرانية، أنه هناك اختلاف في تحديد الأفعال المجرمة حيث نجد ما يعتبر مباح في نظام قانوني لدولة قد يجرم في نظام قانوني لدولة أخرى[1]، يعود ذلك إلى مجموعة من الأسباب والعوامل من بينها اختلاف العادات والتقاليد، تنوع الثقافات من دولة لأخرى الشيء الذي جعل السياسة التشريعية تختلف من دولة لأخرى[2]، هذا ما يعيق التعاون الدولي في مجال مكافحة الجرائم السيبرانية ويسمح للمجرمين من الإفلات من العقاب[3].

---

[1] **محمد عادل علي عبد السلام**، المرجع السابق، ص262.

[2] **بدري فيصل**، المرجع السابق، ص109.

[3] **عادل عبدالعال إبراهيم خراشي**، المرجع السابق، ص235.

2/ اختلاف النظم القانونية الإجرائية

يقصد باختلاف النظم القانونية الإجرائية بين الدول، هو أن تكون بعض طرق التحري والتحقيق والمحاكمة مسموحة وفعالة في دولة ما بينما تعد غير مشروعة أو غير فعالة في دولة أخرى[1]، مثال عن ذلك المراقبة الإلكترونية هناك من الدول من تعتمد عيه وهناك من ترى فيه مساس بالحريات الخاصة للفرد لهذا لا تعتمد عليه[2]، كل هذا يجعل من التعاون الدولي صعب لأنه قد ترفض دولة ما الاعتراف بدليل تم جمعه بطريقة لا تعتبرها مشروعة حتى ولو تم جمعه بشكل قانوني في تلك الدولة[3].

ثانيا: غياب التجريم المزدوج وعدم وجود قنوات اتصال

تكمن الصعوبة أيضا في مجال مكافحة الجرائم السيبرانية في إشكالية التجريم المزدوج **(1)**، وعدم وجود قنوات اتصال **(2)**.

1/ غياب التجريم المزدوج

يقصد بالتجريم المزدوج هو أن يكون الفعل المطلوب فيه تسليم المجرمين خاضع للتجريم والعقاب في قوانين كلتا الدولتين[4]، وهو من أهم الشروط لتسليم المجرمين إلا أنه يعتبر عائقا عندما يتعلق الأمر بالجرائم السيبرانية، لأن الكثير من التشريعات لم تجرم هذه الأفعال بشكل صريح إضافة إلى أن القوانين التقليدية لم تعد كافية للتعامل مع هذه الجرائم

---

[1] **مبروك فاطيمة، ذيب محمد**، "التعاون الدولي لمكافحة الجريمة الإلكترونية، الأشكال والإشكالات"، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، م11، ع01، 2024، ص121.

[2] **لرقط عزيزة**، المرجع السابق، ص05.

[3] **محمد عادل علي عبد السلام**، المرجع السابق، ص263.

[4] نفس المرجع ، ص265.

مما يؤدي إلى صعوبة في تطبيق الاتفاقيات الدولية الخاصة بتسليم المجرمين ويعيق جهود جمع الأدلة ومتابعة المجرمين[1].

2/ عدم وجود قنوات اتصال

يعد التعاون الدولي عاملا أساسيا في مكافحة الجرائم السيبرانية، حيث يهدف إلى تبادل المعلومات الخاصة بالمجرمين ولتحقيق هذا يجب أن يكون هناك اتصال مع الهيئات الأجنبية، مما يسهل عملية جمع الأدلة والمعلومات اللازمة للكشف عن الجرائم، إن غياب قنوات الاتصال يشكل عائق في الحصول على الأدلة الإلكترونية هذا ما يضعف الجهود الدولية في مكافحة الجرائم السيبرانية[2].

ثالثا: الصعوبات القضائية

من بين الصعوبات التي تواجه التعاون الدولي نجد ما يتعلق بالشق القضائي، نذكر منها الصعوبات المرتبطة بالاختصاص القضائي **(1)**، وعدم الاستجابة لطلبات المساعدة القضائية **(2)**.

1/ الصعوبات المرتبطة بالاختصاص القضائي

الأصل أن الاختصاص القضائي محدد مسبقا في القوانين الوطنية لكل دولة، لكن عنما يتعلق الأمر بالجرائم الدولية فقد نجد إشكال في الاختصاص بسبب اشتراك عدة دول فيها[3]، ويقصد بتنازع الاختصاص القضائي بين الدول عندما ترفع دعوى بشأن نفس الجريمة

---

[1] لرقط **عزيزة**، المرجع السابق، ص06.

[2] **شنتير خضرة**، الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية بأدرار–الجزائر–،2021، ص217.

[3] **بدري فيصل**، المرجع السابق، ص113.

أمام أكثر من جهة قضائية تابعة لدول مختلفة، بحيث كل دولة تريد ممارسة اختصاصها ويسمى بتنازع الاختصاص الإيجابي وقد ترفض كل الدول النظر في الدعوى بحجة عدم الاختصاص وهو ما يسمى تنازع الاختصاص السلبي[1].

يعود السبب للنزاعات الناشئة حول الاختصاص القضائي في الجرائم السيبرانية لأنها عابرة للحدود، مثلا إذا ارتكب شخص أجنبي جريمة داخل دولة معينة فإن هذه الدولة لها حق الاختصاص الجنائي وفقا لمبدأ الإقليمية، في نفس الوقت قد تدعي دولته حق الملاحقة استنادا إلى مبدأ الاختصاص الشخصي، وإذا كانت الجريمة تهدد أمن وسلامة دولة أخرى فإنها تخضع لاختصاصها بموجب مبدأ العينية[2].

2/ عدم الاستجابة لطلبات المساعدة القضائية

تعرف المساعدة القضائية بأنها "**كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم**"[3]، ومن صور المساعدة القضائية نجد الإنابة القضائية التي بدورها تواجه تحديا كبيرا بسبب إجراءاتها الدبلوماسية التي تجعل من إجراءات التسليم بطيئة ومعقدة، وهو ما يتعارض مع طبيعة الجرائم السيبرانية التي تتميز بالسرعة والتطور المستمر[4]، تجدر الإشارة إلى أن العديد من القضايا المرتبطة بالجرائم الإلكترونية يتم شطبها نتيجة عدم الاستجابة لطلبات المساعدة القضائية ضمن المهلة المحددة قانونا[5].

---

[1] **لرقط عزيزة**، المرجع السابق، ص05.

[2] **محمد عادل علي عبد السلام**، المرجع السابق، ص265.

[3] **شنتير خضرة**، المرجع السابق، ص218.

[4] **بدري فيصل**، المرجع السابق، ص111.

[5] **مبروك فاطيمة، ذيب محمد**، المرجع السابق، ص112.

المطلب الثاني: سبل التغلب على الصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم السيبرانية

أصبحت الجرائم السيبرانية من أخطر الظواهر الإجرامية المعاصرة، نظرا لطبيعتها وسرعة انتشارها وتطورها المستمر، وللتصدي لها يجب تفعيل التعاون الدولي بين مختلف الأجهزة المختصة بين الدول، إلا أن هذا التعاون الدولي يواجه عدة تحديات وعراقيل على المستويين الوطني والدولي.

من خلال ما سبق يجب البحث عن سبل وآليات فعالة للتغلب على هذه الصعوبات ولتعزيز فعالية التعاون الدولي، يتم ذلك بالبحث عن التدابير الموضوعية والإجرائية لمكافحة الجرائم السيبرانية على المستوى الوطني **(الفرع الأول)**، التغلب على التحديات التي تواجه التعاون الدولي في مجال مكافحة الجرائم السيبرانية **(الفرع الثاني)**.

الفرع الأول: التدابير الموضوعية والإجرائية لمكافحة الجرائم السيبرانية على المستوى الوطني

يبدأ تفعيل التعاون الدولي في مجال مكافحة الجرائم السيبرانية على المستوى الوطني، لهذا فإن أي صعوبات تواجه التعاون الدولي يجب العمل على التغلب عليها، من بين أهم الآليات للتغلب على الصعوبات التي تواجه التعاون الدولي في مجال مكافحة الجرائم السيبرانية على المستوى الوطني هي اتخاذ التدابير الموضوعية **(أولا)**، والتدابير الإجرائية **(ثانيا)**.

أولا: التدابير الموضوعية

تواجه الدول صعوبات حقيقية في التعامل مع الجرائم السيبرانية بسبب طبيعتها الخاصة والمعقدة والتي تختلف عن الجرائم التقليدية ذات الطابع المادي، لذلك أصبح من الضروري

على الدول أن تضع نصوص قانونية جديدة تتلاءم مع هذا النوع من الجرائم، بدلا من الاعتماد على النصوص القديمة التي أثبتت عدم فعاليتها[1].

ينبغي على كل دولة أن تضع سياسة تشريعية تتعاون من خلالها مع باقي الدول لمواجهة مخاطر الجرائم السيبرانية، كما يجب اتخاذ تدابير قانونية وتقنية للكشف المبكر عن هذه الجرائم والتصدي لهذه التهديدات المتطورة[2].

لا يكفي سن قوانين جديدة، بل يجب أيضا تعديل القواعد القانونية المتعلقة بمحل الجريمة لأن الجرائم السيبرانية غالبا ما تكون غير ملموسة، يعتبر هذا التعديل أساسي لضمان مرونة القانون وقدرته على مواكبة التطورات التقنية المستمرة، مما يساهم في تحسين التعاون الدولي في مكافحة هذه الجرائم[3].

ثانيا: التدابير الإجرائية

للتصدي للصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم السيبرانية، يجب على الدول اتخاذ مجموعة من التدابير الإجرائية، نذكر منها[4]:

- سن تشريعات إجرائية تمنح الجهات المختصة صلاحية تفتيش أنظمة الحاسوب وفحص البيانات المخزنة، متى كان ذلك ضروريا لمصلحة التحقيق.
- يجب على كل دولة وضع نصوص قانونية تمكن سلطاتها من القبض على الأشخاص المتورطين سواء داخل الدولة أو خارجها، مع تعزيز التعاون في هذا المجال.

---

[1] **لرقط عزيزة**، المرجع السابق، ص07.

[2] **عادل عبد العال إبراهيم خراشي**، المرجع السابق، ص250.

[3] **لرقط عزيزة**، المرجع السابق، ص07.

[4] **عادل عبد العال إبراهيم خراشي**، المرجع السابق ص 253-254.

- منح صفة الضبطية القضائية للعاملين في مجال خدمات الإنترنت والاتصالات بسبب اتصالهم المباشر بحركة الشبكة، وقيامهم بالتحفظ على الأدلة لغاية وصول السلطات المختصة.
- تعزيز التعاون بين أجهزة الشرطة بين الدول من خلال اتفاقيات دولية، بحيث يتم الإبلاغ عن أي جريمة سيبرانية عابرة للحدود فور اكتشافها.

نصت الاتفاقيات الدولية المتعلقة بالجرائم السيبرانية على ضرورة التزام الدول بإنشاء هيئات وطنية متخصصة تتولى استقبال الشكاوى والبلاغات المرتبطة بهذا النوع من الجرائم، إضافة إلى اتخاذ تدابير وقائية للحد من انتشارها[1].

الفرع الثاني: التغلب على التحديات التي تواجه التعاون الدولي في مجال مكافحة الجرائم السيبرانية

لا يكفي مواجهة الصعوبات التي تواجه التعاون الدولي على المستوى الوطني، بل يجب إيجاد سبل للتغلب على الصعوبات التي تواجه التعاون الدولي على المستوى الدولي، من أبرز هذه الصعوبات التي يجب التغلب عليها نجد سبل مواجهة عدم وجود نموذج موحد للنشاط الإجرامي واختلاف النظم القانونية الإجرائية **(أولا)**، والتصدي للمشكلات المرتبطة بمجالي قنوات اتصال والتدريب **(ثانيا)**، وأخيرا طرق تجاوز الاشكالات القضائية **(ثالثا)**.

[1] **لرقط عزيزة**، المرجع السابق، ص08.

أولا: سبل مواجهة عدم وجود نموذج موحد للنشاط الإجرامي واختلاف النظم القانونية الإجرائية

إن من أهم الحلول الازمة لمواجهة عدم وجود نموذج موحد للنشاط الإجرامي واختلاف النظم القانونية الإجرائية وجوب التوافق حول موضوعات الجرائم السيبرانية وطنيا ودوليا ٠**(1)** وكذا توحيد النظم القانونية الإجرائية الخاصة بمكافحة الجرائم السيبرانية **(2)**.

1/ ضرورة التوافق حول موضوعات الجرائم السيبرانية وطنيا ودوليا

تعد مشكلة غياب نموذج موحد للنشاط الإجرامي المعلوماتي من أبرز العقبات التي تعرقل التعاون الدولي في مجال مكافحة الجرائم السيبرانية[1]، ونظرا لصعوبة توحيد الأنظمة القانونية للدول عمليا، فإن الحل يكمن في العمل على تحديث التشريعات الوطنية الخاصة بالجرائم المعلوماتية وإبرام اتفاقيات دولية تراعي طبيعة هذه الجرائم وتعزز من سبل مكافحتها[2].

2/ توحيد النظم القانونية الإجرائية الخاصة بمكافحة الجرائم السيبرانية

تسعى معظم دول العالم إلى تعديل التشريعات الإجرائية وذلك لمواكبة التطورات المتسارعة التي تشهدها الجرائم الإلكترونية، مع تعديل قانون العقوبات الخاصة بها وترتكز هذه الإصلاحات في تحديث الإجراءات الجنائية المتعلقة بإثبات هذا النوع من الجرائم، حيث تهدف التشريعات الحديثة إلى دمج تقنية المعلومات في مختلة مراحل الإجراءات الجنائية بما يسهل من التحقيق في الجرائم السيبرانية[3].

---

[1] **بدري فيصل**، المرجع السابق، ص114.

[2] **محمد عادل علي عبد السلام**، المرجع السابق، ص267.

[3] **عادل عبد العال إبراهيم خراشي**، المرجع السابق، ص264.

جاءت معظم الاتفاقيات الدولية والإقليمية الخاصة بمكافحة الجرائم العابرة للحدود منها الجرائم الإلكترونية على حث الدول الأطراف على الاعتماد بتقنيات التحقيق الخاصة، سعيا منها لمعالجة الاختلاف بين الأنظمة القانونية الاجرائية وتحقيق تقارب يعزز من التعاون الدولي في مكافحة هذه الجرائم[1].

ثانيا: التصدي للمشكلات المرتبطة بمجالي قنوات الاتصال والتدريب

في سياق الجهود المبذولة في مواجهة الصعوبات التي تواجه التعاون الدولي في مجال التعاون الدولي لمكافحة الجرائم السيبرانية، يجب خلق قنوات اتصال بين الدول **(1)**، واعداد برامج تدريبية متخصصة **(2)**.

1/ خلق قنوات اتصال فعالة بين الدول

تواجه مشكلة غياب قنوات الاتصال بين جهات إنفاذ القانون من خلال الاتفاقيات الدولية التي تحث على تعزيز التعاون بين الدول، والعمل على إنشاء قنوات اتصال رسمية بين السلطات المختصة بهدف تسهيل تبادل المعلومات، من أهم هذه الاتفاقيات نجد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية (المادة 27)، ولاتفاقية الأوروبية بشأن الإجرام المعلوماتي (المادة 27 و35)[2].

يعد توفير قنوات اتصال بين الدول من التدابير الوقائية وذلك في إطار مكافحة الجريمة، حيث تساهم في منع المجرمين من الإفلات من العقاب من خلال القبض عليه

[1] **لرقط عزيزة**، المرجع السابق، ص10.

[2] **بدري فيصل**، المرجع السابق، ص118.

حتى وإن هرب إلى دولة أخرى يتم تسليمه إلى الدولة المعنية، هذا ما يجعل الأفراد لا يرتكبون هذه الجرائم خوفا من المتابعة[1].

2/ اعداد برامج تدريبية متخصصة

يعد تدريب رجال القانون أحد أبرز مظاهر التعاون الدولي في مكافحة الجرائم الإلكترونية، لما له من دور فعال في رفع كفاءة المتدربين واكتساب مهارات وخبرات وقد خصصت العديد من الدول برامج تدريبية متخصصة في هذا المجال، لتسهيل عمليات البحث والكشف عن هذه الجرائم، ففي هذا السياق تم عقد اجتماع في إطار تنفيذ البرنامج الأوروبي لمكافحة الجرائم السيبرانية وقد شهد مشاركة 09 قضاة مختصين في قضايا الجرائم السيبرانية إلى جانب خبراء من المجلس الأوروبي، يهدف هذا الاجتماع إلى تعزيز قدرات القضاة في التكوين القاعدي والمستمر حول القضايا المرتبطة بمكافحة الجرائم السيبرانية وتحسين آليات التصدي لها[2].

ثالثا: طرق تجاوز الاشكالات القضائية

تتمثل سبل مواجهة الصعوبات القضائية في تطبيق الاختصاص القضائي العالمي على الجرائم السيبرانية **(1)**، واعتماد آلية المساعدة القضائية **(2)**.

1/ تطبيق الاختصاص القضائي العالمي على الجرائم السيبرانية

إن اعتبار الجرائم الإلكترونية من الجرائم العالمية من بين الحلول الأساسية لمشكلة تنازع الاختصاص القضائي، لأنه يجعل من كل دولة تجرم هذه الأفعال في قوانينها الداخلية بممارسة الاختصاص القضائي وفقا لمبدأ العالمية، ويقصد بهذا المبدأ تطبيق قانون العقوبات

---

[1] **محمد عادل علي عبد السلام**، المرجع السابق، ص271.

[2] **شنتير خضرة**، المرجع السابق، ص ص224-226.

الوطني على أي جريمة ترتكب خارج حدود الدولة دون النظر إلى جنسية الجاني أو الضحية أو إذا كانت الدولة الأجنبية تجرم هذا الفعل[1].

جاءت العديد من الاتفاقيات الدولية بمبدأ الاختصاص القضائي العالمي، منها اتفاقية جنيف للبحار لسنة 1958 والتي منحت للدول الحق في القبض على القراصنة ومحاكمتهم دون النظر إلى جنسيتهم أو مكان ارتكاب الجريمة، وينطبق هذا المبدأ على الهاكرز الذين يرتكبون الجرائم السيبرانية عبر الشبكة العنكبوتية التي تعد أكثر خطورة لأنها تمثل تهديد خفيا يدمر المجتمعات دون ترك أثر مادي يدل على الجريمة[2].

2/ اعتماد آلية المساعدة القضائية

تعتبر مواجهة الصعوبات الخاصة بالمساعدة القضائية من أهم خصائص مكافحة الجرائم السيبرانية، ويتم ذلك بالاعتماد على آليات سريعة وفعالة خاصة فيما يتعلق بالتأخر في الرد على طلبات بالإنابة ويتحقق ذلك من خلال استحداث وسيلة عملية كإنشاء سلطة مركزية مختصة أو السماح بالتواصل المباشر بين الجهات المعنية بالنظر في هذه الطلبات[3].

أكد مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، المنعقد في بانكوك بين 18و25 أبريل 2005 على أهمية تعزيز دور السلطات المركزية المسؤولة عن المساعدة القانونية المتبادلة من خلال إنشاء قنوات اتصال مباشرة بينها لضمان سرعة تنفيذ تلك الطلبات، هذا ما نصت عليه المادتين 27 و35 من الاتفاقية الأوروبية حول الجرائم الإلكترونية حيث ألزمت الدول الأعضاء بإنشاء هيئة اتصال تعمل 24/24 ساعة و

---

[1] **لرقط عزيزة**، المرجع السابق، ص 11.

[2] **عادل عبد العال إبراهيم خراشي**، المرجع السابق، ص ص274-275.

[3] **بدروي فيصل**، المرجع السابق، ص 119.

طيلة أيام الأسبوع، لتقديم المساعدة الفورية في التحقيقات المتعلقة بالجرائم الإلكترونية وأن يتم التواصل بين هيئات مختلف الدول[1].

[1] **محمد عادل عبد السلام**، المرجع السابق، ص275.

خاتمة

يتضح من خلال دراستنا للآليات القانونية والمؤسساتية لمكافحة الجرائم السيبرانية أن المجتمع الدولي قد قام بمجهودات كبيرة في سبيل التصدي لهذا النوع من الجرائم المستحدثة والعابرة للحدود، يظهر ذلك من خلال اعتماد عدة اتفاقيات دولية وإقليمية، في مقدمتها اتفاقية بودابيست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، واتفاقية الإتحاد الإفريقي للأمن السيبرانية، إلى جانب الدور المهم الذي تلعبه المنظمات الدولية على رأسها هيئة الأمم المتحدة والإنتربول في تعزيز التعاون الدولي وتفعيل آليات الوقاية.

رغم ما تحقق من نتائج إيجابية في مجال مكافحة الجرائم السيبرانية، إلا أن هناك العديد من التحديات خاصة ما تعلق بتباين التشريعات الوطنية وغياب إطار قانوني دولي موحد وشامل خاص بهذا النوع من الجرائم، إضافة إلى الإخفاقات المتعلقة بحماية سيادة الدول وضمان احترام الحقوق والحريات الأساسية، وعليه فيجب العمل على تطوير النصوص القانونية الوطنية والدولية بما يتماشى مع طبيعة هذه الجرائم وكذا تعزيز آليات التعاون والتنسيق الدولي، وتدعيم قدرات الهيئات الأمنية والقضائية المتخصصة وضمان التوازن بين مكافحة الجرائم السيبرانية واحترام حقوق الإنسان.

من خلال ما سبق يمكن استخلاص مجموعة من **النتائج** نذكر منها:

- أن المجتمع الدولي أصبح يهتم أكثر بمكافحة الجرائم السيبرانية من خلال اعتماد مجموعة من الاتفاقيات الدولية والإقليمية في هذا المجال.
- للمنظمات الدولية دور فعال في مكافحة الجرائم السيبرانية من خلال تنسيق الجهود الدولية وتعزيز التعاون الدولي.
- هناك عدة تحديات تواجه مكافحة الجرائم السيبرانية على المستوى الوطني والدولي منها ما يتعلق بالجريمة ومرتكبيها، منها ما تعلق بآليات مكافحة هذه الجرائم.

استنادا إلى ما تم عرضه نقترح بعض **التوصيات**:

- الإسراع في وضع اتفاقية الأمم المتحدة لمنع ومكافحة الجرائم السيبرانية حيز النفاذ.
- انشاء محكمة دولية خاصة لمتابعة مرتكبي الجرائم السيبرانية.
- تشديد العقوبات الخاصة بمرتكبي الجرائم السيبرانية.
- تعزيز التعاون الدولي من خلال وضع اتفاقية دولية ملزمة لتسليم مرتكبي الجرائم السيبرانية.
- مراجعة التشريعات الوطنية بما يتماشى مع تطور الجرائم السيبرانية وتوحيد موضوعاتها.
- انشاء مراكز متخصصة في التكوين لمكافحة الجرائم السيبرانية.
- ضرورة التوافق بين مكافحة الجرائم السيبرانية وعدم المساس بحقوق الإنسان حرياته الأساسية.

قائمة المراجع

أولا: المراجع باللغة العربية

I. الكتب

1. **حسين عباس حميد**، نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية، دار النهضة العربية للنشر والتوزيع، القاهرة، 2021.

2. **سامر نمر سالم الجاروشة**، الجرائم السيبرانية وحقوق الإنسان في القوانين الدولية والوطنية، دار النهضة العربية للنشر والتوزيع، القاهرة، 2023.

3. **شريف حسين محمد محمد حسن**، الجرائم الإلكترومعلوماتية "مفهوم جديد في جرائم الوسط الجيوسيبراني"، دار النهضة العربية، د.ب.ن، 2022.

4. **طاهري حسين**، الجرائم الإلكترونية، دار الخلدونية للنشر والتوزيع، الجزائر، 2022.

5. ----------، جرائم القرصنة الإلكترونية، دار الخلدونية للنشر والتوزيع، الجزائر، 2023.

6. **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والأنترنت {الجرائم الالكترونية} دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، لبنان، 2007.

7. **محمد عادل علي عبد السلام**، الأحكام الإجرائية في جريمة السرقة السيبرانية–دراسة مقارنة–، دار النهضة العربية للنشر والتوزيع، القاهرة، 2023.

8. **محمد عباس محسن**، الهجمات السيبرانية ومنطقة الفراغ التشريعي دراسة في ميثاق الأمم المتحدة والقانون الدولي، منشورات ألفا للوثائق، قسنطينة، 2021.

9. **هالة أحمد الرشيدي**، الإرهاب السيبراني –ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية–، دار النهضة العربية للنشر والتوزيع، القاهرة2021.

II. الأطروحات الجامعية

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

2. **شنتير خضرة**، الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية بأدرار–الجزائر–،2021.

3. **عمر يوسف عبد الله**، الإطار القانوني والمؤسساتي لمكافحة التقليد والقرصنة الإلكترونية، أطروحة للحصول على شهادة الدكتوراه في العلوم، القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة وهران 02، 2022.

4. **عميمر عبد القادر**، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراه علوم في القانون الدولي، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1–بن يوسف بن خدة–، الجزائر، 2020.

III. المقالات

1. **بركات رياض، محمد الصغير مسيكة،** "تسليم الجرمين كآلية لتفعيل التعاون الدولي لمكافحة الجرائم المعلوماتية"، مجلة الدراسات الحقوقية، المجلد11، العدد01، الجزائر، 2024، ص ص 130-151.

2. **بن قطاط خديجة،** "تداعيات الحروب السيبرانية على السيادة الرقمية"، مجلة القانون العام الجزائري والمقارن، المجلد 10، العدد 02، الجزائر، 2024، ص ص 280-299.

3. **بوقرين عبد الحليم، قطاف سليمان،** "الأليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، مجلة الأكاديمية للبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، المجلد 06، العدد01، الجزائر، 2022، ص ص 334-358.

4. ----------، "مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، المجلد 05، العدد 02، الجزائر 2022، ص ص 62-87.

5. **ربيعي حسين،** "المجرم المعلوماتي-شخصيته وأصنافه-"، مجلة العلوم السياسية، جامعة محمد خيضر بسكرة، المجلد 15، العدد 01، الجزائر، 2015، ص ص -302 285.

6. **زكري محمد،** نشأة الجريمة المعلوماتية من بداية الستينات إلى القرن ال21 "التحقيقات الجنائية في مجال مكافحة الجريمة المعلوماتية"، مجلة الشرطة العلمية والتقنية، العدد 04، الجزائر، 2019، ص ص 6-9.

7. **شرقي عبد الغاني**، "التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة لسيادة واستقالية"، مجلة السياسة العالمية، المجلد 07، العدد 02، الجزائر، 2023، ص ص 270-286.

8. **عفاف بعون، نسيمة أولاد سالم**، ""الجريمة الالكترونية-قراءة سوسيوتاريخية في النشأة والأثار-"، مجلة القبس للدراسات النفسية والإجتماعية، جامعة قاصدي مرباح ورقلة، المجلد 05، العدد 20، الجزائر، 2023. ص ص 69-94.

9. **علواش كهينة**، "مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي بين اختراق الخصوصية وآليات المواجهة"، مجلة الدراسات، المجلد 11، العدد 02، الجزائر، 2022، ص ص 88-105.

10. **عمتون كمال، قدوس خديجة**، "انتهاك حقوق الإنسان في ظل انتشار الجريمة الإلكترونية"، مجلة التدوين، المجلد 12، العدد 02، الجزائر، 2020، ص ص -140 128.

11. **فريد ناشف**، "آليات التعاون الدولي في مكافحة الجرائم الإلكترونية"، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، الجزائر، 2022، ص ص 430-450.

12. **كاوجة محمد الصغير**، "الهجمات السيبرانية بين الواقع وسبل المواجهة"، مجلة الرسالة للدراسات الإعلامية، جامعة العربي التبسي-تبسة، المجلد 06، العدد 03، الجزائر، 2022، ص ص 108-117.

13. **لرقط عزيزة**، "التعاون الدولي في مكافحة الجرائم المعلوماتي (إشكالاتها وآليات التغلب عليها)"، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 25، العدد 04، الجزائر، 2018 ص ص 01-18.

14. **لزعر عبد العزيز، زياني رشيد،** "آليات الإتحاد الإفريقي للتعاون الشرطي(الأفريبول) ودورها في مكافحة الجريمة الإلكترونية"، مجلة متون، جامعة مولاي الطاهر سعيدة، المجلد 14, العدد 03، الجزائر، 2021، ص ص 251-270.

15. **لوكل مريم،**" قراءة في اتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات طابع الشخصي لسنة 2014"، مجلة الدراسات القانونية والاقتصادية، المجلد 03، العدد 03، الجزائر، 2021، ص ص 657-673.

16. **مبروك فاطيمة، ذيب محمد،** "التعاون الدولي لمكافحة الجريمة الإلكترونية، الأشكال والإشكالات"، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 11، العدد 01، الجزائر، 2024، ص ص 113-128

17. **ودرار أمين،** "الشرطة الجنائية الإفريقية "الأفريبول" "، حوليات جامعة الجزائر 1، جامعة بن يوسف بن خدة، المجلد 34، العدد 01، الجزائر، 2020، ص ص 135-149.

IV. الاتفاقيات الدولية

1. **ميثاق منظمة الأمم المتحدة،** الموقع من طرف مندوبي حكومات الأمم المتحدة، بتاريخ 26جوان1945، دخل حيز التنفيذ في 24أكتوبر1945، انضمت الجزائر إلى هيئة الأمم المتحدة في 04أكتوبر1962 بموجب قرار الجمعية العامة للأمم المتحدة رقم 176 {د-17}، الصادر بتاريخ 04أكتوبر1962 في جلستها رقم 1020.

2. **الاتفاقية المتعلقة بالجريمة الالكترونية،** المعتمدة بموجب القرار رقم 185، الصادر عن مجلس أوروبا، بودابست، المؤرخ في 23 نوفمبر 2001، متوفر على الموقع: https://rm.coe.int/budapest-convention-in-arabic/1680739173.

3. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 2014/09/08، ج.ر.ج.ج عدد 57، المؤرخ في 2014/09/28 متوفر على الموقع: https://esttf.motrans.gov.iq/wp-content/uploads/2016/04/الاتفاقية-العربية-لمكافحة-جرائم-تقنية-المعلومات.pdf

4. **اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصية**، تم اعتمادها في الدورة العادية 23 لقمة رؤساء دول والحكومات الإتحاد الإفريقي المنعقد في مالابو-غينيا الاستوائية-، في 27 جوان 2014، متوفر على الموقع: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

V. المواقع الإلكترونية

1. **جمال محمد خلفان محمد النقبي، سلطان محمد سالم عوض هيسان المصعبي**، " التعاون الوطني والدولي في الجرائم الإلكترونية "المشكلات والحلول" "، مجلة المعهد العالي للدراسات النوعية، المجلد03، العدد16، د.ب.ن، 2023، ص ص 5449-5550. متوفر على الموقع: https://hiss.journals.ekb.eg/article_342134.html .

2. **عادل عبد العالي إبراهيم خراشي**، "إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها"، مجلة كلية الشريعة والقانون، مصر، د.س.ن، ص ص 129-330. متوفر على الموقع:

https://jfslt.journals.ekb.eg/article_14124_9940c95e1f087a055130a bff802ddbd8.pdf .

3. **عماد حسين محمد الفريحات**،" الجهود العربية والإفريقية لمواجهة الجرائم الإلكترونية في الفترة 2010-2023"، مجلة ابن خلدون للدراسات والأبحاث، المجلد03، العدد05، فلسطين، 2023، ص ص 190-219. متوفر على الموقع: https://www.benkjournal.com/article/view/323/298 .

4. **محمد محمود زيتون**، "العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني"، مجلة وميض الفكر، العدد25، لبنان، 2025، ص ص 178-211، متوفر على الموقع: https://wameedalfikr.com/?p=2522 .

5. **المنظمة الدولية للشرطة الجنائية**، متوفر على الموقع: https://www.interpol.int/ar/3/12 .

ثانيا: المراجع باللغة الفرنسية

I. Ouvrages

1. **Chawki(M)**, Essai sur la nation de cybercriminalité, IEHEI, s.l, 2006.

2. **Rosé P** la criminalité informatique, QSJ, Paris, s.d.

II. Thèses

- **Romain Boos**, La Lutte Contre La Cybercriminalité au Regard de l'action des états, thèse de Doctorat en Droit privé et

Sciences Criminelles, Faculté de Droit Sciences Économiques et Gestion, Université de Lorraine, Français, 2016.

III. Article

- **Maupeou S**, Cybercriminalité, cyberconflits, Revue de la Défense nationale et sécurité collective, 2009, pp 5-141.

الفهرس

الفهرس

الملخص

ملخص باللغة العربية:

تعتبر الجرائم السيبرانية من الجرائم الحديثة التي أصبحت تشكل تهديد حقيقي على الدول، هذا ما جعل المجتمع الدولي يسعى للتصدي لها من خلال مجموعة من الآليات القانونية المتمثلة في اتفاقية بودابست دوليا والاتفاقية العربية لمكافحة جرائم تقنية المعلومات واتفاقية مالابو اقليميا، كما ساهمت المنظمات الدولية مثل الأمم المتحدة والإنتربول الأفريبول في التصدي لهذه الجرائم من خلال دعم التعاون الأمني والتدريبي وتسليم المجرمين.

رغم الإنجازات التي حققتها هذه الآليات إلا أنها لم تسلم من بعض الإخفاقات التي مست سيادة الدول وحقوق الإنسان وحرياته الأساسية، وهذا كله بسبب العراقيل التي تعترضها على المستوى الوطني والدولي والتي تحد من نجاعته، وهذا ما يستوجب تكثيف الجهود للتصدي لها لضمان مكافحة الجرائم السيبرانية بكل فعالية.

الكلمات المفتاحية: مكافحة، الجرائم السيبرانية، الآليات، القانون الدولي.

Résumé en français :

La cybercriminalité est considérée parmi les crimes modernes qui représentent une menace réelle pour les États. C'est pourquoi la communauté internationale s'est employée à y faire face à travers un ensemble de mécanismes juridiques, notamment la Convention de Budapest au niveau international, la Convention arabe sur la lutte contre les crimes liés aux technologies de l'information et la Convention de Malabo au niveau régional. De même, des organisations internationales telles que les Nations Unies, Interpol et Afripol ont contribué à cette lutte en soutenant la coopération en matière de sécurité, de formation et d'extradition des criminels.

Malgré les avancées réalisées grâce à ces mécanismes, certains échecs subsistent, portant atteinte à la souveraineté des États, ainsi qu'aux droits de l'homme et à ses libertés fondamentales. Ces limites sont essentiellement dues aux obstacles rencontrés aux niveaux national et international, entravant ainsi leur efficacité. Cela exige de redoubler d'efforts afin d'assurer une lutte effective contre la cybercriminalité.

Mots-clés : lutte contre la cybercriminalité, mécanismes, droit international.