جامعـة غرداية
كليـة الحقوق والعلوم السياسية
قســـم الحقوق

الجهود الدولية في مواجهة الجرائم السبيرانية

مذكرة مقدمة لاستكمال متطلبات نيل شهـادة ماستر أكاديمي حقوق تخصص قانون جنائي

إعداد الطالبة:
- بن أوذينة سندس

إشراف الأستاذ الدكتور:
خطوي عبد المجيد

لجنة المناقشة:

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
زرباني محمد مصطفى	استاذ التعليم العالي	جامعة غرداية	رئيسا
خطوي عبد المجيد	أستاذ التعليم العالي	جامعة غرداية	مشرفا مقررا
سكيريفة محمد الطيب	استاذ محاضر قسم أ	جامعة غرداية	عضوا مناقشا

نوقشت بتاريخ: 2025/06/02م

الموسم الجامعي:2025/2024

جامعـة غرداية
كليـة الحقوق والعلوم السياسية
قســـم الحقوق

الجهود الدولية في مواجهة الجرائم السبيرانية

مذكرة مقدمة لاستكمال متطلبات نيل شهـادة ماستر أكاديمي حقوق تخصص قانون جنائي

إعداد الطالبة:
- بن أوذينة سندس

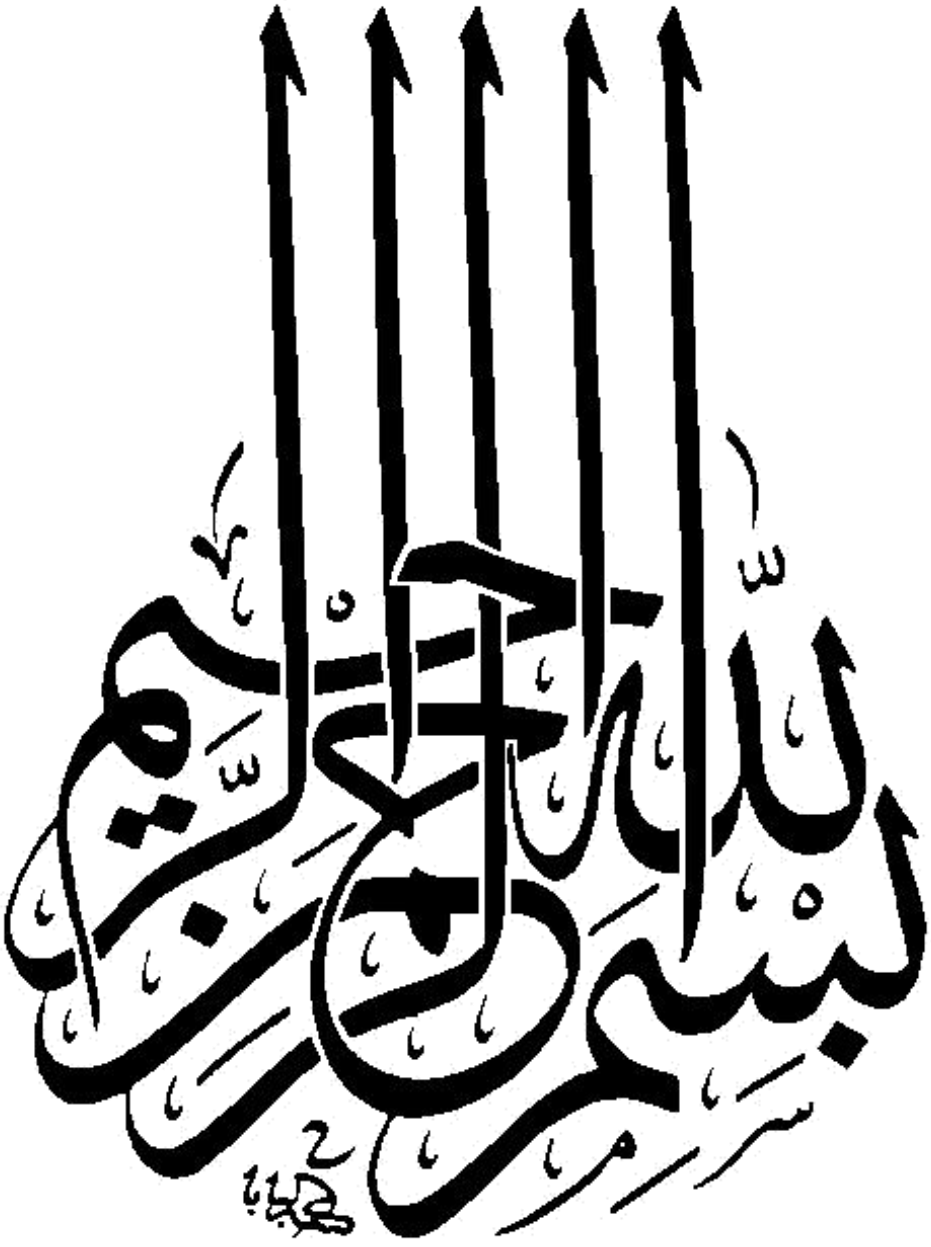
إشراف الأستاذ الدكتور:
خطوي عبد المجيد

لجنة المناقشة:

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
زرباني محمد مصطفى	استاذ التعليم العالي	جامعة غرداية	رئيسا
خطوي عبد المجيد	أستاذ التعليم العالي	جامعة غرداية	مشرفا مقررا
سكيريفة محمد الطيب	استاذ محاضر قسم أ	جامعة غرداية	عضوا مناقشا

نوقشت بتاريخ: 2025/06/02م

الموسم الجامعي:2025/2024


بسم الله الرحمن الرحيم

شكر و تقدير

بسم الله الرحمان الرحيم والصلاة والسلام على أشرف المرسلين محمد الصادق الأمين عليه أفضل الصلاة و التسليم. أولا والأولى الله نشكر ربنا الذي وفقنا لإتمام هذا العمل.

كما أقدم شكري الخالص لكل أساتذتنا الكرام الذين ساهموا في تعليمنا وتكويننا وأخص بالذكر الأستاذ خطوي عبد المجيد الذي له الفضل كبير في إنجاز هذا العمل وأسأل الله أن يجزيه عنا كل الخير ويديم عليه الصحة والعافية.

وأشكر كل من كان عونا لي و موجها لي في مشواري التعليمي

إهـداء

أهدي هذا العمل إلى سندي في السراء والضراء و للذي من أجلهما بذلت هذا المجهود والدي الكريمين أطال الله في عمرهما وأحسن عملهما ... والدي اللذان اشهد لهما بالتضحية و التعب من اجل راحتي ...اللذان حملا العبء معي من اجل نجاحي كما اهديه إلى إخوتي و خاصة صغيرتي مرام والى زوجي الداعم حفظهم الله لي و لا أراني فيهم إلا خيرا .

قائمة المختصرات:

*ص: صفحة

*ط: طبعة

*ق: قانون

*ج س :الجريمة السبيرانية

*س : السبيراني

*ق ع:قانون العقوبات

*إ د : اتفاقية دولية

*م ر:مرسوم رئاسي

مقدمة

مقدمة

في عصر الثورة الرقمية، حيث أصبح الفضاء السيبراني عصباً للحياة العصرية ومحركاً رئيسياً للاقتصاديات والأنظمة السياسية والاجتماعية، ظهرت (الجريمة السيبرانية) كأحد أبرز التحديات العالمية التي تهدد الأمن القومي للدول واستقرار المجتمعات. فمع تزايد الاعتماد على التقنيات الرقمية في مختلف المجالات، تطورت أساليب الهجمات الإلكترونية لتشمل اختراق البنى التحتية الحيوية، وسرقة البيانات الحساسة، وتزييف الهوية، بل وحتى التأثير على العمليات الديمقراطية عبر التضليل الإعلامي .

في مواجهة هذه التهديدات المتشعبة، لم تعد الجهود الفردية للدول كافية، بل أصبح التعاون الدولي ضرورة حتمية لمواكبة التعقيدات المتسارعة لهذه الجرائم. تتبلور الجهود الدولية لمكافحة الجريمة السيبرانية في إطار مبادرات مشتركة تجمع الحكومات والمنظمات الدولية والقطاع الخاص كمبادرات الاتحاد الأوروبي و الشرطة الجنائية الدولية، سعياً لبناء أنظمة دفاعية متكاملة، وتشريعات موحدة، وآليات تنسيق فوري للاستجابة للهجمات العابرة للحدود .

كما تهدف هذه المذكرة إلى تسليط الضوء على طبيعة هذه الجهود و التعرف عليها ، بدءاً من الاتفاقيات الدولية مثل "اتفاقية بودابست" كإطار قانوني،مرورا بمبادرات المنظمات الدولية كمنظمة التعاون الاقتصادي والتنمية ، ووصولاً إلى الشراكات الإستراتيجية بين القطاعين العام والخاص.و لم نغفل في ذلك عن الجهود الداخلية في نفس المجال كما تكشف الدراسة نقاط الضعف في هذه الجهود كتقييم من اجل استدراك النقائص بهدف تقوية جدار التصدي لهذه الجرائم و تناقش الدراسة أيضا التحديات التي تعترض هذه التعاونات، كاختلاف الأولويات الوطنية، والثغرات التقنية، وإشكالية السيادة الرقمية، مقترحةً في النهاية رؤى لتطوير آليات أكثر فعالية لضمان فضاء سيبراني آمن يعزز التنمية العالمية المستدامة

ومن الأسباب الذاتية التي دفعتنا لاختيار هذا الموضوع:

هو الالتزام الأخلاقي حيث أؤمن بأهمية حماية الخصوصية الرقمية و حقوق الإنسان خاصة و أن اغلب سكان العالم حاليا يعتمدون على الأدوات الرقمية في حفظ معلوماتهم الحساسة إضافة لاهتمامي الشخصي بالموضوع باعتباره تحدي فكري لما فيه من تعقيدات و يتطلب فهما متعددا (سياسيا ,قانونيا ,تكنولوجيا) ما يجعل منه موضوعا جذابا للبحث كما انه موضوع يفتقر للبحث خاصة على مستوى الدراسات العربية كما انه لدي تطلع و رغبة في التخصص في مجالات مرموقة مثل : الأمن السبيراني أو القانون الرقمي و التي تعد من المهن الأكثر طلبا في سوق العمل حاليا .

أما عن الأسباب الموضوعية التي دفعتني للبحث في هذا المجال عامة و هذا الموضوع خاصة هو الانتشار السريع جدا للجريمة السبيرانية حيث يشهد العالم تزايد في الهجمات الالكترونية مثل : الاختراقات ,التصيد الاحتيالي ,برامج الفدية ...الخ و التي تهدد الأفراد و المؤسسات و الدول على حد سواء إضافة لارتفاع الخسائر المالية الناجمة عن هذه الجرائم و التي تقدر بملايير الدولارات سنويا وفق تقارير دولية رسمية .

كما أن من أهم الأسباب الموضوعية التي أثارت الموضوع هي الثغرات القانونية و التشريعية الخاصة بهذا النوع من الجريمة فاختلاف القوانين الوطنية بين الدول في تعريف الجريمة السيبرانية و إجراءات الملاحقة القضائية هو من ابرز الأمثلة على الفراغات التشريعية بين دولة و أخرى و التي أدت إلى تفشي هذه الجريمة على المستوى الدولي . إضافة إلى أن تهديد هذه الجريمة للأمن القومي و الاستقرار العالمي من أكثر الأسباب التي تستدعي البحث المستمر في هذا المجال

و من أبرز الدراسات السابقة التي تم الاعتماد عليها هو كتاب حسين عبد الكريم يونس و الدكتور خليل يوسف الجندي بعنوان "الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الأسباب " و الذي كان سباقا في الربط بين العوامل النفسية و السلوك الإجرامي للمجرم الالكتروني كما تميز بلغته العلمية الواضحة و تبسيطه للمفاهيم التقنية و مواكبته للمستجدات و دليل ذلك تحليله للتقنيات الحديثة التي يتم استخدامها حاليا في الجرائم السيبرانية مثل :الذكاء الاصطناعي، العملات الرقمية كالبتكوين ...الخ، كما تميز هذا الكتاب برؤيته الشاملة التي تجمع بين التخصصات (القانون، علم الاجتماع، علم النفس، التكنولوجيا) و لم يقتصر على الجانب الأكاديمي فقط بل يقدم نصائح عملية للوقاية من هذه الجرائم و رسائل توعوية للجمهور .

بالإضافة إلى هذا الكتاب تم الاستفادة من اتفاقية المجلس الأوروبي (بودابست2001) و اتفاقية جامعة العربية (2010) المتعلقة بجرائم تقنية المعلومات إضافة لمذكرة الماجستير المعنونة " الجريمة المرتكبة عبر الانترنت " من إعداد يوسف صغير و التي بدورها كان لها الفضل الكبير في توجيه هذه الدراسة حيث ساعدت في تحديد مجال الدراسة و فهم الموضوع و ذلك لسعة و تعقيد موضوعنا و هذا ما جعل من الدراسة مركزة و مفيدة .

و من الصعوبات التي واجهتنا في هذا البحث هو عدم توفر بطاقات الدفع الالكترونية الدولية في الجزائر من أجل اقتناء بعض الكتب التي كانت ستثري هذه الدراسة كثيرا و تفتح فيها أفقا أوسع للبحث .

نقص في الكتب المحلية فبقدر ما تتوفر المقالات الحرة في هذا المجال بقدر ما تنقص الكتب الجزائرية وقد يعود سبب ذلك إلى نقص الاهتمام بالأمن السبيراني و التهيب منه كمجال جديد

وعدم الإدراك بمدى خطورة هذه الجرائم، إضافة لصعوبة الوصول إلى بعض المراجع عبر الانترنت لكثرة الروابط و التحديثات المستمرة .

ومجال الجهود الدولية في مكافحة الجرائم السبيرانية كغيره من المواضيع البحثية التقنية والمستجدة التي لا تخلو من التساؤلات والإشكاليات التي بدونها لا يستمر البحث العلمي ويتوقف. ومن الإشكاليات الواردة في هذا البحث:

الإشكالية الرئيسية:

- إلى أي حد وُفقت السياسة الدولية في مواجهة الجريمة السبيرانية ؟

الإشكاليات الفرعية:

- فيما تتمثل الجهود الدولية التي ساهمت في مواجهة الجريمة السبيرانية ؟
- وهل نجحت الجهود الدولية المبذولة في تحقيق الأمن السبيراني ؟

و المنهج المتبع في هذه الدراسة هو المنهج التحليلي الوصفي الذي يجنح أحيانا إلى المنهج المقارن فتم الاعتماد على المنهج التحليلي في عدة حالات منها تحليل نصوص في اتفاقيات دولية كاتفاقية المجلس الأوروبي المتعلقة بالجريمة الالكترونية و المعروفة باتفاقية بودابست 2001 و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات2010 .

و اعتمدنا على المنهج الوصفي في الكثير من الأجزاء في مذكرتنا منها وصف بعض الجرائم السبيرانية و أثرها على الأفراد و المجتمع و وخصصت في ذلك بعض الفئات منها (الأطفال و الضعفاء المستهدفين عبر شبكة الانترنت ...الخ) .

كما اعتمدنا المنهج المقارن في المقارنة بين (اتفاقية بودابست 2001 و اتفاقية الأمم المتحدة 2024) من عدة نواحي من آليات و أهداف و النطاق الجغرافي و كذا من ناحية مستوى حماية الخصوصية .

و من هذا المنطلق و من أجل الإجابة على الإشكالية السابقة ارتأينا إلى إتباع خطة تعكس اهتمامات هذه الدراسة وهي خطة ثنائية متكونة من فصلين وذلك للتسهيل على القارئ فهم الموضوع حيث وضعنا في الفصل الأول مبحثين تناولنا من خلالهما طبيعة الجهود المبذولة لمكافحة الجريمة السبيرانية سواء على المستوى الدولي من خلال (مؤتمرات، منظمات ،.....الخ) أو المستوى الإقليمي من خلال الاتفاقيات الإقليمية .

أما في الفصل الثاني تطرقنا إلى تقييم مدى نجاعة تلك الجهود و طرحنا سبل لتعزيزها سواء من الناحية القانونية و القضائية أو من الناحية الفنية بهدف تحقيق حماية أعلى مما هي عليه في الوقت الراهن .

وفي الأخير ننهي دراستنا عند الخاتمة التي وضعنا فيها إجاباتنا عن الإشكاليات المطروحة وذكرنا فيها أبرز النتائج التي توصلنا إليها في البحث .

الفصل الأول : طبيعة الجهود الدولية في مواجهة الجريمة السبيرانية

الفصل الأول : طبيعة الجهود الدولية في مواجهة الجريمة السبيرانية

تمهيد :

- إن التعاون الدولي في مواجهة الجرائم السبيرانية هو السبيل الوحيد لردع هذا النوع من الجرائم لما فيها من خطورة على الأفراد و المجتمعات و حتى الدول و لما تتميز به من طابع منظم و عابر للحدود الدولية، لذا فانه من الضروري تضافر الجهود الدولية و الإقليمية على حد سواء في سبيل التصدي لها، وقد تم في هذا السياق العديد من المبادرات من استحداث هيئات و منظمات و عقد مؤتمرات و اتفاقيات دولية و إقليمية كان لابد منها من أجل تحقيق هذا الهدف، وهذا ما سنتطرق له في هذا الفصل حيث سنخصص المبحث الأول منه للجهود الدولية لمواجهة الجرائم السبيرانية و المبحث الثاني للجهود الإقليمية والوطنية المبذولة في نفس المجال .

المبحث الأول : الجهود الدولية في مواجهة الجرائم السبيرانية .

- سنتطرق في هذا المبحث إلى جهود التي الأمم متحدة كمطلب أول و من ثم إلى بعض المنظمات الدولية كمنظمة التعاون الاقتصادي و التنمية و المنظمة العالمية للملكية الفكرية كمطلب ثاني .

المطلب الأول : جهود الأمم المتحدة في مواجهة الجريمة السيبرانية

– لاشك أن لهيئة الأمم المتحدة الدور البارز و الفعال على المستوى العالمي في مكافحة الجريمة بشتى أنواعها و يشمل ذلك الجرائم السبيرانية حيث تعترف بتأثيرها الخطير على الأمن العالمي و التنمية بشتى فروعها خاصة الاقتصادية للدول كون أن هذا النوع من الجرائم غالبا ما يستهدف الأساس الاقتصادي للدول[1] ,إضافة للطبيعة العابرة للحدود لها فالجرائم السبيرانية لا تعترف لا بسيادة الدول ولا بالحدود الجغرافية بينها مثلها مثل جرائم تبييض الأموال و الاتجار بالمخدرات [2] ففي العصر الحديث يمكن ربط أعداد هائلة من الحواسيب عبر العالم ببعضها ما جعل غالبا الجاني و المجني عليه في دول مختلفة إضافة لإمكانية إلحاق الضرر بدول أخرى ثالثة .

إن هذه الخصوصيات التي تتصف بها الج س هي التي جعلت من مواجهتها مهمة صعبة أمام المجتمع الدولي ما يتطلب تكاتف و تعاون دوليين من اجل الوقوف في وجه المجرمين السبيرانيين[3].

ومن أبرز الجهود التي تبذلها هيئة الأمم المتحدة في هذا المجال :

الفرع الأول : المؤتمرات الدولية الأممية :

–يتم عقد مؤتمرات بالأمم المتحدة لمنع الجريمة و معاملة المجرمين كل خمس سنوات منذ عام 1955، حيث تُناقش تحديات الجريمة الحديثة، بما في ذلك الجرائم الإلكترونية [4].

---

[1] عادل عبد الصادق ,الارهاب الالكتروني و القوة في العلاقات الدولية نمط جديد و تحديات مختلفة ,مطبوعات مركز الدراسات السياسية و الاستراتيجية ,القاهرة ,الطبعة الأولى ,2009 ,ص330 .

[2] الموقع الرسمي لوزارة البريد و المواصلات السلكية و اللاسلكية , https://fs.mpt.gov.dz/cybercriminalite/ ,تاريخ الاطلاع 16 ماي 2025 ,ساعة الاطلاع 17:14 .

[3] علي قويدري ,أمال العايش ,الجريمة السبرانية مفهومها و سبل الوقاية منها ,مجلة نوميروس الأكاديمية ,جامعة عمار الثليجي ,الأغواط ,مجلد03 ,العدد 01 ,2022 ,ص192 .

[4] The official website of the **United Nations for the Prevention of crime and the treatment of criminals** , https://www.unodc.org/congress/ar/previous-congresses.html , date of Access: May 16, 2025, hour of access :16:29 .

في هذا العنصر سنتطرق أولا إلى المؤتمرين الثاني عشر و الثالث عشر إضافة للمؤتمر الثامن للأمم المتحدة بهافانا 1990 و المؤتمر السابع لها المتعلق بمنع الجريمة و معاملة المجرمين على سبيل المثال لا الحصر ثم إلى الاتفاقيات و الإعلانات التي أصدرتها وصولا إلى المعوقات التي تواجهها الأمم المتحدة في نفس المجال.

أولا : المؤتمر السابع للأمم المتحدة بميلانو (1985م):

و الذي انعقد في ايطاليا و بالضبط في ميلانو خلال الفترة الممتدة بين 26 أوت إلى 06 سبتمبر 1985م ,وحينها كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية و الاعتداء على الحاسب الآلي و عادا تقرير قصد عرضه على المؤتمر الثامن [1]

ثانيا : المؤتمر الثامن للأمم المتحدة بهافانا (1990م) :

- تم الوصول في هذا المؤتمر إلى إصدار قانون خاص بالجرائم المتعلقة بالحاسوب، و أشار إلى عدة إجراءات على الدول الأعضاء اتخاذها مثل :(تحديث القوانين و أغراضها الجنائية، اتخاذ تدابير الأمن مع حفظ حرمة الأفراد و خصوصياتهم تحت مسمى حقوق الإنسان، رفع الوعي بمدى خطورة الجريمة الالكترونية، التعاون مع المنظمات و كافة الهياكل المهتمة بهذا الموضوع، حفظ وحماية مصالح الدولة و حقوق الضحايا المتضررين من هذه الجرائم).

تم كذلك في هذا المؤتمر الحديث على وجوب تطبيق التطورات التكنولوجية في كافة مناحي حياة الأفراد مع التنبؤ بظهور أنماط جديدة للجريمة إزاء هذا التطور التكنولوجي لذا تم إثارة موضوع احترام خصوصية و حرمة الأشخاص خلال عمليات التحقيق في هذا النوع من الجرائم لأنها تشكل انتهاك لحقوق الإنسان و اعتداء على حرمة حياته الخاصة و أكد على وجوب اعتماد ضمانات ملائمة لصون السرية [2]

و هذا أيضا ما نصت عليه توصيات المؤتمر التاسع للأمم المتحدة الذي تم عقده في القاهرة 1990.

---

[1] سعيداني نعيم,آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ,مذكرة ماجستير ,كلية الحقوق و العلوم السياسية ,قسم الحقوق ,جامعة الحاج لخضر ,باتنة 2013/2012 ,ص83 .

[2] قطاف سليمان ,بوقرين عبد الحليم ,مواجهة الجرائم السبيرانية في ضوء الاتفاقيات الدولية ,مجلة البحوث القانونية و الاقتصادية ,جامعة عمار ثليجي , الاغواط , المجلد 05 , العدد 02 ,2022 , ص74

ثالثا :المؤتمر الثاني عشر (2010) :

حيث تم عقد هذا المؤتمر بسلفادور – البرازيل – في الفترة الممتدة بين 12 و 19 أفريل 2010وقد ركزت المناقشات خلاله على الجريمة السيبرانية كأحد التهديدات الناشئة، لاسيما أن منظمة الأمم المتحدة تعد الإطار الأمثل لمكافحة الإجرام السبيراني، وقد وضعت مجموعة من القواعد الموضوعية و الإجرائية لمواجهة هذا النوع من الجرائم [1] ، ودعت إلى تعزيز التعاون الدولي لمواجهتها و ذلك من خلال مجموعة من الإجراءات مثل:

- إتباع نهج شامل لإصلاح أنظمة العدالة الجنائية لتعزيز قدراتها في مواجهة الأشكال الحديثة للإجرام مثل القرصنة الالكترونية و الاحتيال الرقمي .
- إدماج العدالة في التنمية : فقد أبرز المؤتمر الحاجة إلى ربط إصلاح العدالة الجنائية بأهداف التنمية المستدامة، مع التركيز على حماية المستضعفين من الاستغلال عبر الانترنت.
- دعوة المجتمع الدولي و القطاع الخاص بتبادل المعلومات بشأن التشريعات الوطنية، و المساعدة التقنية .

و تأكيدا منها في هذا المؤتمر جاء البند 41 من تقريره، بحث الدول على بناء قدرات سلطاتها الوطنية من اجل التعامل مع الجرائم الالكترونية، بما في ذلك المنع و الكشف و التحقيق و ملاحقة هذه الجريمة بكافة أشكالها و تعزيز الأمن في شبكات الكمبيوتر [2]

رابعا: في المؤتمر الثالث عشر (2015) :

حيث تم عقد هذا المؤتمر بالدوحة– قطر– في الفترة الممتدة بين 12 و 19 أفريل 2015 فتم خلال المؤتمر مناقشة آليات دمج مكافحة الجريمة السبيرانية بين الاستراتيجيات الوطنية و الدولية لمواجهة التهديدات الرقمية ,تمت خلالها مناقشة قضايا سرقة الهويات والجرائم المالية الإلكترونية كنموذج، مع التأكيد على أهمية التقنيات المبتكرة للتحقيق في هذه الجرائم [3] .

---

[1] مراد مشوش ,الجهود الدولية لمكافحة الاجرام السبيراني ,مجلة الواحات للبحوث و الدراسات ,جامعة غرداية ,المجلد 12 ,العدد 2 ,2019 ,ص 707 .

[2] بيدي أمال ,المرجع السابق ,ص309

[3] The official website of the **United Nations** , https://www.un.org/ar/conferences , date of Access: May 16, 2025, hour of access :17:43 .

وقد حث المؤتمر على تطوير و تعزيز التكتل الدولي على المستوى التقني خاصة الدول النامية لغرض تطوير التحقيق الرقمي و التشريعات محلية متماشية مع المقاييس الدولية .

ومن أهم التوصيات التي أقرها المؤتمر في مجال مكافحة الجريمة السيبرانية مايلي:

1. وجوب استحداث أدوات و برامج من اجل تسهيل مكافحة ج س و منعها، حيث أن هذا النوع من الجرائم يتطلب من الدول تنمي قدرتها في جانب تدابير المنع و التحري المضادة .

2. بناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية في مجال التحري عن الجرائم السيبرانية والتحقق فيها، وعمليات الاستدلال الجنائي الرقمية، وكيفية التعامل مع الأدلة الإلكترونية [1].

3.وجوب استحداث أدوات وبرامج من أجل تسهيل مكافحة الجريمة السيبرانية ومنعها، حيث أن هذا النوع من الجرائم يتطلب من الدول أن تنمي قدرتها في جانب تدابير المنع والتحري المضادة.

4.إمكانية استحداث أطر متعددة الأطراف، حيث أوصى اجتماع أفريقيا الإقليمي التحضيري للمؤتمر الثالث عشر بأن تنظر الدول في وضع اتفاقية بشأن الجريمة السيبرانية ضمن سياق المؤتمر.

5. إمكانية استحداث اطر متعددة الأطراف، حيث أوصى اجتماع إفريقيا الإقليمي التحضيري للمؤتمر الثالث عشر بان تنظر الدول في وضع اتفاقية بشان الجرائم السبيرانية ضمن سياق المؤتمر .

6. الواضح أن الكثير من أجهزة إنفاذ القانون تواجه صعوبات في إمكانية الوصول إلى البيانات الموجودة خارج نطاق إقليمها أثناء التحري عن الجرائم السبيرانية، وفي المقابل لابد من أن تكون ضمانات حقوق الإنسان وسيادة القانون وصون الحرمة الشخصية كافية لضمان أن يكون ذلك الوصول إلى البيانات من أجهزة إنفاذ القانون محددا وقابلا للتنبؤ ومتناسبا وخاضعا للرقابة .

7. التأكيد على أهمية إشراك القطاع الخاص في مجال مكافحة الجريمة السبيرانية .[2]

[1] بيدي أمال ,المرجع السابق,ص309.
[2] بيدي أمال, نفس المرجع و الصفحة .

الفرع الثاني : الاتفاقيات والإعلانات الدولية :

أولا: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود (2000م):

– تُعتبر هذه الاتفاقية إطارًا رئيسيًا لمكافحة الجرائم العابرة للحدود على العموم ، بما في ذلك الجرائم الإلكترونية المرتبطة بالجريمة المنظمة، حيث تعتبر كذلك (عابرة للحدود) لان الأثر الإجرامي فيها يمكن أن يكون في دولة أخرى غير دولة الجاني و قد تتضرر منه دول أخرى غير دولة الجاني و المجني عليه .

- تنص المادة –6– على تجريم غسل الأموال الناتجة عن الجرائم، وهو أمر مرتبط بالجرائم المالية الإلكترونية .

كما نصت أيضا هذه الاتفاقية على أهمية التعاون الدولي من خلال آليات التعاون القضائي بين الدول من خلال تطوير أدوات قانونية تلائم طبيعة الجرائم الإلكترونية المعقدة، والتي تتجاوز الحدود الجغرافية بسرعة و التدريب على صياغة التشريعات المحلية المتوافقة مع المعايير الدولية مثل : تبادل المعلومات و المساعدة في التحقيقات و التي تستخدم اليوم في ملاحقة شبكات الجريمة المنظمة العاملة في الفضاء الالكتروني و تدعيم الدول النامية من خلال بناء القدرات كالتدريب على التحقيق الرقمي و تقنياته .

ثانيا :اتفاقية 2024 لمكافحة الجريمة السبيرانية :

حيث تعد هذه المعاهدة هي أول معاهدة أممية متخصصة في مجال الإجرام السبيراني وقد اعتمدتها الجمعية العامة للأمم المتحدة في ديسمبر 2024 كمعاهدة ملزمة قانونا تهدف لمواجهة الجرام السبيرانية مثل : الاعتداءات الجنسية عبر الانترنت ضد الأطفال , الاحتيال الالكتروني ,مع تعزيز الدعم الفني للدول النامية . كما تنص الاتفاقية على إنشاء لجنة متابعة و بروتوكولات مكملة ,مع فتح باب التوقيع عليها سنة2025 و ستدخل حيز التنفيذ مباشرة بعد 90 يوم بعد توقيع أربعون دولة عليها حيث ركزت الاتفاقية على 3 أهداف وهي:

– تحسين طرق منع الجرائم الالكترونية و مواجهتها – تعزيز التعاون الدولي لمكافحة الجرائم الالكترونية

-توفير المساعدة الفنية و بناء القدرات لاسيما البلدان النامية [1]

وقد أدلى خلالها فيليمون يانغ رئيس الجمعية العامة للأمم المتحدة عن رؤيته حيث قال"نعيش جميعا في عالم رقمي ,ولدى تكنولوجيا المعلومات و الاتصالات قدرة كبيرة على دعم التنمية في المجتمعات، إلا أنها تحمل أيضا تهديدا متزايدا من الجرائم السبيرانية .ومن خلال اعتماد هذه المعاهدة ,اتفقت الدول الأعضاء على الأدوات و الآليات اللازمة لتعزيز التعاون الدولي و منع و مكافحة الجرام السبيرانية و حماية الأشخاص و حقوقهم في المجال الرقمي "[2]

-جاءت هذه الاتفاقية بآليات جديدة تتمثل في :

- إنشاء (لجنة متابعة) للإشراف على تنفيذ الاتفاقية .
- تسهيل تبادل الأدلة الإلكترونية بين الدول الأعضاء، مع ضمان حماية حقوق الإنسان وفق النص .

ثالثا :إعلان فيينا (2000م) :

- لقد تم إصدار اعلان فيينا 2000 في سياق مكافحة الجريمة العابرة للحدود و في المؤتمر الـ10 الذي تعقده الأمم المتحدة لمنع الجريمة و معاملة المجرمين المنعقد خلال الفترة الممتدة بين 10 و 17 نيسان أفريل 2000 و قد تم إصدار هذا الإعلان بهدف اتخاذ تدابير منسقة دوليا و ذات فعالية أكثر في مجال مكافحة الجرائم المتعلقة بالحواسيب [3] ووضع توصيات لتحسين القدرات التقنية للدول في التحقيق في الجرائم الالكترونية وملاحقتها مع التركيز في كل مرة على التعاون الدولي .

- رغم الجهود المبذولة في هذا المجال على المستوى الدولي على العموم و على مستوى الأمم المتحدة على الخصوص إلا أن (هناك الكثير من المعوقات التي تحول الأمم المتحدة دون تحقيق مكافحة ناجعة حيال الجريمة السيبرانية، ويعود ذلك لعدة عوامل منها ما يتعلق بالجريمة المعلوماتية في حد ذاتها، أو ما يتعلق بالمجني عليه، أو

[1] ميتيهان دورماز ,اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم الالكترونية: الأهداف و الثغرات الموقع الرسمي لمنصة دعم السلامة الرقمية, https://smex.org/ar ,تاريخ الاطلاع :10 أفريل 2025 ,الساعة : 14:19

[2] الأمم المتحدة ,تقرير الجمعية العامة للأمم المتحدة بخصوص اتفاقية تاريخية لمكافحة الجريمة السبيرانية ,الجمعية العامة للأمم المتحدة,نيويورك,25ديسمبر2024 .

[3] اعلان فيينا (2000م) بشأن الجريمة والعدالة ومواجهة تحديات القرن الحادي والعشرين.

ضعف التنسيق و التعاون الدولي في هذا المجال وهناك ما يتعلق بعملية التحقيق الجنائي و الجهات التحقيقية)[1] وهذا ما سنتطرق إليه في الفصل الثاني من دراستنا على وجه التفصيل .

في الختام، تعمل الأمم المتحدة على تكييف أدواتها لمواكبة التعقيدات المتزايدة للجريمة السيبرانية، مع التركيز على التعاون الدولي وبناء القدرات المحلية.

المطلب الثاني : المنظمات الدولية الفاعلة في مجال مواجهة الإجرام السيبيراني

- لقد كان و لا يزال للمنظمات الدولية الدور الكبير في مواجهة الجرائم السبيرانية ذلك أنها في كل مرة تغلق ثغرة من الثغرات التي يسلكها المجرم السبيراني في أعماله .وذلك من خلال تحقيق الردع سواء بواسطة القوانين أو العقوبات التي تقررها على الأفعال المصنفة على أنها جرائم الكترونية.
- و في الواقع بادرت العديد من المنظمات الدولية الكبرى في مواجهة هذا النمط من الجريمة من منظمات تقنية و تشريعية الى منظمات أمنية و غيرها ...الخ ,مثل: الأنتربول [2](INTERPOL), الاتحاد الدولي للاتصالات (ITU)، منظمة التعاون الاقتصادي و التنمية(OECD) المنظمة العالمية للملكية الفكرية (WIPO) . في هذا المطلب سنأخذ منظمة التعاون الاقتصادي و التنمية (الفرع الأول) والمنظمة العالمية للملكية الفكرية (WIPO) (الفرع الثاني)كمثال فقط على المنظمات الدولية الفاعلة في هذا المجال و هذا لا يمنع أن هناك منظمات أخرى فاعلة غير التي ذكرتها سابقا .

[1] عصام حسني الاطرش ,محمد محي الدين عساف ,معوقات مكافحة الجريمة المعلوماتية في الضفة الغربية من وجهة نظر العاملين في اقسام الجرائم المعلوماتية في الأجهزة الأمنية ,مجلة جامعة الشارقة للعلوم القانونية ,جامعة الشارقة ,المجلد 16 ,العدد 9 ,2019 , ص637 .

[2] المنظمة الدولية للشرطة الجنائية (انتربول) هي منظمة حكومية دولية خاضعة للقانون الدولي ولديها هدفان هما ربط أجهزة الشرطة ومنع ومحاربة الجريمة وتعد أكبر منظمة دولية في العالم حيث تضم 195 من البلدان الأعضاء, راجع https://www.moi.gov.sa/!

الفرع الأول: منظمة التعاون الاقتصادي و التنمية (OECD) :

- هي منظمة اقتصادية حكومية دولية تضم 35 دولة عضو، تأسست عام 1961 لتحفيز التقدم الاقتصادي والتجارة العالمية."[1] من خلال العمل على تحقيق أعلى مستويات النمو الاقتصادي، بدأت هذه المنظمة الاهتمام بالجرائم المرتكبة عبر الانترنت منذ عام 1978،حيث وضعت مجموعة أدلة وقواعد إرشادية تتصل بتقنية المعلومات ، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام1980مع التوصية للأعضاء بالالتزام بها [2]
- أصدرت هذه المنظمة تقرير1983، بعنوان الجرائم المرتبطة بالحاسوب و تحليل السياسات الجنائية، وتضمن التقرير الحد الأدنى لأفعال سوء استخدام الحاسوب التي يجب على الدول أن تجرمها وتفرض لها عقوبات في قوانينها، ومن أمثلة هذه الأفعال:
- الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به، ويشمل ذلك الحاسب والمعلومات المخزنة داخله، الإفشاء غير المصرح به للمعلومات المعالجة أليا و النسخ إتلاف أو تخريب ما يحويه من بيانات وبرامج و الإعاقة غير المشروعة للوصول إلى مصادر المخزنة في قواعد الحاسب .[3]

[1] الموقع الرسمي لمنظمة التعاون الاقتصادي و التنمية الدولية , https://www.ccacoalition.org/ar/partners/organisation-economic-co-operation-and-development-oecd ,تاريخ الاطلاع 04 ماي 2025 , ساعة الاطلاع : 20:24 .

[2] غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية (الحاسب و الانترنت) ,اطروحة أعدت لنيل درجة الدكتوراه في القانون ,الجامعة الاسلامية في لبنان ,كلية الحقوق ,2004 ,ص 179 .

[3] غازي عبد الرحمن هيان الرشيد، المرجع نفسه ,ص 179 -180 .

الفرع الثاني :المنظمة العالمية للملكية الفكرية (WIPO):

- تعد المنظمة العالمية للملكية الفكرية، إحدى الوكالات التابعة للأمم المتحدة، وقد اهتمت هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم، بهدف دعم و تشجيع الابتكار، وتطوير الأدوات الإدارية التي تختص بحماية الملكية الصناعية، المصنفات الأدبية و الفنية .
- وقد " انتقل الاهتمام بحقوق الملكية الفكرية من المرحلة المحلية لكل دولة إلى
- مرحلة العالمية، فلقد تعددت الاتفاقيات التي نظمت حقوق الملكية الفكرية عموما
- وبراءة الاختراع بصفة خاصة بداية من اتفاقية"برن " [1] انتقالا إلى اتفاقية المنظمة العالمية للملكية الفكرية(WIPO)، وأخيرا اتفاقية "التربس"[2] "[3]
- اهتمت هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية و قواعد البيانات، فبعد ان استقر الرأي لديها بعدم إمكانية توفير الحماية لهما في تشريعات براءات الاختراع، تم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية و خاصة " التريبس " و "برن " اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها ,وخاصة تشريعات حق المؤلف [4]، وكذلك وضع عقوبات

[1] اتفاقية برن لحماية المصنفات الادبية و الفنية : تتناول اتفاقية برن، التي اعتمدت سنة 1886، حماية المصنفات وحقوق مؤلفيها .وتتيح الاتفاقية للمبدعين، مثل المؤلفين والموسيقيين والشعراء والرسامين وما إلى ذلك، سبل التحكم في طريقة استخدام مصنفاتهم ومن يستخدمها وبأية شروط. وتستند الاتفاقية إلى ثلاثة مبادئ أساسية وتشمل مجموعة من الأحكام المتعلقة بالحد الأدنى للحماية الواجب منحها وبعض الأحكام الخاصة التي وضعت لمصلحة البلدان النامية التي ترغب في استخدامها,الموقع الرسمي للمنظمة العالمية للملكية الفكرية(WIPO) , https://www.wipo.int/treaties/ar/ip/berne/index.html ,تاريخ الاطلاع :05 ماي2025 ,ساعة الاطلاع :15:24 .

[2] اتفاقية تريبس : هي اتفاقية دولية تقوم عليها منظمة التجارة العالمية(WTO) ، والتي تحدد المعايير الدنيا للقوانين المتعلقة بالعديد من أشكال الملكية الفكرية كما تنطبق على أعضاء منظمة التجارة العالمية .على وجه التحديد، يحتوي اتفاق تريبس على الشروط التي يجب توافرها في قوانين الدول فيما يتعلق بحقوق المؤلف، بما في ذلك حقوق فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة؛ المؤشرات الجغرافية، بما في ذلك تسميات المنشأ؛ الرسوم والنماذج الصناعية؛ تصاميم الدوائر المتكاملة، براءات الاختراع، العلامات التجارية، والمعلومات السرية,ربحي محمد ,قراءة في اتفاقية تريبس (TRIPS) ,مجلة المعيار ,جامعة تيسمسيلت ,المجلد 13 ,العدد01, 2022 ,ص552 .

[3] عمر محمد حماد ,الاحتكار و المنافسة غير المشروعة ,دار النهضة العربية ,2009 ,ص288 ,مشار اليه في : أسماء فيلالي ,حقوق الملكية الفكرية للمصنفات المعلوماتية ,مجلة افاق علمية ,جامعة تلمسان ,المجلد 14 ,العدد 01 ,2022 ,ص615 .

[4] غازي عبد الرحمن هيان الرشيد، المرجع السابق ,ص181 .

على كل أعمال تزوير في العلامات التجارية و القرصنة المتعمدة و المرتكبة في إطار تجاري ,وبالطبع يعتبر الانترنت من الأماكن الخصبة لهذا النوع من التصرفات[1]،والتي وفرت بموجبها الحماية القانونية للبرامج و قواعد البيانات المعلوماتية

تنص المادة الرابعة من معاهدة هذه المنظمة(1996) على أنه :

«تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية في معنى المادة الثانية من اتفاقية برن ,وتطبيق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها »

و تنص المادة الخامسة على أنه : «تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات بسبب اختيار محتوياتها أو ترتيبها ».

ساد الاتجاه لدى أغلب الدول الصناعية ودول العالم الثالث إلى الميل إلى خضوع برامج الحاسب الآلي لقوانين حماية حق المؤلف ,حيث عدلت معظم الدول تشريعاتها الخاصة بحق المؤلف و أضافت برامج الحاسب إلى المصنفات الأدبية المحمية وفقا للقانون ,وذلك نتيجة لاستمرار لجان الخبراء في دراسة الأسلوب المناسب لحماية برامج الحاسب الآلي و مسائلتها الفنية عبر الاجتماعات المتكررة و بالتعاون ما بين الويبو و اليونسكو [2].

[1] جون فرنسوا هنروت، « أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصرالشرطة والتعاون القضائي» ، أعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر ,المملكة المغربية ,19-20 يونيو 2007 مشار اليه في يوسف صغير ,الجريمة المرتكبة عبر الانترنت ,مذكرة ماجستير حقوق ,جامعة مولود معمري تيزي وزو ,2013 ,ص98 .

[2] محمود احمد عبابنة ,جرائم الحاسوب و ابعادها الدولية ,دار الثقافة للنشر و التوزيع ,عمان ,2005 ,ص 161 مشار اليه في يوسف صغير ,الجريمة المرتكبة عبر الانترنت ,مذكرة ماجستير حقوق ,جامعة مولود معمري تيزي وزو ,2013 ,ص99 .

المبحث الثاني : الجهود الإقليمية و الوطنية في مواجهة الجرائم السبيرانية .

- ان الجهود الإقليمية و الوطنية في مجال مكافحة الجرائم السبيرانية لا تقل أهمية عن التعاون الدولي للتصدي لها حيث تبدأ الخطوات الأولى من القوانين الداخلية للدول ثم إلى الاتفاقيات الإقليمية و الدولية أو العكس .

في هذا المبحث سنختص في المطلب الأول بالجهود الإقليمية المبذولة في مجال مكافحة الإجرام السبيراني من ادنى الجرائم إلى اعقدها و أهم ما سنتطرق إليه هي اتفاقية بودابست 2001 التي لابد من ذكرها كلما جرى الحديث عن مكافحة الإجرام الرقمي الذي يتمثل في الجرائم السبيرانية أساسا . إضافة لمبادرات أخرى في نفس المجال مثل: اتفاقية الجامعة العربية لمكافحة جرائم تقنية المعلومات (2010) و الجهود الإقليمية لا تنحصر فقط في الاتفاقيات بل سعت بعض الهيئات الإقليمية بجد للمساهمة في التصدي للج س و من ابرز تلك الهيئات : الاتحاد الأوروبي و المجلس الأوروبي. أما المطلب الثاني سنخصصه للجهود الوطنية و التعاون الوطني الدولي في هذا المجال .

المطلب الأول :الجهود الاقليمية في مواجهة الجرائم السبيرانية .

- إن الانتشار الواسع للجرائم السبيرانية هو الأمر الذي أدى إلى تحرك العديد من المنظمات الدولية و الإقليمية لإبرام اتفاقيات في خطورة تهدف إلى مكافحة الجريمة المعلوماتية، و لعل أهمها اتفاقية بودابست المنعقدة في 2001/11/23 تحت إشراف المجلس الأوروبي. [1] و هذا ما سنتطرق إليه في الفرع الأول من هذا المطلب .

الفرع الأول :الاتفاقية المتعلقة بالجريمة الإلكترونية لعام2001 (اتفاقية بودابست) :

جاءت هذه الاتفاقية نتيجة عدة محاولات منذ ثمانينيات القرن العشرين كما جاءت نتيجة مشاورات طويلة بين الحكومات و أجهزة الشرطة و قطاع الكمبيوتر و صاغ نصها عدد من

[1] فاروق خلف ,الاليات القانونية لمكافحة الجريمة المعلوماتية ,مجلة الحقوق و الحريات ,جامعة حمة لخضر ,الوادي ,المجلد 03 ,العدد 02 ,2015, ص 7 .

الخبراء في مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة " [1] و قد أبرمت من طرف المجلس الأوروبي [2] في العاصمة المجرية بودابست في سياق مكافحة الجريمة المعلوماتية و تعد الأولى في هذا المجال حيث شملت العديد من الجرائم التي تتم عبر الانترنت مثل : الاختراق غير القانوني، والاحتيال الإلكتروني، تزوير بطاقات الائتمان ,دعارة الأطفال وغيرها، كما تحدد إجراءات لجمع الأدلة الرقمية وحفظها .

–لقد كانت الاتفاقية في بادئ الأمر تقتصر على دول الاتحاد الأوروبي فقط إلا انه قد " تم توجيه الدعوة إلى الولايات المتحدة الأمريكية و اليابان و كندا و جنوب إفريقيا، لكي تشارك كل منها في إعداد هذه الاتفاقية بصفة مراقب، وذلك لكون الولايات المتحدة الأمريكية تحديدا ذات علاقة ومصلحة مباشرة بموضوع الجريمة عبر الانترنت ,أما مشاركة كل من اليابان و كندا و جنوب إفريقيا في إعداد هذه الاتفاقية، هو الأمر الذي يجعل الاتفاقية صالحة لكي تمتد إلى الدول الغير الأعضاء في الاتحاد الأوروبي "[3] وقد تم السماح للدول الغير أعضاء في الاتحاد الأوروبي الانضمام لهذه الاتفاقية بعد تقديم طلب عضوية و من الدول المنضمة لدينا المغرب سنة 2018 و تونس سنة 2024 حيث انضمت تونس رسميا إلى إتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية المعتمدة ببودابست، لتصبح الدولة رقم السبعين 70 التي تنضم إلى هذه الإتفاقية. ويأتي هذا الإنضمام في إطار مواصلة الجهود الوطنية والتنسيق المحكم بين مختلف الوزارات، من وزارة تكنولوجيات الاتصال وزارة الشؤون الخارجية ووزارة الداخلية ووزارة العدل وهياكل الدولة المختصة في مكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال وحماية الفضاء السيبراني الوطني ومستعملي تكنولوجيات المعلومات والاتصال من الاعتداءات والهجمات السيبرنية التي تهدف إلى النيل

---

[1] نسيمة درار (2017) ,الامن المعلوماتي و سبل مواجهة مخاطره في التعامل الالكتروني دراسة مقارنة .أطروحة دكتوراه ,جامعة ابي بكر بالقايد تلمسان – الجزائر ,كلية الحقوق و العلوم السياسية , ص273 .

[2] مجلس أوروبا المنظمة الرئيسة المعنية بالدفاع عن حقوق الإنسان في القارة الأوروبية. ويضم 47 دولة عضوا، منها 28 دولة عضو في الاتحاد الأوروبي. وقد وقعت جميع الدول الأعضاء في مجلس أوروبا على الاتفاقية الأوروبية لحقوق الإنسان، وهي معاهدة تهدف إلى حماية حقوق الإنسان والديمقراطية وسيادة القانون. موقع مجلس اوروبا في تونس , https://www.coe.int/ar-TN/web/tunis/the-coe ,تاريخ الاطلاع 26 افريل 2025 الساعة 14:20 .

[3] عمر محمد أبو بكر بن يونس ,الاتفاقية الاوروبية حول الجريمة الافتراضية ,مؤسسة ادم للنشر و التوزيع ,مالطا, الطبعة الثانية,2008 ,ص13 ,مشار اليه في : حسين عبد الكريم يونس ,خليل يوسف الجندي ,الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الاسباب ,دار كفاءة المعرفة للنشر و التوزيع ,عمان ,الطبعة الأولى ,2021 ,ص 106.

من أنظمة المعلومات أو المساس بحقوق الأشخاص أو استعمالها دون وجه حق أو المساس بالسلم الاجتماعي أو النظام العام[1]

– إن الأمر الذي يهمنا في دراسة هذه الاتفاقية هو الشق الموضوعي ألا وهو التجريم و مدى مواكبتها للتطور التكنولوجي المعاصر حيث تنص المادة 5 من اتفاقية بودابست بشأن مكافحة الإجرام المعلوماتي على انه :" يجب على كل طرف في الاتفاقية أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم تبعا لقانونه المحلي الإعاقة الخطيرة إذا تم ذلك عمدا و دون حق الوظيفة نظام الحاسب عن طريق إدخال، أو نقل، أو إضرار، أو محو، أو تعطيل، أو إتلاف أو طمس البيانات المعلوماتية "[2] و تم صياغة نص هذه الاتفاقية بطريقة طبيعية بحيث تشمل كافة الوظائف التي يمكن حمايتها بمقتضاه [3] .كما و تنص المادة 7 [4] من نفس الاتفاقية على نفس الأمر بتفصيل أكثر .

تقتضي الاتفاقية أن تكون بمثابة نقطة تلاقي (نقطة مشتركة) في تشريعات كل الدول الأعضاء بما فيها الدول الـ4 + الدول التي قبل طلب انضمامها طالما قبلت بالشروط المتعلقة بها المادة الـ48 من الاتفاقية [5] . كما وحددت الجرائم التي يجب أن تكون ضمن التشريعات الوطنية للدول الأعضاء ,حيث قسمت اتفاقية بودابست هذه الجرائم إلى أربعة أصناف تشمل :

---

[1] وزارة تكنولوجيات الاتصال التونسية ,انضمام تونس إلى إتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية المعتمدة ببودابست , https://www.mtc.gov.tn/index.php?id=119&L=1&tx_ttnews%5Btt_news%5D=4778&cHash=ea7685326b1108a66dcf1a335b5307d3 , تاريخ الاطلاع :26 أفريل 2025 ,الساعة : 12:58 .

[2] مادة 5 من اتفاقية المجلس الاوروبي المتعلقة بالجريمة الإلكترونية لعام 2001 .

[3] رشدي محمد علي محمد عيد علي ,الحماية الجنائية للمعلومات على شبكة الانترنت ,اطروحة دكتوراه ,مقدمة الى كلية الحقوق ,جامعة القاهرة ,2009, ص 167 ,وفيما يلي نص المادة الخامسة باللغة الانكليزية :

" Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law , when committed intentionally .the serious hindering without right of the functioning of a computer system by inputting ,transmitting ,damaging ,deleting ,deteriorating ,altering or suppressing computer data"

مشار اليه في حسين عبد الكريم يونس ,خليل يوسف الجندي ,الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الاسباب ,دار كفاءة المعرفة للنشر و التوزيع ,عمان ,الطبعة الأولى ,2021 ص 107

[4] مادة 7 من اتفاقية المجلس الاوروبي المتعلقة بالجريمة الإلكترونية لعام 2001 .

[5] مادة 48 من اتفاقية المجلس الاوروبي المتعلقة بالجريمة الإلكترونية لعام 2001 .

أ.جرائم تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر.

ب.جرائم متصلة بالكمبيوتر كالتزوير والاحتيال عبر الكمبيوتر.

ج.جرائم متعلقة بالمحتوى كالجرائم المتعلقة بالمواد الإباحية ضد القصر.

د.جرائم متعلقة بحقوق النشر والتأليف و الحقوق المجاورة. [1]

- اعتمدت الاتفاقية لغة تكنولوجية محايدة، لذا تصلح قواعدها الموضوعية الجنائية للتطبيق على كل من التكنولوجيا الحالية و المستقبلية .

اشترطت الاتفاقية العمدية في ارتكاب الجريمة السبيرانية، لذا لا يوجد مجال للارتكاب الغير عمدي فيشترط في الجرائم هذه القصد الجنائي الخاص إضافة للقصد الجنائي العام .كما أكدت على ضرورة تعاون سريع و فاعل .

مما سبق يتضح لنا أن الاتفاقية قد توزعت بنودها على ثلاثة محاور أساسية نختصرها في النقاط التالية :

- الانسجام بين التشريعات الوطنية، التي تجرم الأعمال غير القانونية في الفضاء السبيراني .
- تحديد وسائل التحقيق و الملاحقة الجزائية ,التي تنسجم مع الطبيعة العالمية للشبكة
- وضع نظام تعاون بين الدول ,يتصف بالسرعة و الفاعلية [2] .

[1] مهدي رضا , الجرائم السيبرانية و اليات مكافحتها في التشريع الجزائري ,مجلة ايليزا للبحوث و الدراسات ,جامعة محمد بوضياف ,المسيلة ,المجلد 06 , العدد 02 ,2021 ,ص 115 .

[2] منى الأشقر جبور , السيبرانية هاجس العصر , المركز العربي للبحوث القانونية و القضائية , ب.د.ن , ب. ب. ن ,2016,ص 105.

المقارنة بين الاتفاقيتين: بودابست 2001 والأممية 2024

الجانب	اتفاقية بودابست سنة 2001	اتفاقية الأمم المتحدة سنة 2024
النطاق الجغرافي	أوروبية مع انضمام دول أخرى	عالمية تحت مظلة الأمم المتحدة
الجرائم المعالجة	الجرائم التقليدية (مثل اختراق ,احتيال)	الجرائم المعقدة (مثل جرائم الاعتداءات الجنسية عبر الانترنت)
آليات التنفيذ	تعاون قضائي عبر الإنابات القضائية	تعامل مباشر مع مزودي الخدمات و تبادل الأدلة
حماية الخصوصية	محدودة الضمانات	تشدد على حقوق الإنسان مع التحفظات

الفرع الثاني :اتفاقية الجامعة العربية لمكافحة جرائم تقنية المعلومات (2010):

- لقد سَببَ رواج المعلومات في الدول العربية على غرار باقي دول العالم إلى ظهور سلوكات تكنولوجية إجرامية مما دفع بإقليم الدول العربية إلى التحرك من أجل التصدي لها من خلال سبل إجرائية و تشريعية مختلفة من أهمها اتفاقية الجامعة العربية لمكافحة جرائم تقنية المعلومات و هذا ما سنفصل فيه في هذا العنصر.

– تعتبر هذه الاتفاقية احد ابرز الجهود على مستوى الإقليم العربي في مجال مكافحة الإجرام السبيراني(وما أطلق عليه في هذه الاتفاقية بمصطلح جرائم تقنية المعلومات وهو النوع الذي تختص به) وهي اتفاقية إقليمية عربية أُقرت في 21 ديسمبر 2010 [1]خلال

[1] وردة شرف الدين ,التعاون القضائي و القانوني لمكافحة جريمة غسيل الأموال و المرتكبة بواسطة تقنية المعلومات وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 ,مجلة الباحث للدراسات الأكاديمية ,جامعة بسكرة ,المجلد 08 ,العدد 02 ,2021 ,ص 639 .

القمة الثانية والعشرين لمجلس جامعة الدول العربية، تؤكد في المادة الاولى منها أن الهدف من ابرامها – هذه الاتفاقية – هو "تعزيز التعاون و تدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية و مصالحها و سلامة مجتمعاتها و افرادها "[1] و يتحقق ذلك عبر توحيد السياسات الجنائية وتبني آليات مشتركة للتحقيق والمقاضاة. لذا تُعد هذه الاتفاقية إطارًا قانونيًا مهمًا لمواكبة التحديات الأمنية الناتجة عن التطور التكنولوجي .ويتم ذلك بين الدول المصادقة عليها على مستوى عدة مجالات مهمة في مواجهة الاجرام العابر للحدود بما فيه الجرمة السبيرانية مثل : مشاكل الاختصاص، تسليم المجرمين، المساعدة القضائية المتبادلة "الانابة القضائية"، كما يمكننا القول أن هذه الاتفاقية قد نجحت إلى حد بعيد في تحقيق مساعيها في مجال تدعيم التعاون الدولي بين أعضائها من الناحية النظرية، إلا أن نجاحها الفعلي مرتبط بتجسيد الاتفاقية بين الدول الأطراف فيها من خلال العمل على إدراج أحكامها الخاصة بالتجريم والإجراءات والتعاون القانوني والقضائي ضمن قوانينها الداخلية.

تم التوقيع عليها من طرف 14 دولة عربية كسوريا و الأردن كما صادقت عليها 9 دول لحد الساعة من بينهم الجزائر [2]و من ابرز محتويات هذه الاتفاقية :

- تحديد نطاق تطبيق أحكام هذه الاتفاقية حيث حددت المجال في المادة الـ3 منها على النحو التالي :

المادة الثالثة:مجالات تطبيق الاتفاقية:

جرائم تقنية المعلومات التي :

[1] مادة 1 من الاتفاقية العربية لمكافحة جرائم المعلومات والتي اعتمدتها جامعة الدول العربية , 21 ديسمبر 2010 م

[2] قائمة الاتفاقيات القضائية المتعددة الأطراف المصادق عليها من طرف الجزائر ,الموقع الرسمي لوزارة العدل الجزائرية , https://www.mjustice.dz/ar/ ,تاريخ الاطلاع :16 ماي 2025 ,ساعة الاطلاع : 22:15 .

1-ارتكبت في أكثر من دولة.

2-ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.

3-ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.

4-ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى [1]

- خصصت الفصل الثاني منها (بالتجريم) للأفعال التي تعتبرها مجرمة و التي تلتزم كل دولة طرف بتجريمها وفق تشريعاتها و انظمتها الداخلية و تتمثل تلك الافعال المجرمة في :

1-الدخول غير المشروع : الدخول أو البقاء في أنظمة تقنية المعلومات دون إذن، خاصة إذا تسبب في تدمير البيانات أو الوصول إلى معلومات سرية .

2- الاعتراض غير المشروع : قطع أو اعتراض نقل البيانات عبر الشبكات .

3- لتزوير والاحتيال الإلكتروني : تغيير البيانات أو تعطيل الأنظمة لتحقيق منفعة غير مشروعة .

4- جرائم الإباحية : خاصة تلك المتعلقة بالأطفال، مع تشديد العقوبات في هذه الحالات[2] .

5- جرائم الإرهاب الإلكتروني: مثل نشر أفكار إرهابية أو تمويل العمليات الإرهابية عبر الإنترنت .

[1] مادة 3 من الاتفاقية العربية لمكافحة جرائم المعلومات والتي اعتمدتها جامعة الدول العربية , 21 ديسمبر 2010 م

[2] ميرفت محمد حباية ,مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري و الفلسطيني ,دار اليازوري العلمية ,عمان,الطبعة الأولى,2023,ص271.

6-الجرائم المنظمة: كغسل الأموال والاتجار بالأشخاص أو المخدرات باستخدام التقنيات الرقمية .

7- انتهاك حقوق الملكية الفكرية: مثل توزيع البرامج المقرصنة .

حرصت الاتفاقية على احترام حقوق الإنسان أثناء تطبيقها، و رفضت أي تعاون قد يؤدي إلى انتهاكها .

- **المطلب الثاني : الجهود الوطنية و التعاون الوطني الدولي .**
- ان تحقيق الدول لسياسات إستراتيجية ناجعة ضد الج س من خلال تشريعاتها الداخلية هو ما تعمل عليه الجهود الدولية و تصل الليل بالنهار من اجل تحقيقه سعيا منها في تحقيق الأمن العالمي لمختلف القطاعات و حتى الأفراد من أي اختراق الكتروني ,و في هذا المطلب سنتطرق للجهود الوطنية بعد أن كنا قد فصلنا فيما يخص المبادرات المعتمدة على المستوى الإقليمي .
- **إستراتيجية الجزائر وتعاونها الدولي في مواجهة الجرائم السبيرانية :**
- ان الجزائر كغيرها من الدول أضحت إحدى ضحايا هذه المخاطر خاصة و ان موقعها الجغرافي الذي يعطيها انتماءا إفريقيا ,مغاربيا و متوسطيا جعل منها نقطة تلاقي مثالية بالنسبة للمجرمين السبيرانيين ,لذا كان لابد من وضع إستراتيجية تشريعية و تنظيمية للتصدي لهذا النمط من الجريمة.[1]

و من بين مظاهر التعاون الجزائري الدولي هو انخراطها في اتفاقيات دولية متخصصة ابرز تلك الاتفاقيات لدينا اتفاقية بودابست 2001 ,و في مجال الاتفاقيات الأممية " و على مدى ثلاث سنوات ,بذلت الرئاسة الجزائرية للجنة مباشرة بعد انتخابها في مايو 2021 جهودا لتقريب الآراء المتباينة لدول الأعضاء ,حيث عقدت اللجنة ثمان دورات مخصصة

[1] جمال بوازدية ,الاستراتيجية الجزائرية في مواجهة الجرائم السبيرانية "التحديات و الافاق المستقبلية ",مجلة العلوم القانونية و السياسية,جامعة الجزائر 3,المجلد 10 ,العدد 01 ,2019 ,ص 1263 .

للمفاوضات تخللتها مشاورات مكثفة قادتها الدبلوماسية الجزائرية وفريق عملها[1] في ظروف فائقة التعقيد مع أهم الفاعلين بما فيهم الولايات المتحدة و الصين و روسيا و الاتحاد الأوروبي و الهند و البرازيل وجنوب إفريقيا و غيرها من الدول الأعضاء [2].

كما عملت الجزائر على مطابقة قوانينها الداخلية تماشيا مع بنود الاتفاقيات الدولية التي صادقت عليها و اعتمدتها في هذا المجال [3].

– من هذا المنطلق تم استحداث قطب جزائي وطني سنة 2021 لمكافحة جرائم المتصلة بتكنولوجيا الإعلام و الاتصال

إضافة لاستحداث هيئات مختصة تعمل على التطبيق الصارم للتشريع الجزائري المتعلق بمكافحة الجرائم السبيرانية ."كما حرص المشرع الجزائري على وضع ضوابط لاحترام الإطار الإداري المنظم لصلاحيات الهيئات المدنية و العسكرية و التقنية في إدارة الإستراتيجية الجزائرية للأمن السبيراني " [4]و هذا بهدف تفادي تداخل الصلاحيات بين تلك الأجهزة

ومن أهم هذه الهيئات :

1–الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها

2–مصلحة الدفاع السبيراني ومراقبة امن الأنظمة .

3–المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني (SCLC).

[1] موقع الاذاعة الجزائرية ,اعتماد اتفاقية لمكافحة الجريمة السبيرانية .مكسب اخر في سجل جهود الدبلوماسية الجزائرية بقيادة رئيس الجمهورية , https://news.radioalgerie.dz/ar/node/50035 ,تاريخ الاطلاع :06 ماي 2025 ,ساعة الاطلاع : 13:50 .

[2] موقع الاذاعة الجزائرية ,اعتماد اتفاقية لمكافحة الجريمة السبيرانية ..مكسب اخر في سجل جهود الدبلوماسية الجزائرية بقيادة رئيس الجمهورية , https://news.radioalgerie.dz/ar/node/50035 ,تاريخ الاطلاع :06 ماي 2025 ,ساعة الاطلاع : 13:58 .

[3] بوضياف اسمهان ,الجريمة الالكترونية و الاجراءات التشريعية لمواجهتها في الجزائر ,مجلة الأستاذ البـــاحث للدراسات القـانونيـة و السيـاسـية,جامعة محمد بوضياف ,المسيلة ,العدد 11 ,2018 ,ص369 .

[4] آسيا عمراني ,التعاون الدولي في مواجهة الجرائم السبيرانية :الجزائر نموذجا ,مجلة الجزائرية للعلوم السياسية و العلاقات الدولية ,جامعة الجزائر 3 ,المجلد 3 ,العدد 2,ديسمبر 2010 ,ص72.

4-مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية التابعة للقيادة العامة للدرك الوطني (CPLCIC).

5-المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني التابع للقيادة العامة للدرك الوطني (INCC).

- لم تكتفي الجزائر فقط بإنشاء الهيئات سابقة الذكر بل تم إصدار القانون 09-04 المؤرخ في 5 أوت 2009المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها إضافة لاستحداث المشرع الجزائري قسم جديد في قانون العقوبات (في القسم الرابع مكرر من فصل 3) وهو قسم خاص بجرائم الجنايات و الجنح ضد الأموال بعنوان المساس بأنظمة المعالجة الآلية للمعطيات) [1] و الذي يتضمن 8 مواد (من المادة 394 مكرر إلى المادة 394 مكرر 7).

- تم أيضا عقد أيام دراسية أما من اجل التوعية بمخاطر هذا النمط من الإجرام أو بهدف تكوين الأطر من اجل التصدي الناجع له و نذكر على سبيل المثال :

-اليوم الدراسي بالمركز الجامعي عبد الحفيظ بوالصوف لولاية ميلة الذي تم في إطار متابعة تنفيذ برنامج التكوين المستمر على المستوى المحلي تم خلاله المداخلات التالية: المداخلة الأولى ألقيت من طرف السيد :شباح بوزيد أستاذ بالمركز الجامعي تحت عنوان " الإطار القانوني و خصوصية الجريمة الالكترونية." أما المداخلة الثانية ألقيت من طرف السيد: فردي سمير قاضي التحقيق بمحكمة فرجيوة تحت عنوان " إجراءات التفتيش و الحجز في المنظومة المعلوماتية." والمداخلة الثالثة ألقيت من طرف السيد : بلحربي

[1] تعديل قانون العقوبات الجزائري بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 22-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات .

عومار مدير معهد الحقوق تحت عنوان " آليات التعاون الدولي للوقاية من الجريمة الالكترونية و مكافحتها ".[1]

[1] يوم دراسي حول الجريمة الالكترونية, المركز الجامعي عبد الحفيظ بوالصوف, ميلة ,الموقع الرسمي لمجلس قضاء ميلة , https://courdemila.mjustice.dz/?p=actualite&p1=9 ,تاريخ الاطلاع 06 ماي 2025 ,ساعة الاطلاع : 11:59 .

- **خلاصة الفصل الأول :**

يستخلص من هذا الفصل أن أفراد المجتمع الدولي و خاصة الأمم المتحدة عملت المتحدة عملت بمختلف الآليات للتصدي للجريمة السبيرانية و مكافحتها حيث برزت جهودها عبر سلسلة من المؤتمرات أهمها مؤتمرا ميلانو 1985 و هافانا 1990 اللذان ناقشا تحديات هذه الجريمة ووضعا توصيات لتعزيز التشريعات و حماية البنى التحتية الرقمية ,إضافة لاتفاقيات دولية مثل اتفاقية 2024 لمكافحة الج س التي هدفت إلى تعزيز التعاون التقني و القضائي بين الدول خاصة في مجال تبادل الأدلة الرقمية . كما كان للمنظمات الدولية الدور البارز في مكافحة الج س مثل منظمتي الـ(WIPO) و (OECD) .

تطرقنا أيضا في هذا الفصل للجهود الإقليمية و الوطنية في هذا المجال حيث طرحنا أهمها على المستوى الإقليمي ممثل في اتفاقية بودابست 2001 و اتفاقية جامعة الدول العربية لمكافحة جرائم تقنية المعلومات .

أما على الصعيد الوطني فقد خطت الجزائر خطوات مهمة في هذا المجال من خلال تحديث تشريعاتها كالقانون 09-04 و إنشاء هيئات كالقطب الجزائي و الوطني لمكافحة الجرائم المعلوماتية.

الفصل الثاني:

الجهود الدولية في مواجهة الجريمة السبيرانية بين الواقع و المأمول .

تمهيد :

- على الرغم من الدور المهم الذي لعبته إحكام القانون الدولي, و خاصة الاتفاقيات و المعاهدات الدولية و المنظمات العالمية ,في مواجهة الجرائم السبيرانية العابرة للحدود ,إلا إن هذه الآليات لم تتمكن من صد كافة الهجمات الالكترونية المتزايدة التي يشهدها العالم خاصة و أن أساليب المجرمين السبيرانيين في تطور رهيب مما جعل فرق التطور بين الجرائم السبيرانية و إجراءات التصدي لها شاسعا جدا ,والدليل على ذلك الحروب السبيرانية بين الدول التي نشهدها في الوقت الحالي ما أكد لنا أهمية تطوير آليات الحماية الدولية و الإقليمية مواكبة للتطور الحالي في الجريمة السبيرانية ,في هذا الفصل سنحاول تحديد نقاط قصور الجهود الدولية المبذولة وواقع الأمن السبيراني الدولي وسنخصص لذلك المبحث الأول لهذا الفصل المعنون بـ(تقييم الجهود الدولية في مواجهة الجرائم السبيرانية)أما المبحث الثاني سنخصصه للحلول التي تسهم في تطوير قواعد الحماية وتحقيق المستوى المأمول للأمن العالمي سواءا للأفراد، المجتمعات والبنى التحتية للدول على حد سواء و سيكون المبحث بعنوان (سبل تعزيز الجهود الدولية في مواجهة الجرائم السبيرانية) .

المبحث الأول : تقييم الجهود الدولية في مواجهة الجرائم السبيرانية.

- إن الواقع الحالي يثبت انه و بالرغم من الجهود المبذولة على المستوى الدولي و الداخلي للدول لا تزال الأنظمة بحاجة لحماية أعلى من الهجمات السبيرانية خاصة تلك التي تستهدف المنشات الحيوية للدول مثل (المؤسسات المالية و العسكرية ....) وأكبر دليل على ذلك الهجوم الالكتروني الروسي على أوكرانيا في فيفري 2022[1] و الذي اثبت ضعف القدرة على محاسبة الدول عن الهجمات السبيرانية الخبيثة رغم كل ما تلحقه من ضرر بالدول، كما أن تزايد هذه السلوكيات هو ما أدى إلى ظهور مصطلح الحرب السبيرانية، "وعلى الرغم من أهمية التعاون الدولي و ضرورته للتصدي للجريمة الالكترونية إلا إن عدم فعاليته في الواقع العملي يرجع إلى أسباب عديدة"[2] أهمها : ضعف التنسيق بين أفراد المجتمع الدولي لمكافحة الج س ,بعض الصعوبات المتعلقة بالجريمة ذاتها أو المجني عليه، إضافة لمشاكل الإثبات و التحقيق في هذا النوع من الجرائم . و هذا ما سنفصل فيه في هذا المبحث .

المطلب الأول :ضعف التنسيق الدولي و صعوبات الإثبات و التحقيق في الجرائم السبيرانية .

تعد الجرائم السبيرانية تهديدا عابرا للحدود يتطلب تعاونا دوليا فعالا لمواجهته ,ومع ذلك يواجه المجتمع الدولي تحديات كبيرة في تحقيق التنسيق الكافي مما يضعف القدرة على مكافحة هذه الجرائم بشكل استباقي وفيما يلي أهم أسباب هذا الضعف و تداعياته وهو ضعف التنسيق الدولي (فرع01) و صعوبات الإثبات و التحقيق (فرع02).

---

[1] الحرب الإلكترونية العالمية الأولى , بخصوص الهجوم الاكتروني الروسي الأوكراني ,راجع الموقع :
https://lcss.gov.ly/articles/blog/post-212/ ,تاريخ الاطلاع :18 ماي 2025 ,ساعة الاطلاع :14:25 .

[2] رحيم محمد ,التحديات الجديدة للأمن الدولي التهديدات السبيرانية ,أطروحة دكتوراه في العلوم السياسية و العلاقات الدولية ,جامعة الجزائر 3,الجزائر,2024 ,ص 171 .

الفرع الأول : ضعف التنسيق بين أفراد المجتمع الدولي لمكافحة الجرائم السبيرانية :

في أجواء شبيهة بالحرب الباردة يتصارع اليوم الغرب بقيادة الولايات المتحدة و الشرق بقيادة روسيا و الصين على فرض رؤيتهما لكيفية صياغة قواعد و مبادئ النظام الدولي,و التي من شأنها تنظيم عملية التعامل مع التهديدات الجديدة في الفضاء السبيراني [1] و هذا احد الأمثلة الكثيرة جدا في المجتمع الدولي من حالة اللاتوافق بين أفراده حول رؤية موحدة لهذه السلوكيات التكنولوجية المجرمة و عدم الاتفاق كذلك على كيفيات التعامل معها .

- أدى هذا الصراع بين القوتين و التباين في الرؤى و الاستراتيجيات و كذلك المبادئ و الأهداف و حتى المفاهيم، إلى عدم الاتفاق حول الأمن السبيراني، خاصة و أن الولايات المتحدة الأمريكية متمسكة بالهيمنة السبيرانية بعد تدشين قيادة عسكرية للفضاء الالكتروني عام 2009[2] . و من هنا يظهر لنا أول الإشكاليات التي تسببت في قصور الجهود الدولية و التي أدت لاستفحال الجرائم السبيرانية إلا وهي عدم وجود نموذج موحد متفق عليه فيما يتعلق بالنشاط الإجرامي و يرجع ذلك إلى عدم اتفاق الدول و أنظمتها على صور محددة يندرج ضمنها بما يعرف بإساءة استخدام نظم المعلومات الواجب إتباعها هذا من جهة، ومن جهة أخرى عدم وجود تعريف محدد النشاط المفروض أن يتفق على تجريمه . و هذا لا يقتصر فقط على الو.م.أ و روسيا و الصين بل هذا هو واقع كافة المجتمع الدولي و لكل دولة أسبابها حيث أن العديد من الدول العربية لم تصدر قانونا يتعلق بالجريمة المعلوماتية سواء ارتكبت عن طريق الكمبيوتر أو عن طريق الإنترنت، و لا يزال الخلاف قائما حول أفضلية

[1] عز الدين قطوش ,الحرب الباردة الأمريكية – الروسية في الفضاء السبيراني ,مجلة مدارات سياسية ,جامعة الجزائر3 ,المجلد 07 ,العدد 02 ,2023 ,ص290 .

[2] عز الدين قطوش ,نفس المرجع و الصفحة .

تعديل التشريعات العقابية لكي تستوعب نماذج الجريمة المعلوماتية أم انه تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه الأنشطة من السلوك و يتم تجريمها، أم من الأفضل إصدار تشريعات جديدة خاصة بالجريمة المعلوماتية ،حتى أن الأمر لا يتوقف هنا بل يتعداه ، حيث أن عدم اتفاق الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على تنظيم أنفسهم و ارتكاب جرائمهم دون التقيد بالحدود الجغرافية الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة"[1].

و عدم الاتفاق العربي لحد الآن على إستراتيجية متكاملة البناء أدى لتطور أكثر في الجريمة السبيرانية حيث بينت الدراسات في مجال الجرائم الالكترونية بأن ظاهرة الهجمات الالكترونية تطورت و تنوعت ,من مجرمين عاديين ,و مجرمين الكترونيين الذي يتحركون بشكل منفرد إلى العصابات المنظمة و مجموعات الهاكرز [2]

كما استعرضت الدراسة تطور أنشطة الجرائم السبيرانية ,حيث أوضحت انه في منتصف التسعينات قد نشطت تهديدات تعرف بـ(الفيروسات و الديدان) و في منتصف القرن الماضي في عام 2004 انتشرت البرمجيات الربحية الخبيثة للتطور بعد ذلك و ترفع من مستوى أهدافها لتستهدف البنى التحتية للبيانات و سرقة الشهادات ....الخ و قد بدأ هذا النوع من التهديدات في الظهور تقريبا ابتداء من سنة 2013 .

ما يؤكد انه رغم كل الجهود المبذولة في هذا المجال لازالت قاصرة أمام هذا التطور في الجرائم السبيرانية .

[1] ليندة شرابشة , السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية ,مجلة دراسات و ابحاث ,جامعة الجلفة ,المجلد 01 ,العدد 01 ,2009, ص 250 .

[2] حسين عبد الكريم يونس ,خليل يوسف الجندي , المرجع السابق,ص 77 .

الفرع الثاني : مشاكل الإثبات و التحقيق في الجرائم السبيرانية .

أولا :المعوقات المتعلقة بالجهات التحقيقية (التحقيق) :

– تواجه عملية التحقيق في الجرائم الالكترونية تحديات متعددة ترتبط غالبا بالطبيعة الافتراضية للجريمة فعلى عكس الجرائم الواقعية (الجرائم التقليدية) التي تعرف بسهولة التحقيق فيها وواقعيته نظرا لواقعية الجريمة و لما فيها من أدلة مادية و تقنيات تقليدية فان طبيعة الأدلة الرقمية الهشة التي تتميز بسهولة التعديل و الحذف و زد على ذلك صعوبة فك تشفير البيانات للحصول على تلك الأدلة إضافة لصعوبة التوثيق الزمني حيث يعتبر تحديد التوقيت الدقيق للهجوم مهمة صعبة لما يتطلبه من تحليلات معقدة للسجلات الزمنية ,إضافة لاستعمال المجرمين السبيرانيين لتقنيات تقنية معقدة و متطورة و اعتمادهم على شبكات مظللة ما يزيد عملية التحقيق الرقمي صعوبة [1].

و أحيانا أخرى ترتبط صعوبات التحقيق بالجهات المعنية بالتحقيق، حيث تعود بعض هذه التحديات إلى عوامل شخصية تتعلق بالمحقق نفسه ,كالتحفظ النفسي و التهيب تجاه التعامل مع أجهزة الحاسوب و شبكة الانترنت، أو عدم مواكبة التطورات الحديثة في مجال مكافحة الجرائم الرقمية بينما في المقابل نجد أن مرتكبي هذه الجرائم يتابعون كل جديد و يعملون على تطوير سبل إخفاء أدلة جرائمهم فضلا عن ذلك إن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم و أساليب التفاهم معهم و ليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات و العبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات و هي لغة جديدة و متطورة و كذلك من أهم معوقات التحقيق تلك المتعلقة بأساليب المكافحة مثل عدم توفر الأجهزة و البرامج المناسبة للتحقيق و عدم التنسيق بين المحققين في هيئات التحقيق و العاملين في مجال المعلومات و الأنظمة الالكترونية و الحاسوب [2] لذا اعتبر عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الالكترونية،

[1] خالد عبد الحق ,دعاء عبد العال ,الجرائم الالكترونية و التحقيقات الجنائية ,دار اليازوري ,ب ب ن ,الطبعة الأولى ,2025 ,ص 234 .

[2] خالد عياد الحلبي (2011) إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت .دار الثقافة للنشر و التوزيع, الاردن, بدون طبعة . مشار اليه في : جاسم محمد جندل ,الجرائم الالكترونية ,دار المعتز للنشر و التوزيع , عمان ,الطبعة الاولى ,2022 ,ص192 .

أحد أهم المعوقات في مكافحتها و هذا ما أدى الى عدم وجود وحدة تحقيق أقسم خاص متفرغ للتحقيق في هذه الجرائم، مع ارتفاع تكاليف جمع الأدلة نظير المبالغ الكبيرة التي يطالب بها المختصين الخبراء مقابل ضبطهم و استخلاصهم الأدلة الرقمية [1].

و نجد أن كل ما تم ذكره سابقا غالبا ما يكون في الدول النامية و التي لازالت إلى الآن بحاجة إلى تطوير أكثر في النظام القانوني من جهة وفي الكفاءات والأطر المتخصصة في مكافحة هذه الجرائم من جهة أخرى .

ثانيا:المعوقات المتعلقة بصعوبات الإثبات :

– إن صعوبة إثبات الجريمة السبيرانية مقترن بخاصية صعوبة اكتشافها إذ لا يمكن نسبها إلى شخص معين بذاته و ذلك لاقتران عملية إثباتها بعدد من المعوقات منها :

أن هذه الجرائم لا تترك آثارا مادية كغيرها من الجرائم ذات الطابع التقليدي كالبصمات أو الأجهزة المحطمة نتيجة الاختراق ,فعلى سبيل المثال إعطاء دواء قاتل لمريض يمكن إثباته من خلال المعمل الجنائي بتحليل الأثر المتبقي من هذا الدواء في العبوة الحافظة له أو بتحليل السوائل الموجودة في معدة القتيل .[2]

لهذا فان صعوبة اكتشاف الدليل الالكتروني هو أول ما يجعل من عملية إثبات الجريمة السبيرانية مهمة صعبا جدا و غالبا ما يتم الفشل فيها لذا يرى بعض الباحثين ضرورة إعطاء الدليل الالكتروني دلالة قانونية قاطعة و يدعوا إلى اعتماده من قبل المحكمة كدليل كاف لإثبات الإدانة أو البراءة ,ولو جاء مفردا من غير أدلة أخرى تدعمه, و يبرر أصحاب هذا الرأي موقفهم بصعوبة استخلاص الأدلة في البيئة الرقمية من جهة, ونقص الكوادر المتخصصة, و انخفاض كفاءتها من جهة أخرى, فضلا على أن القول بخلاف ذلك يؤدي إلى إفلات الكثير من الجناة .[3]

[1] عصام حسني الأطرش ,محمد محي الدين عساف ,المرجع السابق ,ص 639 .

[2] طارق عفيفي صادق احمد ,الجرائم الالكترونية /جرائم الهاتف المحمول دراسة مقارنة بين القانون المصري و الاماراتي و النظام السعودي ,المركز القومي للاصدارات القانونية ,القاهرة ,الطبعة الاولى ,2015,ص 36 .

[3] يعيش تمام شوقي ,الجريمة المعلوماتية – دراسة تأصيلية مقارنة ,مطبعة الرمال ,الوادي ,الطبعة الأولى,2019 ,ص 53 .

المطلب الثاني : الصعوبات المتعلقة بالجريمة و المجني عليه .

تتجلى صعوبة مواجهة الجريمة السبيرانية المتعلقة بالجريمة ذاتها و المجني عليه في كون أن هذه الجريمة حديثة وقد لا تستوعبها القوانين التي تحكم الجرائم التقليدية على العموم أما فيما يخص الصعوبات المتعلقة بالمجني عليه يظهر إن نقص الوعي الأمني عند المجني عليهم هو ابرز تلك الأسباب وهذا ما سنتطرق ليه في الفرعين الأول والثاني على بطريقة مفصلة .

الفرع الأول : الصعوبات متعلقة بالجريمة السبيرانية

أولا –الشق الموضوعي : يتمثل في مدى إمكانية تطبيق النصوص التقليدية للقانون الجنائي على هذا النوع من الجرائم و ضرورة احترام مبدأ الشرعية، و التفسير الضيق للنصوص الجنائية [1].

- فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي، الذي قد يكون في صورة ممارسة العنف و الإيذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر و تقليد المفاتيح كما في جريمة السرقة، مفاده إن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها (Soft Crime) لا تحتاج إلى عنف ولا سفكا للدماء [2]، كل ما تطلبه وجود مجرم يسخر خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير

[1] عواطف محمد عثمان عبد الحليم ,الجرائم المعلوماتية : تعريفها ,صورها ,جهود مكافحتها دوليا ,اقليميا ,ووطنيا ,مجلة العدل ,السودان ,المجلد 10,العدد 24 ,2008,ص65 ,مشاراليه في : بيدي أمال , جهود الامم المتحدة في مكافحة الجريمة السبيرانية ,مجلة البحوث في الحقوق و العلوم السياسية ,دورية تصدر عن كلية الحقوق جامعة الجلفة ,العدد 01 ,جوان 2022 ,ص310.

[2] عبد الصبور عبد القوي علي مصري ,المحكمة الرقمية و الجريمة المعلوماتية ,الطبعة الأولى ,مكتبة القانون و الاقتصاد ,الرياض ,المملكة العربية السعودية ,2012 ,ص51 مشار اليه في :حسين عبد الكريم يونس ,خليل يوسف الجندي ,الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الاسباب ,دار كفاءة المعرفة للنشر و التوزيع ,عمان ,الطبعة الأولى ,2021 ,ص 102 .

بالقاصرين دون الحاجة إلى صرف مجهود عضلي أو سفك دماء [1] لكن هذه الطبيعة للج س لا يزيدها إلا تعقيدا إذ تتطلب نصوص خاصة لابد أن ينص عليها القانون صراحة و هذا القصور في النصوص الجنائية يترتب عليه مباشرة مساس بمبدأ المشروعية في حالة توسع القاضي في تفسير النصوص العقابية التقليدية و بهذا يتم إفلات أعداد كبيرة من الجناة من العقاب .

– إضافة لنقص المختصين الجنائيين في المجال الرقمي مقارنة بعدد المجرمين و الجرائم في هذا المجال ونقص المعرفة بمكونات و أدوات الجريمة السبيرانية ما أدى لاستفحال الظاهرة أكثر فأكثر.

ثانيا :الشق الإجرائي : إن من أهم العقبات في هذا الشق تنفيذ الإجراءات التي تضمنتها القوانين الإجرائية كالتفتيش و المعاينة و التحفظ و المصادرة لأن الأدلة غير مادية [2].

- تتميز الجرائم الالكترونية بغياب الآثار المادية الملموسة ,مما يفقدها وجود شهود مباشرين يمكن الاعتماد على شهاداتهم ,كما يصعب طابعها الافتراضي العثور على أدلة مادية تقليدية تثبت وقوعها مقارنة بالجرائم التقليدية و يعود السبب في ذلك إلى استخدام الجاني وسائل فنية و تقنية معقدة في اغلب الأحيان و هذا السلوك المادي في ارتباطها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل و التلاعب به [3]
- يجدر الإشارة أيضا إلى مشاكل الاختصاص فبما أن الجريمة السبيرانية هي جريمة في غالب الأحيان عابرة للحدود فانه يقع إشكال الاختصاص من تساؤلات و اختلاف أي قانون يطبق عليها و أي محكمة تختص بمتابعتها و هل يتم ذلك وفق المبادئ

[1] أسامة احمد المناعسة و جلال محمد الزعبي ,جرائم تقنية نظم المعلومات الالكترونية ,الطبعة الثانية ,دار الثقافة للنشر و التوزيع ,عمان 2014 ,ص97 مشار اليه في :حسين عبد الكريم يونس ,خليل يوسف الجندي ,الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الاسباب ,دار كفاءة المعرفة للنشر و التوزيع ,عمان ,الطبعة الأولى ,2021 ,ص 102 .

[2] عواطف محمد عثمان عبد الحليم ,المرجع السابق ,ص67 .

[3] بن عميروش ريمة ,عن خصوصية الجريمة المعلوماتية ,مجلة الفقه القانوني و السياسي ,جامعة ابن خلدون ,تيارت ,العدد الثاني ,2021ص 79 مشار اليه في : صيلع سعد ,آليات مكافحة الجريمة الالكترونية في التشريع الجزائري ,أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث (ل.م.د) ,تخصص قانون جنائي,المركز الجامعي مرسلي عبد الله , تيبازة ,2025/2024 ,ص 28 .

التقليدية المتعارف عليها (مبدأ الإقليمية , مبدأ العينية ...) أم تخضع لمبادئ جديدة مستحدثة.[1]

- **الفرع الثاني : الصعوبات متعلقة بالمجني عليه :**

- إن من اكبر المعوقات التي حالت دون تحقيق الحماية المطلوبة من الهجمات السبيرانية هو سلوك المجني عليه و الذي قد يكون شخص طبيعي أو معنوي (من شركات ,مؤسسات ...الخ) و غالبا ما يتمثل هذا السلوك في الإعراض عن التبليغ عن الهجومات السبيرانية التي يتعرضون لها، قد يبدو ذلك غير منطقيا لكن الأسباب التي تجعل المجني عليه يقوم بذلك تفسر هذا السلوك و تتمثل تلك الأسباب في التالي :[2]

- عدم الإدراك بأن الأفعال التي يتعرضون لها من هجومات و اختراقات الكترونية تعتبر ضمن الجرائم التي يعاقب عليها القانون .
- تخشى المؤسسات الكبرى الخسائر التي يسببها التحقيق الخاطئ و التي قد تفوق أحيانا ميزانيتها الخسائر التي تسببها الجرائم سبيرانية في حد ذاتها ,إضافة لتعطيل عمل المؤسسات خلال فترات التحقيق .
- إخفاء أسلوب الجريمة لتفادي انتشارها مستقبلا .
- عدم الإبلاغ خوفا من الفضيحة في حال تعلقت الجريمة بجرائم ابتزاز أو جرائم أخلاقية .

[1] قطاف سليمان ,بوقرين عبد الحليم ,المرجع السابق , ص83 .

[2] عصام حسني الأطرش ,محمد محي الدين عساف ,المرجع السابق , ص630 .

المبحث الثاني : سبل تعزيز الجهود الدولية في مواجهة الجرائم السبيرانية

- إن الجرائم السبيرانية و رغم كل الجهود المبذولة في مواجهتها إلا أنها لازالت في تطور مستمر من ناحية النوعية و الأسلوب و فئة المرتكبين لها و حتى الأهداف التي تستهدفها و ليس هذا فقط بل أصبح تطورها يفوق تطور الأساليب و القوانين التي تعمل على مواجهتها لذا لابد من تحديد و اقتراح سبل تعزيز هذه الجهود على المستوى الدولي و الإقليمي و حتى الداخلي للدول حيث أن كل منها يسهم في تعطيلات بالنسبة للمجرم السبيراني خاصة و أن هذه الجريمة لا تعترف بالحدود الجغرافية للدول ولا تعتبرها حائلا بينها و بين تحقيق الغرض الإجرامي ,في هذا المبحث و بعد تقييمنا لتلك الجهود و تحديد على وجه الدقة نقاط القصور فيها سندرس بين المطلبين الأول و الثاني سبل تعزيز هذه الجهود في مواجهة الج س من الناحية القضائية (المطلب 1) و من الناحية الفنية (المطلب 2) .

- **المطلب الأول : تعزيز التعاون القضائي الدولي .**

يعد ضعف التنسيق الدولي احد اكبر العقبات في مكافحة الجرائم السبيرانية و هذا ما تم توضيحه و التأكد منه أعلاه ,حيث تستغل الفجوات بين الأنظمة القانونية لتنفيذ الهجمات و من أبرزها عدم الاتفاق على نموذج موحد للنشاط الإجرامي السبيراني, ولتجاوز مثل هذه العقبات لابد من :

الفرع الأول : تبني رؤية موحدة للنشاط الاجرامي السبيراني .

– إن تحديد نموذج موحد و متفق عليه بين الدول لهذا النشاط الإجرامي هو أولى الخطوات[1] لتعزيز الجهود المبذولة في هذا المجال من الناحية القضائية ذلك أن الوحدة الدولية في أسلوب التعامل مع الجرائم العابرة للحدود و منهم الجريمة السبيرانية هو بمثابة خطوة استباقية للجناة السبيرانيين تغلق عليهم الكثير من الثغرات للإفلات من العقاب إلا إن ذلك لا يكفي لوحده بل يجب إن يتم تفعيل الاتفاقيات الدولية المصادق عليها عمليا و ضمان التزام الدول بتطبيقها[2] من خلال تحديث تشريعات وطنية مواءمة لها ,كتصديق المغرب سنة (2018) على اتفاقية بودابست و تعديل قوانينه الجنائية لتشمل جرائم مثل التحرش الالكتروني و غسيل الأموال عبر الانترنت .[3]

– ومن اجل تعزيز الجهود الدولية المبذولة لا يجب الاكتفاء فقط بما تم ذكره أعلاه بل يجب أيضا التأكيد على :

الفرع الثاني : تسريع الإجراءات و تبني الإنابة القضائية :

تعتمد آليات التعاون التقليدية (مثل طلبات تسليم المجرمين) على إجراءات ورقية معقدة لا تواكب السرعة التي ترتكب بها الجرائم السبيرانية لذا لابد من العمل على وضع قواعد لتسريع هذه الإجراءات لمواكبة هذا التطور و نوعية هذه الجرائم .

---

[1] ماجد احمد الزاملي ,**الاستراتيجية الوطنية للتعاون الدولي في مجال مكافحة الجريمة** ,
https://m.ahewar.org/s.asp?aid=727111&r=0,تاريخ الاطلاع 09 ماي 2025م ,على الساعة 12:27 .

[2] ماجد احمد الزاملي ,**الاستراتيجية الوطنية للتعاون الدولي في مجال مكافحة الجريمة** ,
https://m.ahewar.org/s.asp?aid=727111&r=0,تاريخ الاطلاع 09 ماي 2025م ,على الساعة 12:46 .

[3] ياسين كحلي ,**تحديات الجريمة السبيرانية و الجهود الدولية و الوطنية لمواجهتها** ,https://albab.ma/ ,تاريخ الاطلاع يوم 09 ماي 2025م ,على الساعة 16:06 .

حيث تصنف الإنابة القضائية ضمن ابرز الاستراتيجيات التسهيلية في مواجهة الجريمة عموما و الجريمة العابرة للحدود و المنظمة خصوصا [1] بما فيها الجريمة السبيرانية فبعد أن أصبحت الحدود بين الدول تشكل مشكلة في هذا المجال كونها تعيق القضاة قبل الجناة خاصة مع صعوبة و بطء الإجراءات المتعلقة بالتحقيق في هذا النوع من الجرائم حيث أن الطريق الدبلوماسي التقليدي أصبح سببا في إفلات الجناة نتيجة بطئ إجراءاته كان لابد من استحداثها .

لهذا تعتبر الإنابة القضائية احد أهم سبل تعزيز الجهود الدولية في مكافحة الج س بعد عمليات توحيد المعايير القانونية بين الدول .

الفرع الثالث : محاكاة النماذج الناجحة و محاولة الاستفادة منها :

تمثل اتفاقية مجلس أوروبا المتعلقة بالجريمة الالكترونية و التي تم التطرق إليها سابقا (اتفاقية بودابست 2001) و التي نجحت في توحيد بعض المصطلحات الضرورية في المجال مثل :مصطلح بيانات الحاسوب ,سير البيانات ...الخ نموذجا جيدا للمحاكاة و الاستفادة منه حيث يساهم الأسلوب بشكل كبير و فعال في تسهيل التعاون القضائي بين الدول الأعضاء فيها حيث انه يمثل أول خطوات المجتمع الدولي في التوافق حول نموذج موحد للجريمة السبيرانية من اجل توحيد أساليب التعامل معها و تصعيب على الجاني سبل التهرب و الإفلات من العقوبة التي كذلك يجب الاتفاق عليها دوليا و تبنيها في التشريعات الداخلية للدول .[2]

[1] بن يحي نعيمة ,الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم ,مجلة الدراسات الحقوقية ,جامعة مولاي الطاهر ,سعيدة ,المجلد04 ,العدد01 ,2017 ,ص10 ص11 .

[2] اتفاقية المجلس الاوروبي (بودابست 2001) المتعلقة بمواجهة جرائم الالكترونية .

الفرع الرابع : نشر ثقافة الابلاغ عن الجرائم السبيرانية :

تنقص ثقافة الإبلاغ بين الأشخاص الطبيعيين و المعنويين عن الجريمة التقليدية على العموم و فيما يخص الجريمة السبيرانية على الخصوص و هذا ما سبب عرقلة في اكتشاف هذه الجرائم و استفحال الجناة و بالتالي انتشارها أكثر .

و يعود ذلك لعدة أسباب من بينها الخوف، عدم إدراك خطورتها ....الخ

و من ابرز الأمثلة الحية و التي تمثل خطوة واعدة في مجال نشر ثقافة الإبلاغ لدينا مبادرة "الشبكة الآمنة (NIS DIRECTIVE)" في الاتحاد الأوروبي والتي تلزم الشركات العاملة في قطاعات حيوية بالإبلاغ عن الحوادث السبيراينة و تعزيز التعاون مع الحكومات [1].

- إضافة لاستحداث منصات خاصة و مشتركة بين القطاع العام و الخاص للإبلاغ عن الحوادث عبر قنوات آمنة ,مثل :المنصات الحكومية المشفرة و منها :
مبادرة الإبلاغ السبيراني الموحد في الاتحاد الأوروبي .

- **المطلب الثاني: تعزيز التعاون التقني و الفني .**

- يشمل التعاون التقني و الفني عدة جوانب و تختلف طرقه و أساليبه حيث يعتبر من أهم مظاهر التعاون الدولي ضد الجريمة السبيرانية كما انه في تطور مستمر مع تطور الإجرام السبيراني و يتطلب استراتيجيات متعددة الأبعاد تعزز تنسيق و تبادل الخبرات و فيما يلي آليات التعاون التقني و الفني بين الدول لتعزيز التصدي للجرائم السبيرانية.

[1] الموقع الرسمي للاتحاد الأوروبي ,https://www.eeas.europa.eu/ ,تاريخ الاطلاع :17 ماي 2025 ,ساعة الاطلاع :12:52 .

الفرع الأول : تقاسم الخبرات و تكوين الأطر :

نظرا لأهمية تبادل الخبرات في تفعيل دور الجهات المكلفة بمكافحة الإجرام ,نصت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية [1]على ضرورة أن تساعد الدول الأطراف بعضها البعض على تقاسم الخبرة في هذا المجال، وذلك بإعداد و تخطيط وتنفيذ برامج بحث و تدريب ,مع إمكانية الاستعانة بالمؤتمرات و الحلقات الدراسية الإقليمية، من اجل تحفيز النقاش حول المشاكل التي تعتبر شاغلا مشتركا ,بما في ذلك مشاكل دول العبور و احتياجاتها الخاصة[2]

-كما يجب العمل على على تحديث المؤسسات القضائية و الأمنية في جميع دول العالم و تطويرها و تأهيل أطرها من اجل نجاعة أكثر في مواجهة الجريمة التي تزداد تعقيدا بالشكل الذي يجعل من الصعب كشفها كالجرائم المصرفية و تبييض الأموال التي تتطلب دراية خاصة بالأنظمة المصرفية و قواعد التجارة الدولية، و التعاون بين المكتب المركزي الوطني للمنظمة الدولية للشركة الجنائية، "الأنتربول" و المصالح القضائية أن لهذه المنظمة دور "فعال" في مجال محاربة الجريمة المنظمة [3] بما فيها الجريمة الالكترونية .

ويمكن أن يكون ذلك بتنظيم مراكز تدريب إقليمية خاصة تديرها دولة متقدمة .

الفرع الثاني: استعمال برامج الذكاء الاصطناعي :

كاستعماله في التحقيق و الاستفادة منه للتنبؤ بالهجمات السبيرانية المستقبلية , كون أن المخاطر الالكترونية تتطور باستمرار لابد أن تستعد الأنظمة لمواجهتها باليات

---

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية , تم تبنيها من قبل الجمعية العامة للأمم المتحدة في نوفمبر 2000 ودخلت حيز النفاذ في سبتمبر 2003، تشددهذه الاتفاقية على التعاون الدولي والمساعدة القانونية المتبادلة وتبني التدابير الوطنية الفعالة، وتعكس الموقف الدولي الحاسم ضد الجرائم المنظمة العابرة للحدود,https://www.nazaha.gov.kw/ / ,تاريخ الاطلاع :17 ماي2025 ,ساعة الاطلاع :15:31 .

[2] ماجد احمد الزاملي ,**الاستراتيجية الوطنية للتعاون الدولي في مجال مكافحة الجريمة** ,

https://m.ahewar.org/s.asp?aid=727111&r=0,تاريخ الاطلاع 10 ماي 2025م ,على الساعة 15:52 .

[3] ماجد احمد الزاملي ,**الاستراتيجية الوطنية للتعاون الدولي في مجال مكافحة الجريمة** ,

https://m.ahewar.org/s.asp?aid=727111&r=0,تاريخ الاطلاع 10 ماي 2025م ,على الساعة 16:00 .

تتسم بالذكاء الذي يحاكي ذكاء الج س و مبنية على تقنيات الذكاء الاصطناعي و منهاجياتها لتدعم عمليات التحكم و المراقبة و اتخاذ القرارات الدقيقة من قبل الخبراء و أصحاب المعرفة و دعم عمليات إدارة امن المعلومات و اكتشاف عمليات التلاعب و التجسس [1].

و من الايجابي انه في هذا السياق اتخذت عدة دول مبادرات سباقة في التعامل مع تطورات الذكاء الاصطناعي،حيث أصدرت لجنة العلوم و التكنولوجيا التابعة لبرلمان المملكة المتحدة تقريرا عام 2016 م دعت فيه إلى إنشاء لجنة دائمة مختصة بالذكاء الاصطناعي .

تهدف هذه اللجنة إلى تحليل الآثار المترتبة على هذه التقنية ووضع مبادئ توجيهية لضبط مسار تطورها بالإضافة إلى تصميم إطار قانوني ينظم استخداماتها و تطبيقاتها [2] و ذلك لان هذه التقنية بقدر ما هي مفيدة في مواجهة الجريمة الالكترونية إلا أنها سلاح ذو حدين قد يتم استغلالها في ما هو أسوء و اخطر بإتباع أساليب جديدة في الجرائم الالكترونية حيث ان الذكاء الاصطناعي يتمثل في تطوير خوارزميات برمجية تتمكن مثلا من تمييز الوجوه التي في الصور على الانترنت، المساس بالخصوصية "ويقصد بذلك الخصوصية الرقمية " و التي تشكل انتهاكا لحقوق الإنسان وهذا ما يتم التحريص عليه بشدة في آليات مواجهة الجرائم السبيرانية فلا يمكن اعتبار أن تحقيق الأمن السبيراني ناجحا إذا تم خلاله انتهاك للخصوصيات الرقمية و المعلومات الشخصية للمستخدمين [3].

[1] لخضر دولي ,نفيسة ناصري ,دور الذكاء الاصطناعي في مواجهة الجريمة الالكترونية ,مجلة المؤشر للدراسات الاقتصادية ,جامعة طاهري محمد ,بشار ,المجلد 02 , العدد 02 ,2018 ,ص52 .

[2] دهشان يحي ابراهيم ,قواعد المسؤولية الجنائية عن تطبيقات الذكاء الاصطناعي ,مجلة الشريعة و القانون ,جامعة الامارات العربية المتحدة ,الامارات ,المجلد 34 ,العدد 82 ,2020 ,ص04 .

[3] Robotic and artifisial intelligence ,parliament Uk ,Report of the committee on science and Technology ,Published 12 Oct 2016 p77 .

الفرع الثالث : إبرام تعاقدات مع القطاع الخاص :

و يتم ذلك بتعزيز التعاون بين الحكومات و الشركات التكنولوجية الكبرى مثل : شركة مايكروسوفت وقوقل غيرهم بهدف رصد التهديدات و تقاسم البيانات مع الموازنة بين السعي للأمن الرقمي وحقوق الخصوصية الرقمية لتجنب الانتهاكات.

- وهذه الخطوة في الواقع قد بدأت في الظهور على المستوى الدولي حيث بادرت دولة الإمارات المتحدة في 2023 إلى توقيع مجلس الأمن السبيراني لها على مذكرة تفاهم بشأن التعاون في مجال الأمن السيبراني مع شركة مايكروسوفت و هاذ ما نشجع عليه من اجل توفير بيئة رقمية آمنة، وبموجب هذه المذكرة ستعمل شركة مايكروسوفت و مجلس الأمن السبيراني على تعزيز التعاون المشترك في تبادل المعلومات ضمن المجالات المرتبطة بالأمن السيبراني ,مع تركيز خاص على التعاون الوطني في مجالات الوقاية من الهجمات السبيرانية و إدارتها .
- كما يشمل التعاون تنفيذ برامج توعوية لرفع مستوى الوعي،و استكشاف الفرص التجارية و الاقتصادية المتعلقة بتقنيات الأمن السيبراني إلى جانب ذلك، سيسعى الطرفان إلى تشجيع تبادل المعطيات بينهما لتعزيز القدرات في مواجهة التهديدات السيبرانية و الاستجابة لها بشكل فعال . [1]
- في نفس السياق يمكن التعاون على إنشاء فرق عمل مشتركة بين القطاع العام و القطاع الخاص من اجل التدخل الفوري في حالات الاختراقات الكبرى حيث تعد الاستجابة السريعة للحوادث السبيرانية احد ركائز الأساسية لمواجهة الهجمات الالكترونية خاصة مع تزايد تعقيدها و ارتباطها بتهديدات الأمن القومي و البنى التحتية الحيوية حيث يتطلب تحقيق استجابة فعالة تعاون وثيق بين الحكومة و القطاع الخاص حيث يتمثل هذا التعاون في الآتي :

[1] "مجلس الأمن السيبراني" يتعاون مع "مايكروسوفت" لتعزيز قدرات الأمن السيبراني وتبادل المعلومات,الموقع الرسمي لشركة مايكروسوفت , https://news.microsoft.com/ar-xm/ ,تاريخ الاطلاع :17 ماي 2025 ,ساعة الاطلاع : 12:32 .

- آلية عمل فرق الاستجابة المشتركة :حيث تنشئ الدول فرق عمل متخصصة تضم خبراء من القطاعين العام و الخاص مثل تلك الفرق التي أنشئتها الولايات المتحدة الأمريكية (CISA) [1]. و التي تعمل بالتعاون مع شركات مثل قوقل و مايكروسوفت و أمازون لاحتواء الهجمات على البنية التحتية الحيوية .

- في الجدول التالي نوضح خطوات الاستجابة السريعة للحوادث السبيرانية [2]:

الأدوات/الموارد المستخدمة	ادوار القطاع الخاص	ادوار القطاع العام	الإجراءات	المرحلة
أدوات التحليل و منصات الإبلاغ	مشاركة البيانات الفنية مع الحكومة بواسطة قنوات مشفرة +تزويد الحكومات بعينات من البرمجيات الخبيثة .	توفير منصات آمنة للإبلاغ (مثل CISA) وإصدار تنبيهات فورية للقطاعات الحيوية	جمع البيانات الأولية عن الهجوم (البرمجيات الخبيثة...)و تحديد نطاق الهجوم	1.التقييم الأولي
انظمة العزل و أدوات إدارة الشبكات	تنفيذ إجراءات العزل الفني و التعاون مع شركات الحوسبة السحابية مثل امازون .	تنسيق الجهود مع مزودي البنية التحتية كشركات الاتصالات	عزل الأنظمة المصابة ومنع انتشار الهجوم عبر الشبكة .	2.الاحتواء الفوري
مختبرات التحليل الجنائي +منصات المراقبة	تحضير تقارير مفصلة عن الثغرات المكتشفة +استخدام الذكاء الاصطناعي للكشف عن الأنواع	مشاركة المعلومات الاستخباراتية مع القطاع الخاص و إجراءات تحقيقات جنائية	تحليل البرمجيات الخبيثة لتحديد مصدر الهجوم وتكتيكاته و تتبع الأنشطة المشبوهة عبر الشبكة .	3.التحليل الجنائي

[1] شهر التوعية بالأمن الالكتروني المعلوماتي أو السيبراني ,2021 ,راجع الموقع https://www.cisa.gov/ ,تاريخ الاطلاع :17 ماي 2025 , ساعة الاطلاع :13:18 .

[2] خالد عبد الحق ,دعاء عبد العال , المرجع السابق ,ص 230 .

	الغير معتادة للهجمات	مع الشرطة الدولية		
أنظمة النسخ الاحتياطي +أدوات اختبار الاختراق	تطبيق خطط التعافي بالتعاون مع الخبراء الحكوميين (إصلاح الثغرات و تحديث البروتوكولات)	توفير إرشادات معتمدة لاستعادة الأنظمة و تقديم منح أو تمويل لعمليات التعافي	إعادة تشغيل الأنظمة من النسخ الاحتياطية الآمنة . واختبار الأنظمة للتأكد من خلوها من الثغرات	4.استعادة الخدمات
منصات تبادل المعرفة +أدوات محاكاة الهجمات .	مشاركة التجارب مع القطاع العام لتحسين مستوى الوقاية و تطوير تقنيات أمنية أنجع بالتعاون مع الحكومة	تنظيم ورش عمل مشتركة لتحسين الجاهزية ونشر تقارير عامة عن الحادث (مع حماية هوية الشركات)	تقييم فاعلية الاستجابة وتحديد الدروس المستفادة +تحديث خطط الاستجابة بناءً على التحديات الجديدة	5.المراجعة و التحسين

في الأخير قد يواجه التعاون بين القطاعين العام والخاص تحديات جمة ومن أهمها :

- تضارب المصالح :فقد تتردد بعض الشركات الكبرى و ذات النفع الكبير في هذا المجال في مشاركة بيانات حساسة خوفا من التأثير على سمعتها أو أرباحها .
- قضايا الخصوصية : حيث يثير التعاون بين مخاوف متعلقة بمراقبة البيانات الشخصية أو استخدامها خارج الإطار المتفق عليه بين الأطراف .
- تأخر الإبلاغ : حيث تتردد الشركات في الإفصاح عن الاختراقات إما خوفا من الخسائر المالية أو من تشوه السمعة أو انه يكون تحت الابتزاز نظرا لتعلق الهجمة بقضايا أخلاقية .

لكن رغم التحديات التي يواجهها هذا النوع من التعاون إلا انه يبقى ضرورة حتمية لابد منها لبناء فضاء سبيراني آمن، خصوصا مع تزايد التعقيدات التي تتميز بها الهجمات الالكترونية الأخيرة و تزايد تأثيرها على البنية التحتية الحيوية و الأمن القومي .

- **خلاصة الفصل الثاني :**

نستخلص من هذا الفصل أن الجهود التي تبذلها الدول و مختلف كيانات المجتمع الدولي تواجه عدة تحديات على ارض الواقع حيث أنها نجحت إلى حد ما على المستوى النظري إلا أن نجاعتها الكاملة تتوقف على مدى أخذ الدول بها و بالتوصيات التي تحث و تعمل عليها تلك الجهود من مؤتمرات، اتفاقيات ...الخ إضافة لاستدراك نقاط القصور التي تشوب الآليات المعتمدة .حيث تظهر تلك التحديات و نقاط القصور في عدة مناحي و أهمها : ضعف التنسيق بين الدول، إضافة الصراع الرؤى الأمريكية و الروسية حول إدارة الفضاء السبيراني والصعوبات التي تواجه عمليات التحقيق و الإثبات و التي تعود غالبا للطبيعة الافتراضية للجريمة السبيرانية، كما يعد عدم إبلاغ الضحايا عن الجرائم لمختلف الأسباب عائقا أخر يعيق اكتشاف هذه الجرائم و محاسبة مرتكبيها.

تطرقنا في الفصل الثاني أيضا إلى سبل لتعزيز هذه الجهود من بينها : تسريع إجراءات التسليم الدولي و اعتماد آليات كالإنابة القضائية، أما على الصعيد التقني فيوصى بتبادل الخبرات بين الدول و توظيف الذكاء الاصطناعي، فضلا عن إبرام شراكات مع القطاع الخاص و تحديث التشريعات الوطنية تماشيا مع التطورات التكنولوجية مع الموازنة بين السعي للأمن السبيراني و حماية الخصوصية الرقمية .

الخاتمة

الخاتمة

ختاما فان الجريمة السبيرانية و الهجومات السبيرانية أضحت ظاهرة عالمية تهدد مختلف الفئات ابتداء من الأشخاص الطبيعيين مرورا بالشركات و المؤسسات الكبرى خاصة المالية وصولا إلى الدول و كبرى الكيانات على المستوى العالمي ورغم المحاولات الدولية المتنوعة من (اتفاقيات و مؤتمرات دولية ...الخ) إلا أنها لا تزال في تزايد مستمر و تطور من ناحية النوعية و الأسلوب و حتى الأشخاص المرتكبين لها و يعود ذلك لعدة أسباب تطرقنا لها على وجه التفصيل في الفصل الثاني من دراستنا و من أبرزها القصور التشريعي حيث أن رغم الأهمية و الخطورة التي تكتسيها الجريمة السيبرانية و تأثيرها على جميع المجالات خاصة على الصعيد الاقتصادي و السيادي و الاجتماعي إلا أن تلك الأهمية و الإدراك بالخطورة لم يترجم على الصعيد التشريعي .فصحيح انه معترف بها و بمدى خطورتها إلا أن الجهود ليست بتلك النوعية و الجدية المطلوبة خاصة في الدول النامية .

لم تتوقف دراستنا عند هذا بل قمنا بمحاولة متواضعة لإبراز و تحديد و تحليل النقائص التي تعتري الجهود التي تم بذلها في هذا المجال و تم الانتقال إلى سبل تعزيز تلك الجهود و قسمناها إلى ناحيتين : الأولى من الناحية القانونية و القضائية كما ذكرنا سابقا استدراكا للـ(القصور التشريعي) وذلك من خلال:تحديد نموذج موحد و متفق عليه بين الدول حول هذا النشاط الإجرامي، تسريع الإجراءات، الإنابة القضائية، نشر ثقافة التبليغ ....الخ.

و الثانية من الناحية الفنية و ذلك من خلال :تقاسم الخبرات و تكوين الأطر، الاستعانة ببرامج الذكاء الاصطناعي، إبرام تعاقدات للشراكة مع القطاع الخاص ....الخ.

و من النتائج المتوصل اليها :

- التطور التكنولوجي الذي يشهده العالم بقدر ما هو مفيد من ناحية اختزال الوقت و الجهد و التكاليف إلا انه يشكل تحديات جديدة للدول من خلال تحول طبيعة التهديدات من تقليدية إلى لا تقليدية متمثلة في (الجرائم السبيرانية) مما يستوجب تعاون دولي مكثف .

- تم بذل جهود متنوعة على المستوى الدولي في مجال في مكافحة الجريمة السيبرانية حيث حققت تلك الجهود تقدمًا ملحوظًا من خلال :وضع أطر قانونية دولية (الاتفاقيات)، تعزيز التعاون التقني والقضائي، زيادة الوعي، حماية الفئات الحساسة كالأطفال والمستضعفين و حماية البُنى التحتية الحيوية. لكنها لم تحقق الأمن السيبراني الكامل بسبب : التحديات الهيكلية (كالتناقضات التشريعية و التطور المتسارع للجرائم السيبرانية)إضافة لغياب آليات رقابة دولية صارمة.

- لا تزال العديد من الدول تفتقر إلى البنية التحتية التقنية والقانونية لتنفيذ الاتفاقيات .

- انتُقدت بعض الآليات (مثل جمع البيانات في اتفاقية بودابست) لعدم توازنها بين الأمن و الخصوصية الرقمية و التي تندرج ضمن حقوق الإنسان .

- فشل المجتمع الدولي في وضع آليات فعالة لمحاسبة الدول على الهجمات السيبرانية (مثل الهجوم الروسي على أوكرانيا 2022) .

- مكافحة الجريمة السبيرانية يتطلب نهجا شاملا يجمع بين التكنولوجيا المتطورة و التشريعات الفعالة و الموحدة دوليا و الوعي المجتمعي و التعاون التقني و الفني العالمي،لا يوجد طريق واحد و محدد و لكن التكيف المستمر مع هذه الجريمة هو السبيل الأنجع للتصدي لها.

- لا يزال الطريق طويلا لكن الاتفاقيات الحديثة مثل مبادرة الأمم المتحدة 2024 تشكل خطوة واعدة نحو عالم رقمي أكثر أمانا.

أما عن التوصيات المقترحة :

1 – تحديث الاتفاقيات لمواكبة التهديدات الناشئة مثل الذكاء الاصطناعي المُستخدَم في الهجمات .

2 – العمل على ضمان توازن بين السعي للأمن السيبراني وحماية الخصوصية الرقمية .
3 – دعم الدول النامية عبر تمويل بناء القدرات التقنية والقانونية.من خلال إنشاء مراكز تقودها الدولة الأكثر تقدما في هذا المجال على مستوى الإقليم.
4 – إنشاء محكمة دولية متخصصة لمحاسبة الدول والأفراد على الجرائم السيبرانية العابرة للحدود .
5 – إعداد حملات توعوية للتعريف بالجريمة و مدى خطورتها على الأفراد و المؤسسات بأنواعها إضافة نشر ثقافة التبليغ عنها .
6– تحديث التشريعات الداخلية و أن تعمل الدول أكثر على تحسين تشريعاتها الداخلية و السعي لتوحيدها في مجال الأمن السيبراني بما يتوافق مع الاتفاقيات الدولية .

7–وضع أسس وضوابط للتحقيق و الإثبات مواكبة للتطور الذي تشهده تكنولوجيا المعلومات و الجرائم المرتكبة على مستوى البيئة الرقمية إضافة لاستخدام الوسائل المتطورة و الذكية لمواجهتها كبرامج الكشف السريع .

و أخيرا، الأمن السيبراني ليس هدفًا نهائيًا، بل عملية ديناميكية تتطلب تحديثًا مستمرًا للجهود الدولية، وتعاونًا أعمق بين الحكومات والقطاع الخاص، وإرادة سياسية لتحويل التوصيات إلى واقع ملموس .

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا : باللغة العربية :

1- قائمة المصادر :

1. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من الجمعية العامة للأمم المتحدة , نوفمبر 2000م .

2. اتفاقية برن المتعلقة بحماية المصنفات الأدبية و الفنية (1886م)

3. اتفاقية تريبس المتعلقة بحماية الملكية الصناعية (م2007) و (1994م)

4. اتفاقية المجلس الأوروبي (بودابست 2001) المتعلقة بمواجهة جرائم الالكترونية

5. إعلان فيينا (2000م) بشأن الجريمة والعدالة ومواجهة تحديات القرن الحادي والعشرين.

6. المادة 1 من الاتفاقية العربية لمكافحة جرائم المعلومات المعتمدة من جامعة الدول العربية , 21 ديسمبر 2010 م

7. المادة 3 من الاتفاقية العربية لمكافحة جرائم المعلومات المعتمدة من جامعة الدول العربية , 21 ديسمبر 2010 م

8. المادة 5 من اتفاقية المجلس الأوروبي المتعلقة بالجريمة الإلكترونية لعام 2001 .

9. المادة 7 من اتفاقية المجلس الأوروبي المتعلقة بالجريمة الإلكترونية لعام 2001 .

10. المادة 48 من اتفاقية المجلس الأوروبي المتعلقة بالجريمة الإلكترونية لعام 2001 .

11. القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 22-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات .

2- قائمة المراجع:

المؤلفات و الكتب العامة :

1. عمر محمد حماد ,الاحتكار و المنافسة غير المشروعة ,دار النهضة العربية,الطبعة الأولى,القاهرة ,2009 .

المؤلفات و الكتب المتخصصة :

1. أسامة احمد المناعسة ,جلال محمد الزعبي ,جرائم تقنية نظم المعلومات الالكترونية,دار الثقافة للنشر و التوزيع ,الطبعة الثانية,عمان 2014.
2. جاسم محمد جندل ,الجرائم الالكترونية ,دار المعتز للنشر و التوزيع,الطبعة الأولى , عمان,2022 .
3. حسين عبد الكريم يونس ,خليل يوسف الجندي ,الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الأسباب ,دار كفاءة المعرفة للنشر و التوزيع,الطبعة الأولى ,عمان,2021 .
4. خالد عبد الحق ,دعاء عبد العال ,الجرائم الالكترونية و التحقيقات الجنائية ,دار اليازوري,الطبعة الأولى ,ب ب ن ,2025 .
5. خالد عياد الحلبي ,إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت ,دار الثقافة للنشر و التوزيع, بدون طبعة, الأردن, 2011 .
6. طارق عفيفي صادق أحمد ,الجرائم الالكترونية /جرائم الهاتف المحمول دراسة مقارنة بين القانون المصري و الإماراتي و النظام السعودي ,المركز القومي للإصدارات القانونية,الطبعة الأولى ,القاهرة,2015 .

7. عادل عبد الصادق ,الإرهاب الالكتروني و القوة في العلاقات الدولية نمط جديد و تحديات مختلفة ,مطبوعات مركز الدراسات السياسية و الاستراتيجي,الطبعة الأولى ,القاهرة ,2009 .
8. عبد الصبور عبد القوي علي مصري ,المحكمة الرقمية و الجريمة المعلوماتية ,مكتبة القانون و الاقتصاد ,الطبعة الأولى,الرياض ,المملكة العربية السعودية ,2012 .
9. عمر محمد أبو بكر بن يونس ,الاتفاقية الأوروبية حول الجريمة الافتراضية ,مؤسسة ادم للنشر و التوزيع, الطبعة الثانية,مالطا ,2008 .
10. محمود احمد عبابنة ,جرائم الحاسوب و أبعادها الدولية ,دار الثقافة للنشر و التوزيع,الطبعة الأولى,عمان ,2005.
11. منى الأشقر جبور , السيبرانية هاجس العصر , المركز العربي للبحوث القانونية و القضائية , ب. ب. ن ,2016.
12. ميرفت محمد حبايبة ,مكافحة الجريمة الالكترونية دراسة مقارنة في التشريع الجزائري و الفلسطيني ,دار اليازوري العلمية ,الطبعة الأولى,عمان ,2023.
13. يعيش تمام شوقي ,الجريمة المعلوماتية – دراسة تأصيلية مقارنة ,مطبعة الرمال,الطبعة الأولى, الوادي ,2019 .

الرسائل و المذكرات :

- 1. رحيم محمد ,التحديات الجديدة للأمن الدولي التهديدات السبيرانية ,أطروحة دكتوراه في العلوم السياسية و العلاقات الدولية ,جامعة الجزائر ,2024.
- 2. رشدي محمد علي محمد عيد علي ,الحماية الجنائية للمعلومات على شبكة الانترنت ,أطروحة دكتوراه ,مقدمة إلى كلية الحقوق ,جامعة القاهرة ,2009 .

- 3. سعيداني نعيم,آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة ماجستير ,كلية الحقوق و العلوم السياسية ,قسم الحقوق ,جامعة الحاج لخضر ,باتنة 2013/2012.
- 4. صيلع سعد ,آليات مكافحة الجريمة الالكترونية في التشريع الجزائري ,أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث (ل.م.د) ,تخصص قانون جنائي,المركز الجامعي مرسلي عبد الله , تيبازة ,2025/2024 .

5. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية (الحاسب و الانترنت) ,أطروحة أعدت لنيل درجة الدكتوراه في القانون ,الجامعة الإسلامية في لبنان ,كلية الحقوق ,2004 .

6. نسيمة درار (2017) ,الأمن المعلوماتي و سبل مواجهة مخاطره في التعامل الالكتروني دراسة مقارنة .أطروحة دكتوراه ,جامعة ابي بكر بالقايد تلمسان – الجزائر ,كلية الحقوق و العلوم السياسية .

7. يوسف صغير ,الجريمة المرتكبة عبر الانترنت ,مذكرة ماجستير حقوق ,جامعة مولود معمري تيزي وزو ,2013.

الدوريات و المجلات العلمية :

1. أسماء فيلالي ,حقوق الملكية الفكرية للمصنفات المعلوماتية ,مجلة آفاق علمية ,جامعة تلمسان ,المجلد 14 ,العدد 01 ,2022.

2. آسيا عمراني ,التعاون الدولي في مواجهة الجرائم السبيرانية :الجزائر نموذجا ,مجلة الجزائرية للعلوم السياسية و العلاقات الدولية ,جامعة الجزائر 3 ,المجلد 3 ,العدد 2,ديسمبر 2010 .

3. بن عميروش ريمة ,عن خصوصية الجريمة المعلوماتية ,مجلة الفقه القانوني و السياسي ,جامعة ابن خلدون ,تيارت ,العدد الثاني ,2021 .

4. بن يحي نعيمة ,الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم ,مجلة الدراسات الحقوقية ,جامعة مولاي الطاهر ,سعيدة ,المجلد04 ,العدد01 ,2017 .

5. بوضياف اسمهان ,الجريمة الالكترونية و الإجراءات التشريعية لمواجهتها في الجزائر ,مجلة الأستاذ الباحث للدراسات القانونية و السياسية,جامعة محمد بوضياف ,المسيلة ,العدد 11 ,2018 .

6. بيدي أمال , جهود الأمم المتحدة في مكافحة الجريمة السبيرانية ,مجلة البحوث في الحقوق و العلوم السياسية مجلة البحوث في الحقوق و العلوم السياسية , جامعة الجلفة ,العدد 01 ,جوان 2022.

7. جمال بوازدية ,الإستراتيجية الجزائرية في مواجهة الجرائم السبيرانية "التحديات و الآفاق المستقبلية ",مجلة العلوم القانونية و السياسية,جامعة الجزائر 3,المجلد 10 ,العدد 01 ,2019 .

8. دهشان يحي إبراهيم ,قواعد المسؤولية الجنائية عن تطبيقات الذكاء الاصطناعي ,مجلة الشريعة و القانون ,جامعة الإمارات العربية المتحدة ,الإمارات ,المجلد 34 ,العدد 82 ,2020 .

9. ربحي محمد ,قراءة في اتفاقية تريبس (TRIPS) ,مجلة المعيار ,جامعة تيسمسيلت ,المجلد 13 ,العدد01, 2022 .

10. عز الدين قطوش ,الحرب الباردة الأمريكية – الروسية في الفضاء السبيراني ,مجلة مدارات سياسية ,جامعة الجزائر3 ,المجلد 07 ,العدد 02 ,2023 .

11. عصام حسني الأطرش ,محمد محي الدين عساف ,معوقات مكافحة الجريمة المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية ,مجلة جامعة الشارقة للعلوم القانونية ,جامعة الشارقة ,المجلد 16 ,العدد 9 ,2019.

12. علي قويدري ,أمال العايش ,الجريمة السبرانية مفهومها و سبل الوقاية منها ,مجلة نوميروس الأكاديمية ,جامعة عمار الثليجي ,الأغواط ,مجلد03 ,العدد 01 ,2022.
13. عواطف محمد عثمان عبد الحليم ,الجرائم المعلوماتية : تعريفها ,صورها ,جهود مكافحتها دوليا ,إقليميا ,ووطنيا ,مجلة العدل ,السودان ,المجلد 10,العدد 24 ,2008 .
14. فاروق خلف ,الآليات القانونية لمكافحة الجريمة المعلوماتية ,مجلة الحقوق و الحريات ,جامعة حمة لخضر ,الوادي ,المجلد 03 ,العدد 02 ,2015
15. قطاف سليمان ,بوقرين عبد الحليم ,مواجهة الجرائم السبيرانية في ضوء الاتفاقيات الدولية ,مجلة البحوث القانونية و الاقتصادية ,جامعة عمار ثليجي , الأغواط , المجلد 05 , العدد 02 ,2022
16. لخضر دولي ,نفيسة ناصري ,دور الذكاء الاصطناعي في مواجهة الجريمة الالكترونية ,مجلة المؤشر للدراسات الاقتصادية ,جامعة طاهري محمد ,بشار ,المجلد 02 , العدد 02 ,2018 .
17. ليندة شرابشة , السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية ,مجلة دراسات و أبحاث ,جامعة الجلفة ,المجلد 01 ,العدد 01 ,2009.
18. مراد مشوش ,الجهود الدولية لمكافحة الإجرام السبيراني ,مجلة الواحات للبحوث و الدراسات ,مجلة الواحات للبحوث و الدراسات ,جامعة غرداية ,المجلد 12 ,العدد 2 ,2019 .
19. مهدي رضا , الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري ,مجلة ايليزا للبحوث و الدراسات ,جامعة محمد بوضياف ,المسيلة ,المجلد 06 , العدد 02 ,2021 .
20. وردة شرف الدين ,التعاون القضائي و القانوني لمكافحة جريمة غسيل الأموال و المرتكبة بواسطة تقنية المعلومات وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات

لسنة 2010 ,مجلة الباحث للدراسات الأكاديمية ,جامعة بسكرة ,المجلد 08 ,العدد 02 ,2021 .

المؤتمرات و الندوات العلمية :

1. جون فرنسوا هنروت، « أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصرالشرطة والتعاون القضائي» ، أعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر ,المملكة المغربية ,19-20 يونيو 2007 .
2. يوم دراسي حول الجريمة الالكترونية, المركز الجامعي عبد الحفيظ بوالصوف, ميلة ,الموقع الرسمي لمجلس قضاء ميلة , 10 أكتوبر 2023 .

المواقع الالكترونية :

1. موقع وزارة البريد و المواصلات السلكية و اللاسلكية , https://fs.mpt.gov.dz/cybercriminalite/ ,تاريخ الاطلاع 16 ماي 2025 ,ساعة الاطلاع 17:14 .
2. موقع وزارة تكنولوجيات الاتصال التونسية ,انضمام تونس إلى إتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية المعتمدة ببودابست , https://www.mtc.gov.tn/index.php?id=119&L=1&tx_ttnews%5Btt_news%5D=4778&cHash=ea7685326b1108a66dcf1a335b5307d3 , تاريخ الاطلاع :26 أفريل 2025 ,الساعة : 12:58 .
3. موقع وزارة العدل الجزائرية ,قائمة الاتفاقيات القضائية المتعددة الأطراف المصادق عليها من طرف الجزائر , https://www.mjustice.dz/ar/ / ,تاريخ الاطلاع :16 ماي 2025 ,ساعة الاطلاع : 22:15 .
4. موقع وزارة الداخلية للملكة العربية السعودية, https://www.moi.gov.sa / ,تاريخ الاطلاع 19ماي2025 ,ساعة الاطلاع :22:40 .

5. موقع منظمة التعاون الاقتصادي و التنمية الدولية ,
https://www.ccacoalition.org/ar/partners/organisation-economic-co-operation-and-development-oecd ,تاريخ الاطلاع 04 ماي 2025 ,
ساعة الاطلاع : 20:24 .
6. موقع المنظمة العالمية للملكية الفكرية(WIPO) ,
https://www.wipo.int/treaties/ar/ip/berne/index.html ,تاريخ
الاطلاع :05 ماي2025 ,ساعة الاطلاع :15:24 .
7. موقع المجلس اوروبا في تونس , https://www.coe.int/ar-TN/web/tunis/the-coe ,تاريخ الاطلاع 26 افريل 2025 الساعة 14:20 .
8. موقع الاذاعة الجزائرية ,اعتماد اتفاقية لمكافحة الجريمة السبيرانية ..مكسب اخر في
سجل جهود الدبلوماسية الجزائرية بقيادة رئيس الجمهورية ,
https://news.radioalgerie.dz/ar/node/50035 ,تاريخ الاطلاع :06 ماي
2025 ,ساعة الاطلاع : 13:50 .
9. الحرب الإلكترونية العالمية الأولى , بخصوص الهجوم الاكتروني الروسي الأوكراني
,راجع الموقع : https://lcss.gov.ly/articles/blog/post-212/ ,تاريخ الاطلاع
:18 ماي 2025 ,ساعة الاطلاع :14:25 .
10. عن اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ,
https://www.nazaha.gov.kw/ ,تاريخ الاطلاع :17 ما الموقع الرسمي للاتحاد
الأوروبي ,https://www.eeas.europa.eu/ ,تاريخ الاطلاع :17 ماي 2025 ,
ساعة الاطلاع :12:52 .
11. "مجلس الأمن السيبراني" يتعاون مع "مايكروسوفت" لتعزيز قدرات الأمن
السيبراني وتبادل المعلومات,الموقع الرسمي لشركة مايكروسوفت ,

https://news.microsoft.com/ar-xm/ ,تاريخ الاطلاع :17 ماي 2025 ,ساعة الاطلاع : 12:32 .

12. شهر التوعية بالأمن الالكتروني المعلوماتي أو السيبراني ,2021 ,راجع الموقع https://www.cisa.gov/ ,تاريخ الاطلاع :17 ماي 2025 , ساعة الاطلاع :13:18 .

13. ماجد احمد الزاملي , **الإستراتيجية الوطنية للتعاون الدولي في مجال مكافحة الجريمة** ,راجعhttps://m.ahewar.org/s.asp?aid=727111&r=0 , تاريخ الاطلاع 09 ماي 2025م ,على الساعة 12:27 .

14. ياسين كحلي ,**تحديات الجريمة السيبرانية و الجهود الدولية و الوطنية لمواجهتها** , راجع https://albab.ma/ ,تاريخ الاطلاع يوم 09 ماي 2025م ,على الساعة 16:06

15. ميتيهان دورماز ,اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم الالكترونية: الأهداف و الثغرات الموقع الرسمي لمنصة دعم السلامة الرقمية, https://smex.org/ar ,تاريخ الاطلاع :10 أفريل 2025 ,الساعة : 14:19 .

16. موقع مجلس قضاء ميلة , https://courdemila.mjustice.dz/?p=actualite&p1=9 ,تاريخ الاطلاع 06 ماي 2025 ,ساعة الاطلاع : 11:59 .

التقارير :

1. الأمم المتحدة ,تقرير الجمعية العامة للأمم المتحدة بخصوص اتفاقية تاريخية لمكافحة الجريمة السيبرانية ,الجمعية العامة للأمم المتحدة,نيويورك,25ديسمبر 2024 .

ثانيا : باللغة الاجنبية :

The official website of the **United Nations** , https://www.un.org/ar/conferences , date of Access: May 16, 2025, hour of access :17:43 .

The official website of the **United Nations for the Prevention of crime and the treatment of criminals** , https://www.unodc.org/congress/ar/previous-congresses.html , date of Access: May 16, 2025, hour of access :16:29 .

Robotic and artifisial intelligence ,parliament Uk ,Report of the committee on science and Technology ,Published 12 Oct 2016 p .

فهرس المحتويات

فهرس المحتويات

شكر وتقدير

اهداء

قائمة المختصرات

مقدمة..... أ

الفصل الأول: طبيعة الجهود الدولية في مواجهة الجريمة السبيرانية -7-

تمهيد الفصل الأول:..... -8-

المبحث الأول: الجهود الدولية في مواجهة الجرائم السبيرانية .....-9-

المطلب الأول: جهود الأمم المتحدة في مواجهة الجريمة السيبرانية .....-9-

الفرع الأول :المؤتمرات الدولية و الأممية.....-9-

الفرع الثاني :الاتفاقيات و الاعلانات الدولية .....-12-

المطلب الثاني: المنظمات الدولية الفاعلة في مجال مواجهة الاجرام السيبيراني..-15-

الفرع الأول :منظمة التعاون الاقتصادي و التنمية (OECD).....-15-

الفرع الثاني :المنظمة العالمية للملكية الفكرية (WIPO)..... -16-

المبحث الثاني: الجهود الاقليمية و الوطنية في مواجهة الجرائم السبيرانية..... -19-

المطلب الأول: الجهود الاقليمية في مواجهة الجرائم السبيرانية .....-19-

الفرع الأول :الاتفاقية المتعلقة بالجريمة الالكترونية لعام 2001(بودابست)....-19-

الفرع الثاني:اتفاقية الجامعة العربية لمكافحة جرائم تقنية المعلومات (2010) .. -23-

المطلب الثاني: الجهود الوطنية و التعاون الوطني الدولي.....-26-

خلاصة الفصل الأول..... -30-

تمهيد الفصل الثاني: ..... -32-
المبحث الأول: تقييم الجهود الدولية في مواجهة الجرائم السبيرانية ..... -33-
المطلب الأول: ضعف التنسيق الدولي و صعوبات الإثبات و التحقيق في الجرائم السبيرانية.....-33-
الفرع الأول :ضعف التنسيق بين أفراد المجتمع الدولي لمكافحةالجرائم السبيرانية-34-
الفرع الثاني :مشاكل الاثبات و التحقيق في الجرائم السبيرانية ..... -35-
المطلب الثاني: الصعوبات المتعلقة بالجريمة و المجني عليه.....-38-
الفرع الأول :الصعوبات المتعلقة بالجريمة السبيرانية .....-38-
الفرع الثاني :الصعوبات المتعلقة بالمجني عليه..... -40-
المبحث الثاني: سبل تعزيز الجهود الدولية في مواجهة الجرائم السبيرانية..... -41-
المطلب الأول: تعزيز التعاون القضائي الدولي.....-41-
الفرع الأول :تبني رؤية موحدة للنشاط الاجرامي السبيراني.....-41-
الفرع الثاني :تسريع الاجراءات وتبني الانابة القضائية.....-42-
الفرع الثالث :محاكاة النماذج الناجحة ومحاولة الاستفادة منها .....-43-
الفرع الرابع :نشر ثقافة الابلاغ عن الجرائم السبيرانية ..... -43-
المطلب الثاني: تعزيز التعاون التقني و الفني.....-44-
الفرع الأول :تقاسم الخبرات و تكوين الأطر.....-44-
الفرع الثاني:استعمال برامج الذكاء الاصطناعي.....-45-
الفرع الثالث :ابرام تعاقدات مع القطاع الخاص.....-46-
خلاصة الفصل الثاني ..... -51-

خاتمة ..... **-53-**

قائمة المصادر والمراجع..... **-57-**

فهرس المحتويات ..... **-70-**

الملخص ..... Erreur ! Signet non défini. **-74-**

اللغة العربية :

تنوعت آليات التعاون الدولي لمكافحة الجريمة السيبرانية بين إطارين رئيسيين هما: الاتفاقيات الدولية كاتفاقية بودابست (2001) التي وضعت إطارًا قانونيًا عابرًا للحدود، واتفاقية الأمم المتحدة (2024) التي شملت جرائم مثل التعديات الجنسية الرقمية، بالإضافة إلى المؤتمرات الدولية (مؤتمرَي الأمم المتحدة 1990 و2015) التي دعمت تحديث التشريعات وبناء قدرات الدول النامية. كما ساهمت منظمات مثل الإنتربول و(OECD) في تنسيق التحقيقات وتوحيد المعايير الأمنية .

واجهت هذه الجهود عدة تحديات كالتباين التشريعي بين الدول، وصعوبة جمع الأدلة الإلكترونية، والتطور التكنولوجي المتسارع (كالتحديات التي يفرضها الذكاء الاصطناعي). أما على الصعيد الإقليمي، انضمت دول كالمغرب وتونس لاتفاقية بودابست، بينما تبذل دول عربية جهودًا لتوحيد التشريعات عبر اتفاقيات كاتفاقية الجامعة العربية (2010).

رغم النجاح النسبي في تعزيز الأمن السيبراني عبر تبادل المعلومات ورفع الوعي بأهميته، إلا أن التحديات المستمرة تتطلب تحسينًا، خاصةً في سد الفجوة بين التشريعات والتطبيق، وتجنب انتهاكات الخصوصية الناتجة عن آليات جمع البيانات، كما في اتفاقية المجلس الأوروبي للجريمة الإلكترونية .

الكلمات المفتاحية: الجريمة الإلكترونية، التصيد الاحتيالي ، الأمن السيبراني، اتفاقية بودابست.

English :

The mechanisms of international cooperation to combat cybercrime have been diversified into two primary frameworks: international agreements, such as the Budapest Convention (2001), which established a cross-border legal framework, and the United Nations Convention (2024), which expanded criminalization to include offenses like digital sexual exploitation. Additionally, international conferences (e.g., the 1990 and 2015 UN conferences) focused on modernizing legislation and building technical capacities in developing nations. Organizations such as INTERPOL and the OECD also played pivotal roles in coordinating investigations and harmonizing cybersecurity standards.

These efforts faced challenges, including legislative disparities among nations, complexities in collecting and validating digital evidence, and rapid technological advancements (e.g., challenges posed by artificial intelligence). Regionally, countries like Morocco and Tunisia acceded to the Budapest Convention, while Arab states pursued legislative harmonization through regional agreements, such as the Arab League Convention (2010).

Despite relative success in enhancing cybersecurity through information-sharing and raising awareness of its strategic importance, persistent challenges necessitate further improvements. Key issues include bridging the gap between legal frameworks and their implementation, and mitigating privacy violations stemming from data-collection mechanisms, as exemplified by the Council of Europe's Convention on Cybercrime.

Keywords: Cybercrime, Phishing, Cybersecurity, Budapest Convention

الملخص:

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية الحقوق و العلوم السياسية
قسم الحقوق

Ministère de l'Enseignement Supérieur et
de la Recherche Scientifique
Université de Ghardaia
Faculté des Sciences Droit, et Sciences
Politiques
Département Droit

شهـــادة تـــصحيح

يشـــهد الدكتور زرباني محمد مصطفى
بصفتـــه رئيـــسا فـــي لـــجنة المناقـــشة لـــمذكرة المـــاستر
أن الطالب(ة): بن أوذينة سندس ، رقم التسجيل: 220390 81411
أن الطالب(ة): ، رقم التسجيل:
تخصص: قانون جنائي ، دفعة: جوان 2022 النظام (ل م د)

أن المذكرة المعنونة بـ: الحصانة الدولية في مواجهة الجرائم الدولية

تم تصحيحها من طرف الطالب/ة وهي صالحة للايداع

غرداية في: 2025/06/29

إمضاء الاستاذ رئيس اللجنة المكلف بمتابعة التصحيح

رئيس القسم

إمضاء: م. زرباني