# الجرائم المعلوماتية وسبل مكافحتها على الصعيد الدّولي

د. فاتن علي بشينة ـ قسم القانون – الأكاديمية الليبية للدراسات العليا

**E-amil addres-f.ebshena@academy.edu.ly**

**https://www.orcid.org/0000-0003-3104-4295**

## الملخّـــص :

**لقد أدّى** التطـــوّر الهائل الحاصل في مجال تقنيــة المعلومات وتكنولوجيا الاتصالات ، وبرامـــج الحاسوب، وتزايد أعداد المستخدمين لها بشكل مطّـــرد ، إلى ظهور شكل جديد من الجرائم ، تسمى بالجرائم المعلوماتيـــة، وذلك نتيجة لسوء استخدام بعضهم لهذه التقنية ، أن هذه الجرائم تتسم بالعديد من الخصائص التي جعلت منها تشكل خطـــرًا محدقًا يهدد المجتمع الدولي بأسره، وهذا ما من شأنه أن يجعل من مسألة التعاون والتآزر وتضافر الجهود بين الدول لمواجهتها ضرورة ملحة، لذلك تظهر أهمية دراسة هذا الموضوع، وذلك لمعالجة الإشكالية الرئيسة المتمثلة في تقصي مدى فاعلية ونجاعة سبل مكافحة الجرائم المعلوماتية على الصعيد الدولي.

وسيتم دراسة الموضوع من خلال تقسيمه إلى مطلبين، نخصص المطلب الأول للتعريف بالجرائم المعلوماتية، بينما ينفرد المطلب الثاني لبيان سبل مكافحة الجرائم المعلوماتية على المستوى الدولي والمعوقات ذات الصلة.

**الكلمات المفتاحيـــة :** الجرائم المعلوماتية ـ الاتفاقيات الدولية ـ التعاون الدولي ـ سبل المكافحة ـ المعوقات.

## المقـــدمـــة:

**تعد الثورة** المعلوماتية من أبـــرز سمات العصر الحالي التي أسهمت في تيسير حياة الأفراد في كافة المجالات وعلى جميع الأصعدة، إلا أنه وبالرغم من آثارها الإيجابية وما حققته من فوائد عديدة للمجتمعات البشرية في مختلف نواحي الحياة التعليمية والاقتصادية والصحية والثقافية ، فقد تزامن مع الانتشار الواسع لاستخدام تقنية المعلومات وشبكة الإنترنت الدولية، إلى ظهور أنماط جديدة من الجرائم المستحدثة،

التي تتخطى الحدود الإقليمية للدولة الواحدة، مخلفه آثار سلبية وخطيرة بعدة دولة من شأنها زعزعة أمنها واستقرارها وهذا ما يفرض ضرورة تكاثف الجهود الدولية لمكافحتها.

## أهمية البحث:

تبرز أهمية البحث في الموضـــوع من الناحيتين النظرية والعملية ، فمن الناحية النظرية تكمن أهمية دراسة الموضوع في معرفة أهم التدابير المتخذة على الصعيد الدولي في سبيل التصدي لهذه الجرائم، أما من الناحية العملية فتبرز أهمية دراسة الموضوع في ما نشهده في الآونة الأخيرة من ازدياد عدد هذا النوع من الإجرام بشكل متسارع، وتعدد أشكاله وسهولة ارتكابه وإتلاف أدلة القيام به، مع ارتفاع حجم الخسائر الناجمة عنه وما له من أضرار قد تمس في بعض أنواعه بأمن الدولة القومي وسيادتها، لذلك فإن الحاجة ملحة لمعرفة أبرز سبل مكافحة هذه الجرائم، وما يعترضها من عقبات ويواجها من معوقات، وطرق تذليلها، لما لذلك من أهمية في ضمان ملاحقة ومعاقبة مرتكبيها، والتصدي لها بكل حزم.

## نطاق البحث:

يقتصر نطاق البحث على بيان خصائص الجرائم المعلوماتية وأنواعها، وأهم سبل مكافحتها دوليًا والمتمثلة في الاتفاقيات الدولية، والتعاون الدولي وما يواجها من صعوبات.

## إشكالية البحث:

تتمثل الإشكالية الرئيسة للبحث في تقصي مدى فاعلية ونجاعة سبل مكافحة الجرائم المعلوماتية على الصعيد الدولي.

## منهج البحث:

لقد اعتمدت في دراسة الموضوع على المناهج التالية:

1- المنهج الوصفي: وذلك في عرض الأفكار المعلومات المتعلقة بموضوع البحث.
2- المنهج التحليلي: في تحليل نصوص الاتفاقيات الدولية موضوع البحث.
3- المنهج النقدي : سنوظفه في تقييم مدى فعالية التدابير المتخذة لمكافحة الجرائم المعلوماتية على الصعيد الدولي.

## خطـــة البحث :

تم تقسيم البحث إلى مطلبين : تناولت فـــي ( المطلب الأول) التعريف بالجرائم المعلوماتية، أفردت الفرع الأول لبيان خصائص الجرائم المعلوماتية، وفي الفرع الثاني تناولت بيان أنواع الجرائم المعلوماتيـــة ، بينما خصصت ( المطلب الثاني) لبيان سبل مكافحة الجرائم المعلوماتية على المستوى الدولي والمعوقات ذات الصلة، تناولت في الفرع الأول سبل مكافحة الجرائم المعلوماتية، بينما أفردت الفرع الثاني لبيان معوقات مكافحة الجرائم المعلوماتية.

## المطلب الأول ـ التعريف بالجرائم المعلوماتية:

ارتبط ظهور وتعدد الجرائم المعلوماتية كما وسبق أن أشرنا بالتطور التكنولوجي الحاصل في مجال تقنية المعلومات والاتصالات، أن هذه الجرائم المستحدثة تتسم بالعديد من الخصائص التي تميزها عن غيرها من الجرائم التقليدية، لبيان خصائص هذا النوع من الإجرام وأهم أنواعه قسمنا هذا المطلب إلى فرعين، حيث خصصنا الفرع الأول لبيان خصائص الجرائم المعلوماتية، وأفردنا الفرع الثاني لعرض أهم أنواع الجرائم المعلوماتية.

### الفرع الأول ـ خصائص الجرائم المعلوماتية:

تتسم الجرائم المعلوماتية [1] بعـــدة خصائص وذلك من حيث أسلوب ارتكابها والوسيلة المستعملة، والصفات التي يتميز بها المجرم الذي يقوم بارتكابها، بالإضافة إلى خصوصية بعض الدوافع التي تدفعه للقيام بها، نتناول تفاصيل ذلك فيما يلي.

**1- الجريمة المعلوماتية[2] لا حدود جغرافية لها.**

تعد الجريمة المعلوماتية شكلًا جديدًا ومتطورًا من الجرائم العابرة لحدود الدولة الواحدة، فالجريمة المعلوماتية هي من نوع الجرائم التي يتم ارتكابها عن بعد عبر المسافات، حيث تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الجاني وبين النتيجة، وبالتالي قد لا تقف الجريمة المعلوماتية عند الحدود الإقليمية لدولة معنية، بل قد تعبر الحدود الإقليمية لدولة أخرى[3]، وهذا ما من شأنه أن يثير العديد من الإشكاليات منها صعوبة تحديد الدولة صاحبة الاختصاص القضائي، والقانون الواجب التطبيق، وغيرها من الإشكاليات التي تتعلق بإجراءات الملاحقة القضائية[4].

**2- صعوبة اثبات الجرائم المعلوماتية والكشف عنها.**

من الصعوبة بمكان اكتشاف الجريمة المعلوماتية، كما أن مسألة اثباتها ليس بالأمر الهين، ويعود ذلك لعدة أسباب يكمن أبرزها في التالي بيانه.

أ- أن الجريمة المعلوماتية لا تخلف آثار مادية فهي تتم في بيئة الكترونية بسرعة وذكاء، ولا تتطلب مجهود بدني لارتكابها بالتالي ليس هناك آثار لاقتحام مكان ما لسرقة الأموال أو سفك دماء لغرض التجسس على سبيل المثال، إنما هي بيانات

ومعلومات يتم تغييرها أو تعديلها أو مسحها كليًا أو جزئيًا من الأنظمة والسجلات الإلكترونية[5].

ب- سهولة إخفاء وإتلاف الجناة لأدلة الجريمة، إذ يستطيع الجاني في الجرائم المعلوماتية محو الدليل على شبكات الإنترنت وجهاز الكمبيوتر في زمن قياسي، وبضغطة زر واحدة[6].

ج- نقص الخبرة الفنية والتقنية لدى مأموري الضبط القضائي، وجهات الادعاء والتحقيق والقضاء بشكل عام، فهذا النوع من الإجرام يتطلب المام خاص بتقنيات الكمبيوتر ونظم المعلومات سواء بالنسبة لمرتكبها أو لمن يحقق فيها، بالتالي قد يصعب على المحقق التقليدي التعامل معها إذا كانت تنقصه الخبرة والمهارة في هذا المجال، حيث إنه قد يتلف المحقق الدليل الإلكتروني عن طريق الخطأ نتيجة لافتقاره للخبرة ولنقص التدريب[7].

**3- ارتفاع حصيلة الخسائر المادية الناجمة عن الجرائم المعلوماتية.**

ففي عام 2014، قدر مركز الاستراتيجية والدراسات الدولية CSIS أن الجريمة المعلوماتية كلفت العالم ما بين 345 مليار دولار، و445 مليار دولار، حيث تشر التقديرات إلى أن هذه الجرائم تتسبب في خسائر مالية هائلة في العديد من الدول نذكر منها على سبيل المثال إنه بلغت خسائر الجرائم المعلوماتية في قارة أمريكا الشمالية عام 2017 ما بين 140 إلى 175 مليار دولار[8]، ووفقًا للتقرير الصادر عن شركة cybersecurity ventures فإنه من المتوقع أن تزداد الأضرار المادية الناجمة عن الجرائم المعلوماتية بنسبة 15% سنويًا لتصل إلى 10.5 تريليون دولار سنويًا بحلول عام 2025[9].

**4- خصوصية بعض الدوافع الباعثة على ارتكاب الجرائم المعلوماتية.**

يعد الدافع المادي من أهم الدوافع التي تحرك الجاني لارتكاب الجريمة المعلوماتية بغية تحقيق الكسب المادي السريع بأقل جهد، بالإضافة إلى سهول التنفيذ وقلة الخطورة لإمكانية محو الدليل بيسر خصوصًا إذا كان محترف في هذا المجال، كما قد يرتكب الجاني الجريمة المعلوماتية لتحقيق غايات أخرى غير الكسب المادي، منها الرغبة في الانتقام أو التعاون والتواطؤ، أو بدافع سياسي كتهديد الأمن القومي لدولة ما عن طريق التجسس الإلكتروني، وغيرها من الدوافع الأخرى التي تتشابه مع الغاية والباعث على ارتكاب الجرائم التقليدية، إلا أن هناك بعض الدوافع الأخرى التي تتميز بها الجرائم المعلوماتية عن الجرائم التقليدية، حيث أنه قد يحدث أن يرتكب الفاعل هذه الجريمة رغبة منه في اثبات الذات، أو بدافع المتعة والتسلية دون أن تكون له أي نوايا آثمة، أو إرادة إجرامية، فقد تكون غايته فقط فهم النظام المعلوماتي، أو رغبة منه في الشعور بالتفوق أو لغرض التسلية فحسب[10].

**5- اختلاف طبيعة مرتكبي الجرائم المعلوماتية.**

في الغالب لا يتطلب ارتكاب الجرائم التقليدية أن يكون الجاني على مستوى علمي أو ثقافي معين، أو أن يكون على درجة عالية من الذكاء، بقدر ما قد يتطلب ارتكابها بدل مجهود بدني كالضرب والتحطيم والقتل...الخ، إلا أن الأمر مختلف بالنسبة للجرائم المعلوماتية التي يتطلب ارتكابها أن يكون الجاني شخص متمكن في مجال تقنية المعلومات، أي أنه على دراية كافية بها، لديه رصيد معرفي مكتسب عن طريق الخبرة والتجربة والممارسة العملية، فالمجرم المعلوماتي يتصف بالذكاء، ولا يميل إلى العنف، وتحدد مقدار المهارة التي يمتلكها المجرم المعلوماتي نوع الجرائم التي يرتكبها، فإذا كان يتمتع بقدر ضئيل من المهارة نجد أن الجرائم التي يرتكبها لا تتعدى إتلاف المعلومات أو نسخ البيانات والبرامج، أما إذا كان على درجة عالية من المهارة والاحتراف فإن ذلك قد يؤهله لارتكاب جرائم مثل سرقة الأموال أو التجسس الإلكتروني أو زرع الفيروسات[11].

**6- وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات.**

من خصائص الجريمة المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعلومات الخاصة بالكمبيوتر في أي مرحلة من مراحل تشغيل المعالجة الآلية للبيانات، سواء في مرحلة إدخال البيانات، أو عند مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات، وتعد هذه الخاصية شرط أساسي لابد من توافره حتى يمكننا البحث

في قيام أو عدم قيام أركان الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات، وبتخلفه تنتفي الجريمة المعلوماتية[12].

7- **الجريمة المعلوماتية جريمة متطورة** :

لا يمكن حصر أساليبها في الوقت الحاضر، وأن أمكن حصرها فإنه لا يمكن التنبؤ بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا المعلومات مستقبلًا[13].

**الفرع الثاني ـ أنواع الجرائم المعلوماتية**

أن التطور السريع الذي تشهده الجرائم المعلوماتية، يجعل من مسألة حصرها في أنواع محددة أو التنبؤ بها أمر في غاية الصعوبة، ولقد اختلف الفقهاء في تقسيم الجرائم المعلوماتية وفقًا للمعيار والأساس الذي استند عليه كل منهم، ويمكننا تقسيمها إلى نوعان أساسيان تندرج تحتهما عدة صور، وهي على التالي بيانه:

**أولًا- الجرائم الواقعة على النظام المعلوماتي.**

**1- جريمة الدخول غير المشروع إلى النظام المعلوماتي:**

أن مصطلح الدخول لا ينصرف إلى المعنى المادي أي الدخول إلى الغرفة التي يوجد بها جهاز الكمبيوتر، إنما ينصرف إلى النشاط الذهني الذي قام به الجاني بغية الوصول إلى موقع إلكتروني، أو إلى حساب شخصي، أو نظام معلوماتي بدون إذن أو بدون رضاء صاحبه، وتقع هذه الجريمة من كل إنسان سواء كان متخصص ويعمل في المجال المعلوماتي، أو من غير العاملين في هذا المجال سواء كان يستفيد من الدخول، أما لا، أي أن الجريمة تقوم بفعل الدخول إلى النظام مجردًا عن أي نتيجة[14]، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى نظام، أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخل بها، كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط[15].

**2- جريمة البقاء غير المشروع.**

تتحقق هذه الجريمة بالبقاء أو التواجد غير المشروع على موقع إلكتروني، أو حساب شخصي أو نظام إلكتروني، ويستوي في ذلك أن يكون دخول الجاني للموقع الإلكتروني، أو النظام المعلوماتي مصرحًا به أم غير مصرحًا به، فقد يكون دخول الجاني للموقع الإلكتروني مشروعًا، ولكنه يتجاوز بقاءه المدة الزمنية المسموح بها[16].

**3- الاعتداء على النظام المعلوماتي واستعمال مخرجاته.**

وتتحقق هذه الجريمة بقيام الجاني بإدخال أو تبديل أو محو بيانات في النظام المعلوماتي بطريقة غير مشروعة لتحقيق أغراض قانونية، وكذلك إتلاف وإفساد برامج ومكونات النظام المعلوماتي بواسطة إدخال فيروسات تتسبب في إحداث شلل تام أو جزئي لمكونات النظام[17].

**ثانيًا- الجرائم المرتكبة باستخدام النظام المعلوماتي:**

تتعدد الجرائم الواقعة بواسطة النظام المعلوماتي وتختلف باختلاف الغرض من ارتكابها، نتناول فيما يلي بيان أهم صورها.

1- **جرائم الأشخاص :**

تتنوع الجرائم المعلوماتية الواقعة بواسطة الأشخاص الطبيعيين، وتتمثل أبرزها في جرائم السب والقذف عبر الإنترنت من خلال مواقع التواصل الاجتماعي على سبيل المثال، وجرائم التعدي على حرمة الحياة الخاصة مثال ذلك: أن يقوم الفاعل بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكنه يطلع الغير عليها دون إذنه، ومن صور جرائم التعدي على حرمة الحياة الخاصة تسجيل المحادثات الشخصية، أو مراقبتها بأية وسيلة والتنصت على المكالمات بطرق غير مشروعة[18]، وأيضًا جريمة الاعتداء على حقوق الملكية الفكرية كحقوق المؤلف وبراءات الاختراع فهذه الحقوق بالإضافة إلى قيمتها المادية لها قيمة معنوية وأدبية[19]، والجرائم المخلة بالآداب العامة وتتمثل أهمها في الجرائم الجنسية كالتحريض على الدعارة، وإنتاج المواد الإباحية وترويجها، استغلال الأطفال والقصر أو المعوقين نفسيًا أو عقليًا في أنشطة جنسية غير مشروعة، والتحرش الجنسي..... وغيرها[20] من الأفعال والسلوكيات التي من شأنها نشر الرذيلة، والاعتداء على المبادئ والقيم الأخلاقية والدينية السائدة في المجتمع.

2-**جرائم الأموال**:

وتتمثل جرائم الأموال في الجرائم المرتكبة باستخدام النظام المعلوماتي بقصد تحقيق منفعة مادية، وتتنوع هي الآخرة ويتمثل أبرز أنواعها في جريمة التجارة الإلكترونية حيث شاع بيع وشراء وتأجير مختلف السلع عن طريق شبكة الإنترنت ويتم دفع الثمن بالنقود الإلكترونية، وكثيرًا ما قد يحدث أن يقع المستهلك فريسة للإعلانات الخادعة والمضللة بأن يقوم بشراء منتج يعتقد أنه أصلي ينتمي لعلامة تجارية معينة بناًء على ما تم الإعلان عنه ثم يكتشف بعد استلامه ودفع مبالغ مالية كبيرة أنه مقلد، ومن صور

جرائم الأموال غسيل الأموال إلكترونيًا[21]، وأيضًا استخدام بطاقات ائتمان منتهية الصلاحية أو مقلدة أو مسروقة ، والتعدي على أموال الغير بالوسائل الإلكترونية مثل الدخول إلى مواقع البنوك، والدخول إلى حسابات العملاء، وإدخال بيانات أو مسح بيانات بغرض اختلاس الأموال أو نقلها، وعلى سبيل المثال في عام 2003، تم التحقيق في الولايات المتحدة الأمريكية في جريمة سرقة أرقام 8 ملايين بطاقة ائتمان من شركات تجارية في حادثة تعد الأخطر من نوعها، بالرغم من تكرار مثيلاتها في فترات لاحقة، وقد اعترفت الشركات التي تجري عمليات تحويل مالية لشركات فيزا وماستر كارد وأمريكان إكسبريس بتعرضها لاختراق في نظام العمل من طرف خارجي غير مصرح له بالدخول على النظام[22].

**3- الجرائم الواقعة على الدولة.**

تتعدد الجرائم الواقعة على الدولة، والتي يكون الغاية منها تحقيق أهداف سياسية، ويتمثل أبرزها في جرائم التجسس الإلكتروني، حيث كشفت مجموعة من الوثائق بأن وكالة الأمن القومي الأمريكية تجسست على حوالي 125 مليار اتصال هاتفي ورسائل نصية عام 2013 كانت غالبيتها من دول شرق أوسطية[23]، ومن بين صور هذه الجرائم الإرهاب الإلكتروني، ويتم ذلك باستعمال وتوظيف النظام المعلوماتي في إنشاء مواقع إلكترونية بغية تعزيز النشاط الإرهابي، وذلك لتبادل المعلومات، وتسهيل الاتصال بين القيادات أو الأعضاء، وترويج أفكارهم، وأيضًا لتجنيد العناصر الجديدة وتعليمهم الطرق والوسائل التي تساعدهم على القيام بالعمليات الإرهابية، وأيضًا تدريبهم على كيفية تصنيع المتفجرات وغيرها من الأسلحة التي تدخل في تنفيذ الأعمال الإرهابية، كما تدخل في نطاق الجرائم المعلوماتية الواقعة على الدولة بث الإشاعات ونشر معلومات مغلوطة عبر الوسائل الإلكترونية بهدف إثارة الفوضى وتهديد الأمن والسلامة العامة بالدولة[24]، ومن أخطر صور الجرائم الواقعة على الدولة باستخدام النظام المعلوماتي الهجمات السيبرانية على الأخص تلك الموجه ضد قطاع الطاقة، فبعض الدول تستخدم هذه الهجمات كأداة لمحاربة خصومها، كما أن هذه الهجمات باتت هدفًا للتنظيمات التي تسعى من خلالها إلى تحقيق مكاسب مالية، وقد يتم استخدام هذه الهجمات أيضًا لغرض الانتقام من بعض أنظمة الحكم نتيجة مواقفهم السياسية.

وتجدر الإشارة إلى أن حدة وكثافة هذ الهجمات وتأثيراتها الخطيرة تتجاوز الأبعاد الاقتصادية لتصل إلى مسألة تهديد الأمن القومي، الأمر الذي دفع العديد من دول العالم إلى وضع استراتيجيات متكاملة لمواجهتها، ورفع ميزانيتها المتعلقة بالأمن السيبراني،

وقد تعرضت العديد من الدول لهذه الهجمات، نذكر منها على سبيل المثال الهجمات السيبرانية الموجه ضد قطاع الطاقة والمنشآت النووية الإيرانية من أهمها هجوم ستونكس (stunex 2010)، وأيضًا الهجمات السيبرانية الروسية ضد منشآت الطاقة الأوكرانية من عام 2015 حتى عام 2022[25].

**المطلب الثاني ـ سبل مكافحة الجرائم المعلوماتية على المستوى الدولي والمعوقات ذات الصلة**

أصبحت مسألة مكافحة الجرائم المعلوماتية هاجس يؤرق كافة الدول في الآونة الأخيرة، ولكون هذه الجرائم تتخطى الحدود الإقليمية للدولة الواحدة، فإنه يصعب على الدولة مواجهتها بمفردها مهما بلغت قوتها، الأمر الذي يستدعى بل يستلزم ضرورة دعم وتعزيز التعاون الدولي لمواجهتها، وأيضًا اتخاذ عدة وسائل والقيام بالعديد من الإجراءات لكفالة فاعلية مكافحتها، نتناول بيان تفصيل ذلك من خلال تقسيم هذا المطلب إلى فرعين نخصص الأول لعرض سبل مكافحة الجرائم المعلوماتية على المستوى الدولي ، وفي الفرع الثاني نستعرض المعوقات التي تحد من فاعلية سبل المكافحة.

**الفرع الأول ـ سبل مكافحة الجرائم المعلوماتية:**

تتعدد وتتنوع سبل مكافحة هذه الجرائم على الصعيد الدولي وسوف نركز في بحثنا هذا على بيان النصوص القانونية الدولية المعنية بذلك، والتعاون الدولي لكونه من أهم آليات التصدي لها نتناول فيما يلي بيانها على التوالي.

**أولًا- الاتفاقيات الدولية المعنية بمكافحة الجرائم المعلوماتية.**

تقر الاتفاقيات الدولية القائمة ذات الصلة بالموضوع قواعد قانونية تكفل مكافحة هذا النوع من الجرائم، حيث تعد الاتفاقيات الدولية إحدى أهم مصادر القانون الدولي، فهي بمثابة التشريع لاحتوائها على ذات المزايا التي يحتويها التشريع الوطني من حيث كونها مكتوبة ومحددة، وتتضمن قواعد قانونية تحدد حقوق وواجبات المخاطبين بأحكامها، ونظرًا لأن المقام لا يتسع لذكر جميعها، سنقتصر على بيان أهم هذه الاتفاقيات بشكل موجز.

1- **اتفاقية بـــــرن :** هي إحدى الاتفاقيات العالمية المعنية بحماية الملكية الفكرية للمبدعين في كافة المجالات، تم إبرامها لأول مرة في برن بسويسرا عام 1886،

وطرأت عليها عدة تعديلات في العديد من المؤتمرات، أخر نسخة معتمدة كانت عام 1971[26].

وتبرز أهمية هذه الاتفاقية في كونها حجر الأساس والقاعدة الأولية التي تم الاعتماد عليها في الاتفاقيات اللاحقة في هذا الإطار، حيث تم الاستناد عليها في منح الحماية القانونية الدولية لبرامج الحاسوب باعتبارها مصنفات أدبية في معاهدة الويبو تحديدًا بموجب المادة الرابعة منها[27]، التي استند واضعوها على ما أقرته المادة 1/2 من اتفاقية برن التي تنص على: " تشمل عبارة الآثار الأدبية والفنية جميع المنتوجات الأدبية والعلمية والفنية مهما كانت طريقة أو شكـــــل نشرها ..." [28].

**2- معاهدة الويبو(wipo) (المنظمة العالمية للملكية الفكرية).**

تم انشاء المنظمة العالمية للملكية الفكرية بمقتضى اتفاقية دولية دخلت حيز التنفيذ عام 1970، وفي عام 1974 أصبحت هذه المنظمة في عداد الوكالات المتخصصة التابعة لمنظومة الأمم المتحدة[29] وتنقسم معاهدة الويبو إلى معاهدتين هما:

أ- معاهدة الويبو بشأن حق المؤلف لعام 1996، والتي تعني بحماية حقوق المؤلفين في مصنفاتهم الأدبية والفنية، وبموجبها تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية.

ب- معاهدة الويبو بشأن الأداء والتسجيل الصوتي لعام 1996 والتي تعني بحماية حقوق فناني الأداء ومنتجي التسجيلات الصوتية[30].

**3- اتفاقية جوانب حقوق الملكية الفكرية المتصلة بالتجارة (اتفاقية تريبس TRIPS) :** دخلت حيز النفاذ عام 1996، وتهدف إلى حماية حقوق الملكية الفكرية المتصلة بالتجارة كالعلامات التجارية، والتصاميم الصناعية، وبراءات الاختراع[31]، ولقد تضمنت الاتفاقية على مواد من شأنها مكافحة الجرائم المعلوماتية ذات الصلة بموضوعها، من ذلك ما نصت عليه المادة (10) المتعلقة بحماية برامج الحاسب الآلي[32].

**4- اتفاقية بودابست المتعلقة بالجريمة الإلكترونية لعام 2001 م :** ويطلق عليها البعض اتفاقية مجلس أوروبا[33]، وتعد هذه الاتفاقية أول اتفاقية دولية متعددة الجنسيات – حيث تضم في عضويتها مجموعة دول أوروبا وغيرها من الدول الأخرى- التي تعني بشكل

أساسي بمكافحة الجرائم المعلوماتية[34]، وذلك من خلال ما تضمنته من نصوص تهدف إلى التصدي لهذه الجرائم عن طريق مجموعة من التدابير التشريعية والإجرائية الواجب اتخاذها على الصعيد الوطني بالإضافة إلى آليات التعاون الدولي[35].

ومن المهم الإشارة في هذا المقام إلى أنه في ديسمبر 2019، تبنت الجمعية العامة للأمم المتحدة قرارًا بإنشاء اللجنة الحكومية الدولية المعنية بإعداد اتفاقية دولية لمكافحة الجرائم الإلكترونية في إطار الجمعية العامة للأمم المتحدة[36]، وبعد عدة مفاوضات في السنوات التالية لإنشائها فإنه من المتوقع اعتماد المسودة النهائية لاتفاقية الأمم المتحدة للجرائم الإلكترونية من قبل الجمعية العامة في العام 2024 [37].

**ثانياً- التعاون الدولي.**

نظرًا لكون الجرائم المعلوماتية لا حدود إقليمية لها، تشكل مسألة متابعة وحفظ الأدلة المتعلقة بها تحديًا كبيرًا، وذلك لارتباطها باختصاصات قضائية متعددة ذات نظم مختلفة في حفظ الأدلة، لذلك تبرز الحاجة إلى ضرورة التعاون الدولي فيما بين سلطات الدولة التي ارتكبت فيها الجريمة والدولة التي عبر من خلالها النشاط الإجرامي، وسلطات الدولة التي نفذت فيها الجريمة.

ويتخذ التعاون الدولي عدة أوجه يتمثل أهمها في التعاون القضائي، والتعاون في مجال تسليم المجرمين.

**أولًا ـ التعاون القضائي. ينقسم التعاون القضائي إلى التعاون الأمني الدولي، والمساعدة القضائية.**

1- **التعاون الأمني الدولـــي :** ويتم من خلال ثلاثة آليات تتمثل في أ-إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المعلوماتية، حيث تهدف هذه المكاتب إلى تنمية التعاون بين سلطات الدول القضائية في مجال مكافحة الجريمة وملاحقة المجرمين وذلك بتتبع المعلومات وتعميمها بالإضافة إلى تقديم المعونة وتبادل الخبرات عند الاقتضاء[38].

ب-القيام ببعض العمليات الشرطية والأمنية المشتركة، ذلك أن تعقب المجرم المعلوماتي وجمع الأدلة الرقمية وضبطها. والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية بحثًا عن الأدلة، كلها أمور تستدعي القيام ببعض العمليات

الشرطية والأمنية المشتركة، واشتراك الدول فيما بينها للقيام بهذه العمليات من شأنه أن يؤدي إلى صقل مهارات وخبرات القائمين على مكافحة هذه الجرائم والمساهمة بشكل فعال في الحد منها[39].

ج ـ التعاون في إطار المنظمة الدولية للشرطة الجنائية (الإنتربول): وتهدف هذه المنظمة إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها وتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، والجرائم المعلوماتية تعد من أهم الجرائم التي أولتها المنظمة اهتمامًا كبيرًا، حيث أنشأت عام2004 وحدة خاصة لمكافحة الجرائم المعلوماتية، كما قامت بالتعاون مع مجموعة الثمانية (G8) بوضع استراتيجية خاصة بمواجهة هذه الجرائم، وهذا من شأنه كفالة فعالية مكافحة هذا النوع من الإجرام[40].

**2-المساعدة القضائيـــــة:** تعّرف المساعدة القضائية بأنها" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم".

وتتخذ المساعدة القضائية في المجال الجنائي عدة صور منها:

أ- تبادل المعلومات.

ب- نقل الإجراءات.

ج-الإنابة القضائية.[41]

ومما تجدر الإشارة إليه في هذا المقام أن اتفاقية بودابست المعنية بمكافحة الجرائم المعلوماتية قد تناولت في الباب الثالث منها النص على التعاون الدولي كواحد من الوسائل الهامة في مجال التصدي للإجرام المعلوماتي[42].

**ثانيًا- التعاون في مجال تسليم المجرمين.**

يقصد بتسليم المجرمين قيام دولة ما بتسليم شخص موجودًا في اقليمها إلى دولة أخرى بناًء على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها. ويستند نظام تسليم المجرمين على ثلاثة مصادر رئيسية تتمثل في:

1- المعاهدات والاتفاقيات الدولية الثنائية والمتعددة الأطراف بالإضافة للاتفاقيات التي تتضمن أحكام متعلقة بتسليم المجرمين دون أن تكون في حد ذاتها اتفاقية تسليم ومن أبرز الأمثلة على ذلك في نطاق بحثنا اتفاقية بودابست لعام 2001.

2-القوانين الوطنية.

3- العرف الدولي الذي يطبق في حالة عدم وجود اتفاقيات أو قوانين وطنية، وهناك ثلاثة صور للتسليم وفقًا لما جرى به العمل في الممارسة الدولية وهي: (التسليم القضائي، والتسليم الإداري، والتسليم المختلط)[43].

**الفرع الثاني ـ معوقات مكافحة الجرائم المعلوماتية**

تواجه مسألة مكافحة الجرائم المعلوماتية والتصدي لها على الصعيد الدولي عدة معوقات تحد من فعالية الجهود المبذولة في سبيل مواجهتها، وتحول في بعض الأحيان دون الوصول إلى النتائج المرجوة، يتعلق بعضها بسبل المكافحة في إطار الاتفاقيات الدولية، وذلك في مسألة انضمام الدول لها، ومواءمة تشريعاتها الوطنية مع أحكامها بما يكفل وضعها موضع التنفيذ الفعلي، حيث أنه قد يحدث في الممارسة العملية أن تتردد بعض الدول في الانضمام للاتفاقية، ذلك أن الأساس في نشوء وسريان القاعدة القانونية الدولية هي الإرادة، فالاتفاقيات الدولية التي تمثل أهم مصادر القانون الدولي لا تنعقد إلا بإرادة الدول ورضاها في الانضمام إليها[44]، بالتالي لا يوجد التزام على الدولة يجبرها على الانضمام للاتفاقية، وطالما أنها غير طرف فيها فلا ترتب عليها أي : التزام استنادًا الى مبدأ نسبية أثر المعاهدات، يستثنى من ذلك المعاهدات الشارعة التي تقر قواعد آمرة من شأنها حماية حقوق الإنسان والحفاظ على السلم والأمن الدوليين أو تلك التي تعنى بتقنين أعراف دولية.

وقد تنضم الدولة للاتفاقية ـ والتي من بينها الاتفاقيات المعنية بمكافحة الجرائم المعلوماتية موضوع بحثنا ـ إلا أنها لا تلتزم بتنفيذها ، وموائمة تشريعاتها الوطنية مع أحكامها[45]،لعل السبب الرئيسي وراء ذلك يكمن في غياب السلطة التي تمتلك إلزام الدول بتنفيذ الاتفاقيات الدولية أسوة بتلك الموجودة على الصعيد الوطني.

ويتعلق البعض الأخر من المعوقات والصعوبات بالتعاون الدولي، ويتمثل أبرزها فيما يلي بيانه:

1- عدم وجود اتفاق بين جميع الدول حول ماهية الجرائم المعلوماتية، ومتى نكون أمام جريمة من عدمه، فما يكون مباحًا في دولة ما، قد يكون مجرمًا وغير مباحًا في دولة أخرى، ويعود بطبيعة الحال السبب في ذلك إلى اختلاف العادات والتقاليد والديانات والثقافات من مجتمع لآخر وانعكاس الأمر على السياسة التشريعية في الدولة(46)، ويرى البعض أنه من الممكن مواجهة هذه الإشكالية من خلال إبرام اتفاقيات دولية تضع وتحدد الإطار العام لمكافحة الجرائم المعلوماتية مع مراعاة مواءمة الدول لتشريعاتها الوطنية مع أحكامها، وإدخالها حيز التنفيذ الفعلي(47).

2- تنوع واختلاف النظم القانونية الإجرائية، فبعض طرق التحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى، أو قد لا تسمح بإجرائها كالمراقبة الإلكترونية، وطرق جمع الاستدلالات بالتجسس المأذون به من السلطات المختصة، قد يكون أمرًا متاحًا وقانونيًا في دولة ما في حين يعتبر من قبيل التعدي على الحقوق والحريات العامة وبالتالي غير مشروع في دولة أخرى(48).

وبخصوص هذه المعضلة نجد أن الكثير من الوثائق الدولية تشجع الدول الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة وهذا من شأنه التخفيف من حدة الاختلاف الكبير بين النظم القانونية الإجرائية، ويساهم في الدفع نحو التعاون الدولي بشكل فعال(49)، مثال ذلك ما نصت عليه المادة 29 من اتفاقية بودابست التي " أجازت لأي دولة طرف فيها أن تطالب دولة طرف أخرى أو أن تأمرها بالتعجيل في حفظ بيانات مخزنة بواسطة نظام كمبيوتر، يوجد على أراضي الدولة الطرف الأخرى، والتي تنوي أن تقدم بشأنها طلبًا بالمساعدة المتبادلة من اجل البحث عن بيانات، النفاذ إليها، مصادرتها، تأمينها أو كشفها".

3- تنازع الاختصاص القضائي فيما بين الدول، حيث إنه ولكون أن الجرائم المعلوماتية عابرة لحدود الدولة الواحدة، قد يحدث على سبيل المثال أن تقع الجريمة في إقليم دولة ما من قبل شخص أجنبي وتنتج آثارها في نطاق إقليم دولة أخرى، فهنا في هذه الحالة نكون أمام تنازع إيجابي في الاختصاص ما بين دولة جنسية الجاني استنادًا إلى مبدأ الاختصاص الشخصي، والدولة التي وقعت الجريمة فوق إقليمها استنادًا إلى مبدأ الإقليمية، والدولة التي هددت مصالحها وأمنها وسلامتها على أساس مبدأ العينية(50)، وهنا توجد فرضيتان لحل هذه الإشكالية تتمثل الأولى في إبرام اتفاقيات دولية ثنائية وجماعية يتم من خلالها توحيد وجهات النظر بخصوص قواعد الاختصاص القضائي،

مع ضرورة اهتمام الدول بتطوير وتحديث منظومة قوانينها الجنائية الوطنية بما يتلائم ويتناسب مع التطور الهائل الذي يشهده مجال تقنية المعلومات والاتصالات.

أما الفرضية الثانية تتمثل في اعتبار الجرائم المعلوماتية من الجرائم الدولية، وبالتالي ينطبق عليها الاختصاص القضائي العالمي، وذلك بإعطاء الحق لكافة الدول بملاحقة مرتكبي هذا النوع من الإجرام بصرف النظر عن جنسيتهم، أو الدولة التي ارتكبت في إقليمها الجريمة، أو التي تضررت منها[51].

4- الصعوبات التي تواجه التعاون القضائي الدولي، تحديدًا فيما يتعلق بالإنابة القضائية لتعارضها مع مبدأ السيادة، والولاية القضائية، فكل دولة عادة ما تقوم من خلال جهازها القضائي بالفصل في كل الجرائم الواقعة فوق إقليمها الأمر الذي يشكل عائقًا قد يحول دون التعاون القضائي بين الدول في مكافحة الجرائم المعلوماتية، إلا أن هذه المسألة غالبًا ما يتم حلها من خلال الاتفاقيات الدولية المبرمة المعنية[52]، أما فيما يتعلق بإشكالية بطء إجراءات المساعدات القضائية مقارنة مع ما تتسم به الجرائم المعلوماتية من سرعة في أسلوب ارتكابها، فإن هذا يتطلب إيجاد آلية تتسم بالسرعة في استكمال الإجراءات المتعلقة بالمساعدات القضائية كتعيين سلطة مركزية، أو إنشاء قنوات اتصال بين السلطات المختصة تكفل استعمال وسائل اتصال عاجلة[53]، وهذا ما نصت عليه وأكدته نصوص المادتين (25، 27)، من اتفاقية بودابست.

5- الإشكالية المتعلقة بتسليم المجرمين، حيث يُعد شرط التجريم المزدوج من أهم الشروط الواجب توافرها في نظام تسليم المجرمين فيما بين الدول[54]، وقد يقف هذا الشرط عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية إذا كان قانون الدولة المطلوب منها التسليم لا يجرم هذه الجرائم، لذلك في هذا الإطار نجد أن التطورات التشريعية الخاصة بتسليم المجرمين ركزت على تخفيف التطبيق الصارم لهذا الشرط من خلال إدراج أحكام عامة في الاتفاقيات ذات العلاقة من شأنها أن تكفل ذلك إما بسرد الأفعال التي تتطلب أن تجرم كجرائم، أو باعتبارها أفعال مخلة بمقتضى قوانين الدولتين معًا، أو السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة[55].

مما سبق بيانه يتضح لنا أن من أهم وسائل مكافحة الجرائم المعلوماتية هي الاتفاقيات الدولية، حيث إنه من شأنها تذليل العديد من المعوقات والصعوبات التي تواجه الجهود المبذولة في التصدي لها، وتكفل بالتالي فعالية التعاون الدولي.

ونشير أخيراً إلى أنه كل الآليات والإجراءات والوسائل المتخذة في سبيل مكافحة هذه الجرائم تساهم فقط في الحد منها قدر الإمكان وليس القضاء عليها بشكل نهائي، فالجريمة موجودة بوجود المجتمعات البشرية.

## الخاتمة:

من خلال دراسة الموضوع توصلت إلى النتائج والتوصيات التالي بيانها:

### أولًا- النتائج:

1- تعد الجرائم المعلوماتية من أخطر الجرائم التي تهدد أمن واستقرار كافة الدول في عصرنا الحديث، لكونها عابرة للحدود، ليس من السهل اثباتها، يرتكبها أشخاص على درجة عالية من الذكاء والاحتراف.

2- الجريمة المعلوماتية، جريمة متطورة من الصعب حصر أنواعها، أو التنبؤ بأساليب ووسائل ارتكابها.

3- تعد الاتفاقيات الدولية من أهم وسائل مكافحة الجرائم المعلوماتية ، والتصدي لها على الصعيد الدولي ، وهذا ما تنبّه له أعضاء المجتمع الدولي، لذلك تبنت الجمعية العامة في ديسمبر 2019 م ، قرارًا بإنشاء لجنة حكومية دولية معينة بإعداد اتفاقية دولية لمكافحة الجرائم المعلوماتية من المتوقع اعتمادها في 2024.

4- يعترض الاتفاقيات الدولية العديد من المعوقات التي تحول دون فعاليتها في تحقيق الغاية المتوخاة من إبرامها يتمثل أهمها في مسألة عدم انضمام الدول ومواءمة تشريعاتها الوطنية مع أحكامها.

5- بالرغم من أهمية الدور الذي يؤديه التعاون الدولي في مكافحة الجرائم المعلوماتية، إلا أنه تواجه العديد من الإشكاليات التي تحد من نجاعته في تحقيق النتائج المرجوة يتمثل أهمها في مسألة عدم اتفاق الدول حول تحديد ماهية الجرائم المعلوماتية، وتنوع واختلاف النظم القانونية الإجرائية، وتنازع الاختصاص القضائي، وإشكالية تسليم المجرمين.

### ثانيًا- التوصيات:

1- أوصي بضرورة الانضمام إلى الاتفاقيات الدولية المعنية بمكافحة الجرائم المعلوماتية وتحدد الإطار العام لها، ووضع أحكامها موضع التنفيذ الفعلي بما يكفل توحيد الجهود والرؤى فيما بين الدول في مجال التصدي لها.

2- تعزيز التعاون الدولي، وإنشاء قنوات ومراكز اتصال مباشر بين السلطات المختصة في الدول لضمان سرعة وتيسير إجراءات المساعدة القضائية.

3- أناشـــد بضرورة العمل على رفع مستوى الوعي المجتمعي بمخاطر الجرائم المعلوماتية، ونشر الثقافة حول برامج الحماية الكفيلة بتوقي أضرارها قدر الإمكان.

4- أوصي بضرورة عقد ندوات وورش تدريبية للرفع من كفاءة جهات التحقيق بما يضمن إلمامهم بتكنولوجيا المعلومات ويساهم بالتالي في زيادة قدرتهم على الكشف عن هذه الجرائم وإثباتها.

## الهوامـــــــــــش :

1- لقد اختلف فقهاء القانون في المصطلحات المستخدمة للدلالة على هذا النوع من الإجرام، فهناك من يستخدم مصطلح الجرائم الإلكترونية وهناك من يطلق عليها تسمية الجرائم المعلوماتية، في حين يستخدم آخرون مصطلح جرائم الكمبيوتر= والأنترنت للدلالة عليها، عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، بحث منشور بمجلة مركز دراسات الكوفة – العراق، العدد السابع، 2008، ص112، منشور الكترونياً على الرابط الثاني:
journat.uokufa.edu.iq

2- تعددت الجهود الفقهية الرامية إلى تعريف الجريمة المعلوماتية، فهناك من يعرفها على أنها " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية لازما لارتكابه من ناحية ولملاحقته والتحقيق فيه من ناحية أخرى"، ويعرفها البعض الأخر على أنها " كل سلوك سلبي أو إيجابي يتم بموجبه الاعتداء على برامج المعلومات للاستفادة منها بأي صورة كانت" للمزيد يمكن القارئ الرجوع إلى سليمان أبو النمر، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، كلية الحقوق والعلوم السياسية/جامعة محمد خيضر بسكرة، رسالة ماجستير، 2021، ص2-7.

3- خالد ممدوح إبراهيم، الجرائم المعلوماتية، مصر، دار الفكر الجامعي، الطبعة الثانية، 2019، ص77، 78.

4- ياسمينة بو نعارة، الجريمة الإلكترونية، بحث منشور بمجلة المعيار بجامعة الأمير عبد القادر للعلوم الإسلامية، العدد39، 2015،ص281، منشور إلكترونيًا على الرابط التالي:http//ojs.univ.emir-constantine.edu.dz

5- عادل يوسف عبدالنبي الشكري، مرجع سبق ذكره، ص116.

6- شريهان ممدوح حسن، الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي، بحث منشور بالمجلة الإلكترونية الشاملة متعددة المعرفة، العدد الواحد والعشرون، 2020، ص9، بحث منشور إلكترونياً على الرابط التالي: mecsj.com/ar/

7- سليمان أنو نمر، مرجع سابق، ص11.

8- بن جدو بن علية ودرار عياش، الآثار الاقتصادية للجريمة الالكترونية، بحث منشور بمجلة أبحاث اقتصادية معاصرة، المجلد5، العدد1، 2022، ص565-566، منشور الكترونياً على الرابط التالي:
asjp.cerist.dz/en/article/184351

9- الموقع الإلكتروني للعربية: alarabiya.net

10- لمعرفة المزيد من المعلومات يمكن القارئ الرجوع إلى ياسمينة بونعارة، مرجع سبق ذكره، ص286-289.

11- لمعرفة المزيد حول سمات وأصناف المجرم المعلوماتي يمكن للقارئ الرجوع إلى يونس نفيد، المكافحة التشريعية لبعض صور الجرائم المعلوماتية وأصناف المجرم المعلوماتي، بحث منشور بالمجلة العربية للدراسات الأمنية، المجلد 38، العدد2، 2022، ص139-140، منشور الكترونيًا على الرابط التالي: journals.nauss.edu.sa . رامي متولي القاضي، الجرائم المعلوماتية وطرق مواجهتها، بحث تمت المشاركة به بمؤتمر تأمين المعلومات والدليل الرقمي وكيفية اثباته في الجرائم

الإلكترونية المنعقدة خلال فترة (15-16 ديسمبر 2010)، ص9-11، منشور الكترونيًا على:http//www.researchgate.net

12- خالد ممدوح إبراهيم، مرجع سبق ذكره، ص84-85، الأخنش نورة أمينة والعيداني محمد، الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية، بحث منشور بمجلة القانون والعلوم البيئية، المجلد2، العدد2، 2023، ص533، منشور الكترونيًا على الرابط التالي: https://www.researchgate.net

13- كوثر حازم سلطان، موقف القانون والقضاء من الجريمة الإلكترونية (دراسة مقارنة)، بحث منشور بمجلة كلية التربية الأساسية، المجلد22، العدد96، 2016، ص974، منشور إلكترونيًا على الرابط التالي: https://www.researchgate.net

14- حسبنا أن نشير في هذا الإطار إلى أن المشرع الليبي في القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية ميز بين العقوبة المقررة على مجرد الدخول غير المشروع، والعقوبة المقررة على الدخول غير المشروع بقصد إلغاء أو حذف أو إضافة أو تدمير أو تعطيل عمل النظام المعلوماتي، وأيضاً العقوبة المقررة إذا نجم عن الدخول إعاقة عمل النظام المعلوماتي أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني أو إفساد محتوياتهم، فالعقوبة المقررة لمجرد الدخول هي الحبس مدة لا تزيد عن سنة أو غرامة لا تقل عن 100 ولا تزيد على 500 دينار أو العقوبتين معًا، بينما تكون العقوبة في الحالة الثانية هي الحبس مدة لا تقل عن سنة وغرامة لا تقل عن 500 دينار ، ولا تزيد على 5000 دينار، وتكون العقوبة في الحالة الأخيرة أي إذا ترتب على الدخول إحداث إعاقة أو تعطيل أو إفساد لمحتويات النظام المعلوماتي أو الشبكة المعلوماتية هي السجن والغرامة التي لا تقل عن 10000 دينار، مما يعني أنه اعتبر ذلك من قبيل الظروف المشددة. للمزيد يمكن للقارئ الرجوع إلى نصوص القانون منشور إلكترونيًا في المجمع القانوني الليبي على الرابط الليبي:
https://lawsociety.ly

15- نايرى عائشة، الجريمة الإلكترونية في التشريع الجزائري، كلية الحقوق والعلوم السياسية/ جامعة ادرار، رسالة ماجستير، 2017، ص28.

16- رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في أحكام القانون (175) لسنة 2018 مقارنًا بالمواثيق الدولية والتشريعات المقارنة، بحث منشور بمجلة البحوث القانونية والاقتصادية(المنصورة)،العدد2021،75،ص1033.

17- للمزيد حول ذلك يمكن للقارئ الرجوع إلى: شريهان ممدوح حسين، مرجع سبق ذكره، ص12-13، رامي متولي القاضي، الجرائم المعلوماتية وطرق مواجهتها، مرجع سبق ذكره، ص6.

18- فريحة حسين، الجرائم الإلكترونية والانترنت، بحث منشور بمجلة المعلوماتية، العدد36، 2011، ص6-7، منشور إلكترونيًا على موقع دار المنظومة على الرابط التالي:
https://search.mandumah.com

19- نايري عائشة، مرجع سبق ذكره، ص25.

20- الجهني منصور بن صالح، الجرائم المعلوماتية أنواعها وصفات مرتكبيها، بحث تمت المشاركة به في المؤتمر الدولي الرابع للعلوم الاجتماعية بالكويت، 2019، ص5، منشور إلكترونيًا على موقع دار المنظومة التالي بيانه:https://www.mandumah.com

21- فريحة حسين، مرجع سبق ذكره، ص4-6.

22- بن جدو بن علية ودرار عياش، مرجع سبق ذكره، ص564.
23- ياسمينة بونعارة، مرجع سبق ذكره، ص300.
24- لقد نص القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية على هذه الأنواع في المواد (37، 45).
25- للمزيد حول ذلك يمكن للقارئ الرجوع إلى أحمد الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختارة، بحث منشور بمجلة كلية الاقتصاد والعلوم السياسية/ الجامعة المصرية الروسية، المجلد24، العدد4، 2023، ص150 وما بعدها، منشور إلكترونيًا على الرابط التالي: https://www.rescarehgate.net
26- محمود محمد شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الأنترنت، بحث منشور بمجلة البحوث القانونية والاقتصادية – جامعة المنوفية، المجلد 54، العدد3، 2021، ص538، منشور إلكترونيًا على الرابط التالي:
https://jslem.journals.ekb.eg
27- معاهدة الويبو بشأن حق المؤلف لعام 1996، منشورة إلكترونيًا على الرابط التالي:
https://www.wipo.int
28- اتفاقية برن لحماية المصنفات الأدبية والفنية، منشورة الكترونياً على نفس الرابط السابق ذكره.
29- شريهان ممدوح حسين، مرجع سبق ذكره، ص20.
30- معاهدتي الويبو بشأن حق المؤلف والأداء والتسجيل الصوتي لعام 1996، كلاهما منشور على ذات الرابط الإلكتروني:
https://www.wipo.int
31- عبدالسلام مخلوفي، اتفاقية حماية حقوق الملكية الفكرية المرتبطة بالتجارة TRIPS أداة لحماية التكنولوجيا أم لاحتكارها، بحث منشور بمجلة اقتصاديات شمال أفريقيا، العدد3،بدون ذكر تاريخ النشر، ص118، منشور إلكترونيًا على الرابط التالي:
https://www.univ-chlef.dz
32- نص اتفاقية تريبس منشورة إلكترونيًا على الرابط التالي: https://customs.gov.jo
33- دراجي شهرزاد وجديدي ضياء الدين رمضان، مكافحة الجريمة السيبرانية على المستوى الدولي، بحث تمت المشاركة به في الملتقى الدولي الافتراضي المعنون بالإجرام المنظم العابر للحدود بين المكافحة الدولية والتعاون القضائي 2023، ص2، منشور الكتروني: على: https://www.researchgate.net
34- قطاف سليمان وبوقرين عبد الحميد، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، بحث منشور بالمجلة الاكاديمية للبحوث القانونية والسياسية، المجلة 6، العدد1، 2022، ص337-338. منشور إلكترونيًا على الرابط التالي:
https://www.asjp.cerist.dz
35- نص الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، منشورة إلكترونيًا على الرابط التالي:
https://rm.coe.int
36- الأمم المتحدة، الجمعية العامة، الدورة الرابعة والسبعون، وثيقة رقم: A/RE5/74/247

37- الجدول الزمني لاتفاقية الأمم المتحدة للجرائم الإلكترونية، منشور إلكترونيًا على الرابط التالي: htpps://www.eff.org

38- قزران مصطفى وزرقين عبد القادر، الآليات الدولية لمكافحة الجريمة الإلكترونية، بحث منشور بمجلة صوت القانون، المجلد8، العدد2، 2022، ص1226، منشور إلكترونيًا على الرابط التالي: https://www.asjp.cerist.dz/en/article/194290

39- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، بحث منشور بموقع المنشاوي للدراسات والبحوث، 2007، ص10، منشور إلكترونيًا على الرابط التالي: https://www.minshawi.com

40- ولهي المختار، فعالية التعاون الدولي في مواجهة الجرائم المعلوماتية، بحث تم المشاركة به في الملتقى العلمي الوطني حول مواجهة الجرمية المعلوماتية في ضوء التشريعات الجزائية بجامعة محمد بوضياف المسيلة بالجزائر، 2023،ص3، منشور إلكترونيًا على الرابط التالي: https://www.researchgate.net

41 - للمزيد حول التعاون القضائي الدولي يمكن للقارئ الرجوع إلى حشيفة عبد الهادي، التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، كلية الحقوق والعلوم السياسية/ جامعة زيان عاشور-الجلفة-بالجزائر، رسالة ماجستير، 2020، ص41 وما بعد.

42- للمزيد حول تدابير مكافحة الجرائم المعلوماتية في إطار اتفاقية بودابست يمكن للقارئ الرجوع إلى مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، بحث منشور بمجلة الواحات للبحوث والدراسات، المجلد12، العدد2، 2019، ص713-726، منشور إلكترونيًا على الرابط التالي: https://www.asjp.cerst.dz/ew/article/108893

43- حسين بن سعيد بن سيف الغافري، مرجع سبق ذكره، ص15 وما بعدها.

44 - للمزيد حول ذلك يمكن للقارئ الرجوع إلى علي ضوي، القانون الدولي العام، ليبيا، بدون ذكر الناشر، الطبعة الخامسة،2013،ص58وما بعد.

45 - للمزيد حول ذلك يمكن للقارئ الرجوع إلى محمد خالد برع، المعاهدات الدولية وآليات توطينها في القانون الوطني، لبنان، منشورات الحلبي الحقوقية، الطبعة الأولى، 2017.

46- ولهي المختار، مرجع سبق ذكره، ص7-8.

47- عباس أحمد المبارك، الجرائم الإلكترونية وسبل مواجهتها على المستوى الوطني والدولي، بحث تمت المشاركة به في ملتقى الدكتوراه الدولي متعدد الاختصاصات بجامعة الشهيد حمة لخضر الوادي بالجزائر، 2020، ص7، منشور إلكترونيًا على الرابط التالي: https://www.researchgate.net

48- قزران مصطفى وزرقين عبدالقادر، مرجع سبق ذكره، ص1236-1237.

49- حسين بن سعيد بن سيف الغافري، مرجع سبق ذكره، ص56.

50- سليمان أبو نمر، مرجع سبق ذكره، ص46.

51- ولهي المختار، مرجع سبق ذكره، ص11.

52- عباس أحمد المبارك، مرجع سبق ذكره، ص6-7.

53- قرزان مصطفى وزرقين عبدالقادر، مرجع سبق ذكره، ص1239.

54- حشيفة عبدالهادي، مرجع سبق ذكره، ص51.

55 - حسين بن سعيد بن سيف الغافري، مرجع سبق ذكره، ص59.