جامعة محمد خيضر بسكرة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة ماستر

الميدان : الحقوق والعلوم السياسية
الفرع: حقوق
التخصص: قانون دولي عام.

رقم: 191332124152
141435038447

إعداد الطالب (ة):
اسم ولقب الطالب
سليمان أبو نمر
يوسف بوكشريدة
يوم: تاريخ الإيداع

عنوان المذكرة

مكافحة الجريمة المعلوماتية في إطار القانون الدولي

لجنة المناقشة:

اسم ولقب الأستاذ **أمينة سلام**	رتبة أستاذ	جامعة بسكرة	رئيسا
اسم ولقب الأستاذ	رتبة أستاذ	جامعة بسكرة	مشرفا ومقررا
اسم ولقب الأستاذ	رتبة أستاذ	جامعة بسكرة	مناقشا

السنة الجامعية : 2020 - 2021

بسم الله الرحمن الرحيم

"وَتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَى وَلَا تَعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ"

{المائدة: آية 2}

الإهداء

- إلى كل من علمني حرفا في هذه الدنيا الفانية.
- إلى أمي وأبي "حفظهما الله ورعاهما".
- إلى وطني الثاني الجزائر وشعبها "حفظهم الله".
- إلى أرواح شهداء فلسطين والجزائر "رحمهم الله".
- الي زميلتي سارة وخيرة "حفظهما الله"

الإهداء

مرت قاطرة البحث بكثير من العوائق، ومع ذلك حاولت أن اتخطاها بثبات بفضل من الله ومنه

إلى أبي وإخوتي وأصدقائي فلقد كانوا بمثابة العضد والسند في سبيل استكمال البحث.

إلى كل أفراد عائلتي بدون استثناء.

أهدي لكم بحث تخرجي داعيا المولى عز وجل أن يطيل في أعماركم ويرزقكم بالخيرات.

يوسف

شكر و تقدير

قال تعالى (ومن يشكر فإنما يشكر لنفسه) {لقمان :12}

وقال رسوله الكريم: "من لم يشكر الناس، لم يشكر الله عز وجل"

نحمد الله تعالى حمدا كثيرا طيبا مباركة ملئ السماوات والأرض على ما أكرمنا به من إتمام هذه الدراسة التي نرجو أن تنال رضاه.

ثم نتوجه بجزيل الشكر وعظيم الامتنان إلى كل من:

*الدكتورة الفاضلة / سلام أمينة، حفظها الله وأطال في عمرها، لتفضلها الكريم بالإشراف على هذه الدراسة، وتكرمها بنصحنا وتوجيهينا حتى إتمام هذه الدراسة.

*أساتذة كلية الحقوق الكرام، لما كان لهم من نصح وتوجيه.

مقدمة :

تعتبر الجريمة ظاهرة قديمة ارتبطت بوجود الإنسان البدائي على الأرض، فلا يمكن تصور وقوع جريمة بغير إنسان، وكما أنها تطورت وازداد انتشارها بتطور هذا الإنسان على مر العصور، وقد شهد عصرنا الحالي تطوراً غير مسبوق في الاعتماد على التقنيات الحديثة، وأصبح الحاسوب والبرمجيات ركيزة أساسية لأهداف التطور في كافة مجالات الحياة، بما فيها من أنشطة مختلفة سواء أكانت اقتصادية، علمية، تجارية، عسكرية، أم اجتماعية...إلخ، وذلك على المستوى الفردي والمؤسسي والمجتمعي والدولي.

وعلى الرغم مما تحمله هذه التقنيات الحديثة من تسهيلات وإمكانات هائلة، يسرت على الإنسان الوقت والجهد والمال، فإن البعض قد أساء استخدامها، وهو ما أدى إلى ظهور نمط جديد من الجرائم، وهي ما سمي بالجرائم المعلوماتية، والتي تختلف في شكلها ومضمونها ووسائلها عن الجريمة بشكلها التقليدي. ويستمد هذا النوع المستحدث من الإجرام نشاطه من الإمكانات الهائلة للحاسوب والبرامج، وتطور شبكة الإنترنت، والتطور الثقافي والعلمي فى التعامل مع التكنولوجيا الحديثة بمختلف أنواعها. وتتعاظم المخاطر الناتجة عن الجرائم المعلوماتية لقدرتها الفائقة على التطور والانتشار وتخطيها للحدود الجغرافية، مستغلة في ذلك ما أتاحته شبكة الإنترنت من انفتاح معلوماتي على العالم بأسره.

وككل ثمين فالمعلومات –دائماً –في خطر، ولذلك لم يكن غريباً أن يصبح أمن المعلومات هاجسًا للجميع، من دول ومنظمات وشركات وأشخاص، لاسيما أن الجريمة تطورت تطوراً أدى إلى تعريض أمن المعلومات على شبكات نظم المعلومات والإنترنت للخطر الشديد. وتزايدت مخاطر هذه الجرائم على المستوى الدولي والإقليمي والمحلي بسبب وجود قصور في التعامل مع هذه الجرائم ومواجهتها، وترجع أسباب القصور في التعامل مع الجرائم المعلوماتية إلى المعوقات التي يواجهها المحقق الجنائي، المنوط به كافة الإجراءات الأمنية والقانونية في التعامل مع هذه الجرائم، بدءاً من تلقى البلاغات حتى الضبط ومثول المتهم أمام العدالة لمحاكمته محاكمة عادلة ،ونظرا لخطورة والطبيعة الخاصة بهذه الجرائم بذلت جهود دولية في إطار المنظمات الدولية عبر عقد العديد من المؤتمرات التي أنتج العديد من المعاهدات الدولية الخاصة بمكافحة الجرائم المعلوماتية ، رغم الجهود الدولية المبذولة لمكافحة هذه الجرائم إلا إن هناك العديد من الصعوبات والتحديات التي تواجه التعاون الدولي في مجال

مكافحة هذه الجرائم نظرا للعديد من العوامل، لعل من أبرزها الطبيعة الخاصة للجرائم المعلوماتية وتميزها عن الجرائم التقليدية سواء من حيث وسائل ارتكابها أو من حيث فاعلها أومن حيث الضحية .

_أسباب اختيار الموضوع :-

لقد جاء اهتمام الباحث بهذا الموضوع لاعتبارات ذاتية و موضوعية تتمثل في :

أولا/ الأسباب الذاتية وهي كما يلي:

أ-الرغبة في معرفة مدى التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، وأهم مجالاته بين الدول.

ب-الرغبة في معرفة مدى تطبيق قواعد القانون الدولي وقواعد مكافحة الجرائم المعلوماتية خاصة في أرض الواقع مقارنة بالنصوص القانونية.

ج – الرغبة في الدراسة ميدان مكافحة الجرائم المعلوماتية بغية الوقوف على أهم النصوص القانونية المتعلقة بمكافحة الجريمة المعلوماتية.

ثانيا/أسباب الموضوعية تتمثل في:

أ-إزدياد متسارع للجرائم المعلوماتية في ظل الثورة التكنولوجية الهائلة في ظل قصور التشريعات الوطنية في مكافحة الجرائم المعلوماتية.

ب-الرغبة في التعرف على مضمون المكافحة للجرائم المعلوماتية المقررة بموجب الاتفاقيات الدولية.

ج أهمية موضوع مكافحة الجرائم المعلوماتية بوصفه ضمانة لحماية الأمن المعلوماتي الدولي.

د-الرغبة في الوقوف على أوجه القصور ومحاولة إيجاد حلول تحسن

المكافحة الدولية للجرائم المعلوماتية.

- أهمية الموضوع:

يكتسب هذا الموضوع الذي يحمل عنوان (**مكافحة الجرائم المعلوماتية في ظل القانون** الدولي) أهميته

من طبيعة الظاهرة التي يتناولها، والذي يعد من المواضيع بالغة أهمية في الوقت الراهن، وتتجلى أهميته في النقاط الآتية:

-الطبيعة الخاصة للجرائم المعلوماتية التي ميزتها عن الجرائم التقليدية سواء من حيث فاعلها او محلها أو مسرح الجريمة.

- تعتبر الجرائم المعلوماتية من الجرائم عابرة الحدود فقد يكون فاعلها في دولة والضحية في دولة أخرى.

-تعتبر الجرائم المعلوماتية من الجرائم المستحدثة التي تعتمد على التقنيات الحديثة، التي ظهرت في مطلع القرن العشرين.

-خطورة هذه الجرائم وآثارها السلبية على الأفراد والدول، في ظل قصور التشريعات الوطنية عن مواكبة هذه التطورات في عالم الجريمة مما يتطلب تعاون دولي لمكافحة هذا النوع من الجرائم المستحدثة.

-أظهرت الدراسات العلمية التي أجريت حول هذه الجرائم ازدياد عددها بشكل مطرد، واتساع مجالاتها ليشمل أمور حساسة تتعلق بأمن وسلم الدول.

- إفلات العديد من مرتكبي هذه الجرائم من العقاب نظرا للغياب تقنين خاص بهذه الجرائم، وحتى إن وجد هذا التقنين فإنه يعاني من قصور نظرا لتميز هذه الجرائم عن الجرائم التقليدية.

أهداف الموضوع:

1_ يهدف الموضوع الى التعريف بمكافحة الجرائم المعلوماتية باعتبارها إحدى وسائل القانون الدولي العام والتي تسهم في تحقيق الأمن والسلم الدوليين.

2. يهدف البحث إلى إبراز الدور الهام للتعاون الدولي في حل القضايا والأزمات الدولية.

3. ضمان عدم زعزعة الاستقرار والأمن الدوليين والحد من انتشار ثقافة العنف بين الشعوب.

4_إبراز أهم الصعوبات والتحديات التي تواجه التعاون الدولي في مجال مكافحة الجرائم المعلوماتية وسبل التغلب عليها.

الدراسات السابقة:

هناك جملة من الدراسات التي تناولت في فحواها الإشارة إلى مكافحة الجريمة المعلوماتية، وهذا التناول كان يقتصر على الناحية الاجرائية والجنائية الوطنية مع إشارة إلى الجانب الدولي، حيث لم يتم التركيز على مكافحة الجرائم المعلوماتية في القانون الدولي كموضوع مستقل.

فعلى حد علمنا أن هناك ندرة في الدراسات المتخصصة بمكافحة الجرائم المعلوماتية في القانون الدولي في الجامعات الجزائرية أن لم تكن منعدمة، فجل الدراسات تناولت الجرائم المعلوماتية على الصعيد الوطني ومنها:

1-رسالة ماستر للأستاذة فريال لعاقل بعنوان الجريمة المعلوماتية في ظل التشريع الجزائري حيث ركزت الباحثة مجال دراستها على الناحية الاجرائية والجنائية للجرائم المعلوماتية في التشريع الجزائري، دون أي إشارة إلى الجانب الدولي في مجال مكافحة الجرائم المعلوماتية.

2-رسالة ماستر للأستاذ يوسف جفال بعنوان التحقيق في الجرائم المعلوماتية، حيث ركز الباحث موضوع دراسته على إجراء من إجراءات مكافحة وإثبات الجرائم المعلوماتية على الصعيد الوطني.

وعند الرجوع إلى الدراسات العربية نجد كتاب بعنوان إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها لأستاذ عادل خراشي، حيث يوضح المؤلف أهم إشكاليات التي تعيق التعاون الدولي في مكافحة الجرائم المعلوماتية و يقترح حلول لأجل التغلب عليها ، لكن نجد أن هذا الكتاب لم يواكب التطور الحاصل في العالم الجريمة المعلوماتية حيث اقتصرت الحلول على المسائل التقليدية فيما يتعلق بتسليم المجرمين وتدريب الأجهزة الأمنية ،دون التركيز على حلول تتعلق بطبيعة الجريمة بحد ذاتها.

ونحن من جانبنا سنحاول في دراستنا لهذا الموضوع التعرف على التعاون الدولي لمكافحة الجرائم المعلوماتية، والتعرف على أهم الصعوبات والتحديات التى تواجه التعاون الدولي لمكافحة الجرائم المعلوماتية وإيجاد حلول تسهم في الحد من هذه الظاهرة على الصعيد الوطني والدولي.

الإشكالية:

ما مدى فاعلية التعاون الدولي في مكافحة الجرائم المعلوماتية؟

المنهج المتبع:

حرصنا في هذه الدراسة و نزولا عند موجبات البحث العلمي، على اختيار منهج يتناسب مع طبيعة البحث القانونية التي تفرض علينا نوعية المنهج المتبع، لذا اخترنا منهجا يلم بدراسة الموضوع بكل جوانبه، و هو المنهج الوصفي التحليلي الذي يهدف إلى بيان ماهية التعاون الدولي في مكافحة الجرائم المعلوماتية من خلال بيان ماهية هذه الجرائم، وأهم مجالات التعاون الدولي في مكافحتها ، وكذا بيان أهم التحديات التي تواجه المكافحة عل الصعيد الوطني والدولي ،وكذا بيان الحلول لها، وذلك من خلال الرجوع الى المراجع القانونية المتخصصة ،وكذا الاتفاقيات الدولية ذات صلة.

-تقسيمات الموضوع

بهدف الإجابة على إشكالية البحث قسمنا موضوع الدراسة إلى فصلين، فالفصل الأول بعنوان ماهية التعاون الدولي لمكافحة الجريمة المعلوماتية والذي من خلاله تم التطرق إلى مبحثين: الأول يتطرق الى ماهية الجريمة المعلوماتية ، أما الآخر يتطرق الى أهم مجالات التعاون الدولي في مكافحة لجريمة المعلوماتية، ثم يأتي بعد ذلك الفصل الثاني تحت عنوان تحديات التعاون الدولي في مكافحة الجريمة المعلوماتية وسبل معالجتها، والذي من خلاله تم التطرق الى مبحثين : الأول يتطرق الى تحديات التعاون الدولي لمكافحة الجريمة المعلوماتية على المستوى الوطني والدولي، أما آخر يتطرق الى سبل معالجتها على المستوى الوطني والدولي، وأخيرا خاتمة تضمنت أهم النتائج والتوصيات التي خلص إليها البحث.

-صعوبات الدراسة:

واجهنا عدة صعوبات في إعداد الدراسة، ولعل من أهمها ما يلي:

1-ندرة المراجع المتخصصة بمكافحة الجرائم المعلوماتية في ضوء القانون الدولي، فجل المراجع تتطرق الى هذا موضوع على المستوى الوطني.

2-عدم ملائمة البيئة الاجتماعية المحيطة لإعداد الدراسة بشكل مناسب.

3-ظروف فيروس كورونا التي أثرت على تكوين الباحث خلال هذه الفترة.

الفصل الأول: التعاون الدولي في مجال مكافحة الجريمة المعلوماتية

لقد أثبت الواقع العملي أن الدولة لا تستطيع بجهودها المنفردة القضاء على الجريمة المعلوماتية مع هذا التطور الملموس والمذهل في كافة ميادين الحياة، لذلك أصبحت هناك حاجة ماسة الى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة، وتتعاون من خلاله الاجهزة المختلفة في الدول خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة، بالإضافة الى تعقب المجرمين الهاربين من وجه العدالة. وعلى ضوء ذلك سنقسم الفصل الأول إلى مبحثين، الأول بعنوان ماهية الجرائم المعلوماتية، أما المبحث الثاني فسيكون تحت عنوان مجالات التعاون الدولي لمكافحة الجريمة المعلوماتية.

المبحث الأول:

ماهية الجريمة المعلوماتية

تعد الجريمة المعلوماتية ظاهرة اجرامية مســـتحدثة نظرا لارتباطها بالتكنولوجيا، فقد ترتب على ذلك احاطة هذه الظاهرة بالكثير من الغموض، لأجل ذلك فقد بدا لنا أنه؛ وقبل الخوض في مجالات التعاون الدولي لمكافحة الجريمة المعلوماتية، كان لابد من الحديث عن مفهوم الجريمة المعلوماتية، وعلى ضـــوء ذلك ســـنحاول من خلال هذا المبحث التطرق الى مفهوم الجريمة المعلوماتية ضـــمن المطلب الأول، أما في المطلب الثاني ســـنتطرق الى تصـــنيف الجريمة المعلوماتية.

المطلب الأول:

مفهوم الجريمة المعلوماتية

ظهرت تعاريف كثيرة حول مفهوم الجريمة المعلوماتية ما بين مضـيق لمفهومها وموسـع، كما تعددت المصـطلحات المسـتخدمة للدلالة عليها؛ فالبعض أطلق عليها جريمة الغش المعلوماتي والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية[1] فيما يلي تفصيل لمفهوم هذه الجريمة من حيث التعريف والخصائص.

الفرع الأول: تعريف الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من الظواهر المســـتحدثة كما أســـلفنا الذكر، ولقد تعددت الجهود الرامية الى وضـــع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعريف محدد بل ان بعض الفقه ذهب الى ترجيح عدم وضـع تعريف بحجة ان مثل هذا النوع من الجرائم ما هو الا جريمة تقليدية ترتكب بأسلوب الكتروني[2].

أولا/ تعريف الجريمة المعلوماتية لغة:

الجريمة لغة: مأخوذة من الجرم وهي الذنب والجناية[3].

---

[1] الأطرش حسـني عصـام عسـاف محمد، معوقات مكافحة الجرائم المعلوماتية في الضـفة الغربية من وجهة نظر العاملين في أقسام الأجهزة الأمنية، مجلة جامعة الشارقة، المجلد 16، العدد 1، 16يونيو 2016، ص636.

[2] – خالد ممدوح أمن الجريمة الالكترونية، الدار الجامعية الاسكندرية 2008 ص41

[3] – الرازي بن أبي بكر محمد، مختار الصحاح، إخراج دائرة المعاجم، مكتبة لبنان ،بيروت ،1989،ص89.

أما المعلوماتية مصـــطلح مســـتحدث مشـــتق من كلمة معلومات فهي كلمة مكونة من مقطعين الأولINFORMATION و المقطع الثاني AUTOMATIQUEويرجع الفضل في اقتراح مصطلح المعلوماتية الى الاستاذ DREFUSحيث استخدمه عام 1962 لتميز المعالجة الآلية للمعلومات، و تبنته بعد ذلك الأكاديمية الفرنســـية في ابريل 1966 ومنحته التعريف الآتي: "علم المعالجة المنطقية للمعلومات التي تعتبر بمثابة دعامة للمعارف الانســـانية و الاتصـــالات في المجالات الفنية و الاقتصادية و الاجتماعية وذلك باستخدام آلية".[1]

ثانيا: تعريف الجريمة المعلوماتية في الفقه، والقانون، وفي إطار المنظمات الدولية:

1-تعريف الجريمة المعلوماتية في الفقه:

انقسم الفقه الى عدة اتجاهات منهم من ضيق من مفهوم الجريمة المعلوماتية، ومنهم من وسع من مفهومها فمن التعريفات المضيقة للجريمة المعلوماتية نورد الآتي:

أ/ "كل فعل غير مشـــروع يكون العلم بالتكنولوجيا الحاســـبات الآلية لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية اخرى"[2]

وحسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضـــيق بدرجة كبيرة من الجريمة المعلوماتية، حيث يحصرها بالحاسب الآلي.

[1] -الشوا سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات ط1 دار النهضة العربية القاهرة 1994 ص4

[2] - قورة نائلة جرائم الحاسب الاقتصادية، ط1 دار النهضة العربية، القاهرة 2003ص21

ب/ كذلك عرفت الجريمة المعلوماتية: "هي الفعل الاجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية."[1]

نرى أن هذا التعريف يحصـــر الجريمة المعلوماتية بالحاســـب الآلي دون غيره من التقنيات المعلوماتية.

ج/ يرى الأستاذ Tredmanأن الجريمة المعلوماتية" تشمل أي جريمة ضد المال باستخدام المعالجة الآلية للمعلومات".

نجد أن هذا التعريف حصر الجريمة المعلوماتية بالأمن المعلوماتي.

د/ عرفها (rosenblatt) على أنها "نشاط غير مشروع موجه لنسخ أو الوصول الى المعلومات المخزنة داخل الحاسوب، أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه". [2]

نلاحظ على هذا التعريف أنه يضـــيق جدا من مفهوم الجريمة المعلوماتية إذ يخرج من مجالها العديد من الأفعال غير المشروعة الذي يستخدم الحاسوب أداة لارتكابها.

د/ يرى الأستاذ (Mass) أن المقصود بالجريمة المعلوماتية "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح".[3]

نلاحظ أن هذا التعريف حصـــر الجريمة المعلوماتية بكل اعتداء يســـتهدف مصـــلحة يحميها القانون من خلال المعلوماتية بهدف تحقيق الربح، وبالتالي أخرج الاعتداءات التي لا تســـتهدف تحقيق أهداف ربحية.

---

[1] - أحمد هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة 1997ص13

[2] - يونس عرب، دليل أمن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والأنترنت، ط1، اتحاد المصارف العربية ،2002، ص23

[3] - أحمد هلالي عبد اللاه، المرجع السابق، ص6

وفي المقابل فان هناك تعريفات توسعت في مفهوم الجريمة المعلوماتية، وسنورد أهمها كالآتي:

أ/"كل فعل أو امتناع عمدي ينشأ عن استخدام غير مشروع لتقنية المعلوماتية بهدف الاعتداء على الأموال المادية والمعنوية."[1]

ب/ "كل سلوك سلبي أو ايجابي يتم بموجبه الاعتداء على البرامج المعلومات للاستفادة منها بأي صورة كانت".[2]

ج/ عرفها الخبير الامريكيParker "بأنها كل فعل اجرامي متعمد أي كان صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل" [3]

د/ عرفها الأستاذ (L'estancو Vivan) بأنها "مجموعة من الأفعال المرتبطة بالمعلوماتية التي تكون جديرة ".[4]

2_تعريف الجريمة المعلوماتية في القانون:

أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة بتكنولوجيا الإعلام والاتصال فانه يعرفها بأنها "جرائم الماسة بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام اتصالات الكترونية".[5]

وبهذا قد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة للجرائم التقليدية، ولولا هذه النظم المعلوماتية وشبكات الاتصال ما كان لنا أن نصبغ صفة المعلوماتية على هذه الجرائم.

---

[1] - الشوا سامي، المرجع السابق، ص07

[2] الهيثي محمد حماد، التكنولوجيا الحديثة والقانون الجنائي، ط1 دار الثقافة للنشر والتوزيع، عمان، 2004، ص152

[3] - الشوا سامي، المرجع السابق، ص 06.

[4] - المرجع نفسه، ص 06

[5] – نص المادة 2 من قانون 09-04

أما المشـرع الفرنسـي لم يعطي تعريف للجريمة المعلوماتية، ويلاحظ على تعريف المادة2 من قانون رقم 09 – 04 عدة ملاحظات:

1–أن المشــرع قد اعتمد على معيار الجمع على عدة معايير لتعريف الجريمة المعلوماتية أولها معيار وسيلة الجريمة وهو نظام الاتصـالات الالكترونية، وثانيها معيار موضـوع الجريمة الماس بأنظمة المعالجة الآلية للمعطيات، وثالثا معيار القانون الواجب التطبيق أو الركن الشـــرعي المنصوص عليه في قانون العقوبات. [1]

2–كمـا حـدد المشـــرع الجزائري نطـاق الجريمـة المعلومـاتيـة عن طريق اقراره بـأن الجريمـة المعلوماتية ترتكب في نظام معلوماتي أو يسـهل ارتكابها عليه، وهذا ما يوسـع من مجال الجرائم المعلوماتية في القانون الجزائري.

[1]– بوضياف أسماهان، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، العدد 11 سبتمبر 2018، ص ص 352––353

ج/ تعريف الجريمة المعلوماتية في إطار المنظمات الدولية:

عرفتها لجنة خبراء منظمة التعاون الاقتصـــادي للتنمية في عام 1983 بأنها "كل ســلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها."[1]

2-عرفها المجلس الأوروبي في تقرير المتعلق بجرائم الحاسوب بأنها "تغيير معطيات او بيانات او برامج الحاسوب او محوها أو كتابتها او اي تدخل اخر في مجال انجاز البيانات او معالجتها وتبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكيه شخص اخر او بقصد الحصول على كسب اقتصادي غير مشروع له او لشخص اخر".[2]

3-عرفها مؤتمر الامم المتحدة العاشــر لمنع الجريمة ومعاقبه المجرمين بأنها "اي جريمة يمكن ارتكابها بواســطة نظام حاســوبي والجريمة تلك تشــمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية".[3]

ونحن من جانبنا نؤيد هذا التعريف بانه حاول قدر الامكان الإحاطة بمفهوم الجريمة المعلوماتية حيث انه لم يركز على فاعل الجريمة ولا على الوســـيلة والغاية وذلك من اجل عدم افلات المجرمين من دائرة العقاب.

---

[1] – قورة نائلة ، جرائم الحاسب الاقتصادي ، المرجع السابق ،ص23

[2] – نهلا عبد القادر المومني، الجرائم المعلوماتية، المرجع السابق، ص 49.

[3] – المرجع نفسه، ص 49.

الفرع الثاني

خصائص الجريمة المعلوماتية

ارتباط الجريمة المعلوماتية بجهاز الحاسوب والأنظمة المعلوماتية الحديثة اضفى عليها مجموعه من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية ومن أهم هذه الخصائص ما يلي:

أولا/ الجريمة المعلوماتية عابرة للحدود:

اصـــبح العالم في ظل ثوره التكنولوجيا المعلوماتية قرية صـــغيره لا يعترف بالحدود الجغرافية فبعد ظهور شـــبكات المعلومات لم يعد هناك حدود مرئية قف امام نقل المعلومات عبر الدول المختلفة وهذا نتيجة التطور التكنولوجي في عالم تقنية الحواسيب، وهذا الامر ادى الى سهوله حركه المعلومات عبر انظمه التقنية الحديثة الذي جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دوله معينه بينما يتحقق الفعل الاجرامي في دوله اخرى، هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابره للحدود الوطنية انتجت العديد من المشـــاكل حول تحديد الدولة صـــاحبه الاختصـــاص لهذه الجريمة ، فكذلك حول تحديد القانون الواجب التطبيق ، بالإضافة الى اشكاليات تتعلق بالإجراءات الملاحقة القضائية وغير ذلك من الامور التي تثيرها الجرائم العابرة لحدود بشكل عام.

ولعل أبرز قضـــية في هذا الشـــأن القضـــية المعروفة باســـم الايدز التي لفتت النظر الى البعد الدولي للجرائم المعلوماتية[1] وتظهر أهمية هذه القضية من ناحيتين:

الأولى: أنها المرة الأولى التي يتم فيها تسليم المتهم في جريمة معلوماتية.

الثانية: أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة اعداد فيروس.

[1] – تتلخص وقائع هذه القضية التي حدثت في عام 1989 في قيام أحد الأشخاص بتوزيع عدد لبيلر من النسخ الخاصة بأحد البرامج الذي هدفه في الظاهر الى اعطاء بعض النصائح بشأن مرض الايدز ، الا أن هذا البرنامج في الحقيقة يحتوي على فيروس ؛ اذا كان يترتب على تشغيله تعطيل جهاز الحاسوب في العمل ثم تظهر بعد ذلك على الشاشة عبارة تطالب المجني عليه بإرسال مبلغ مالي الى عنوان معين حتى يتمكن من التخلص من الفيروس ؛ وفي الثالث من أفريل عام 1990 تم القاء

ونتيجة لهذه الطبيعة الخاصـــة بالجريمة المعلوماتية وخطورتها على المســـتوى الدولي تعالت الاصـوات الداعية الى التعاون الدولي المكثف من اجل التصـدي لهذه الجرائم، حيث يتمثل في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسـيق بين الدول الأطراف فيها، الامر الذي يكفل الايقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل.

ثانيا/ صعوبة اكتشاف الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بصـعوبة اكتشـافها واذا اكتشـفت فان ذلك يكون بمحضـي الصـدفة عادة[1] ، ويمكن رد الاسـباب التي تقف وراء الصـعوبة في اكتشـاف الجريمة المعلوماتية لعده امور، قيام الجاني بارتكاب هذه الجريمة في دول وقارة اخرى وقدرته على إخفاء دليل الإدانة في وقت قياسي يشكل عاملا اضافيا في صعوبة اكتشاف هذه الجرائم يلعب المجني عليه دور رئيســيا في صــعوبة وقوع الجريمة المعلوماتية ويظهر ذلك في عدة جوانب منها تحرص اكثر الجهات التي تتعرض انظمتها المعلوماتية للانتهاك على عدم الكشـــف عن ما تعرضـــت له وتكتفي عاده باتخاذ اجراءات اداريه داخليه دون الابلاغ عنها السلطات المختصة تجنبا للتشهير بها وهز الثقة في كفايتها الى جانب ذلك فان المجني عليه يتردد احيانا في الابلاغ عن هذه الجرائم.

ولعل أبرز مثال على احجام المجني عليه عن الابلاغ يظهر في المؤسـسـات المالية خوفا من التشهير بها وزعزعه ثقة العملاء بها.

القبض على المتهم جوزيف بوب أوهايو بالولايات المتحدة الأمريكية وتقدمت بريطانيا بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي حيث أن إرسال هذا البرنامج من داخلها ، وبالفعل وافق القضاء الأمريكي على تسليمه .

[1] – لصغير جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، ط1، دار النهضة العربية، القاهرة 1992، ص 17

جهل المجني عليه ببرامج عالم التقنية في الجرائم المعلوماتية في أكثر صورها خفيه لا يلاحظها المجني عليه او لا يدري حتى بوقوعها والامعان في حجب السلوك المكون لها واخفاؤها عن طريق تلاعب الغير المرئي في نابضات او ذبذبات الإلكترونية أو التي تسجل البيانات عن طريقها امرا ليس عسيرا في الكثير من الاحوال بحكم توافر المعرفة والخبرة في مجال التقنية المعلوماتية لدى مرتكبها[1].

3- طبيعة هذه الجريمة حيث ان هذه الجريمة لا تترك اي اثر خارجي لها بصوره مرئية.

ثالثا/ صعوبة اثبات الجريمة المعلوماتية

اكتشـــاف الجريمة المعلوماتية يعد أمرا ليس بالســـهل، ولكن حتى في حال اكتشـــاف وقوع هذه الجريمة والابلاغ عنها؛ فان اثباتها امر يحيط به كذلك الكثير من الصـــعاب ولعل من أبرزها ما يلي:

1- الجريمة المعلوماتية تتم في بيئة افتراضـية حيث تقع في العالم الافتراضـي فتقوم أركانها في بيئة الحاسوب والانترنت والتقنيات المعلوماتية مما يجعل الامر يزداد تعقيدا لدى سلطات الامن المختصة.

[1] – رستم هشام فريد، الجوانب الاجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، أسيوط، 1999، ص 16.

ففي هذه البيئة تكون البيانات عبارة عن نبضـــات الكترونيه غير مرئية تنســـاب عبر النظام المعلوماتي، مما يجعل أمر تدمير الدليل من قبل الفاعل أمرا في غاية الصعوبة.

2- أن وســـائل المعاينة وطرقها التقليدية لا تفلح غالبا في اثبات هذه الجرائم نظرا لطبيعتها الخاصـــة التي تختلف عن الجريمة التقليدية فالأخيرة لها مســـرح مادي حيث تخلف اثار ماديه تقوم عليها الأدلة مما يساعد السلطات الاستدلال والتحقيق الجنائي في الكشف عنها لكن فكره مسرح الجريمة المعلوماتية يتضاءل دوره في الافصاح عن الحقائق المؤدية لأدلة المطلوبة وذلك لسببين: [1]

الأول: ان الجريمة المعلوماتية لا تخلف اثار مادية.

الثاني: ان كثير من الاشـــخاص يردون الى مســـرح الجريمة خلال فتره من زمان وقوع الجريمة وحتى اكتشـــافها، هي فتره طويلة نســـبيا الأمر الذي يســـمح للجاني بان يغير او يعبث بالآثار المادية ان وجدت الامر الذي يثير الشك في تلك الأدلة.

3-نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء يشكل عائق اساسيا امام اثبات الجريمة المعلوماتية ذلك ان هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في بيئة الحاســـوب والانترنت ونتيجة لنقص الخبرة والتدريب كثيرا ما تخفق اجهزه الشـــرطة في تقدير اهميه الجريمة المعلوماتية بل في بعض الاحيان قد يدمر جهاز التحقيق الدليل دون علم.

[1] – حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، ط1، دار الكتب القانونية، القاهرة، 2002، ص 59

رابعا/ اسلوب ارتكاب الجريمة المعلوماتية:

خصوصية الجرائم المعلوماتية تظهر بصوره أكثر وضوح في اسلوب ارتكابها، فاذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي تتعدد صوره إما بصورة ممارسة عنف كجريمة القتل وغيرها، او تدمير ممتلكات كجريمه السرقة وغيرها ... فان الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج الى العنف بل كل ما تحتاجه الخبرة والقدرة على التعامل مع التقنية المعلوماتية[1].

وتحتاج كذلك الى وجود انترنت مع وجود مجرم يوظف خبرته على التعامل معها للقيام بجرائم مختلفة كالتجسس انتهاك خصوصيات الغير وغيرها وكل ذلك دون الحاجة الى سفك الدماء.

[1] نفس المرجع السابق، الصفحة نفسها

خامسا/ الجريمة المعلوماتية تتم عاده بتعاون أكثر من شخص

تتســـم الجريمة المعلوماتية بأنها يتم تنفيذها من عدة اشـــخاص حيث يكون هناك شـــخص متخصـص في التقنيات المعلوماتية يقوم بالجانب التقني من المشـروع الاجرامي وشـخص اخر من المحيط او من خارج المؤسسة المجني عليها لتغطيه عمليه الاحتيال والتحويل الارباح اليه[1] والاشتراك في اخراج الجريمة المعلوماتية الى حيز الوجود قد يكون بفعل سلبي من خلال صمت من يعلم بهذه الجريمة لتســـهيل تنفيذها وقد يكون بفعل ايجابي من خلال المســـاعدة اي كان نوعها. [2]

سادسا/ خصوصية مرتكبي الجرائم المعلوماتية:

الفاعل الذي يرتكب الجريمة المعلوماتية يطلق عليه المجرم المعلوماتي حيث يتصـــف هذا المجرم بخصـــائص معينه تميزه عن المجرم التقليدي، فاذا كانت الجريمة التقليدية لا إثر فيها للمســـتوى العلمي والثقافي للمجرم في عمليه تنفيذها باعتبارها الاصـــل العام فان الامر يختلف بالنســبة للجريمة المعلوماتية فهي جريمة التقنية تحتاج الى معرفة وقدرة عالية في مجال التقنية المعلوماتية .

كذلك فان القصـــد الجنائي من ارتكاب هذه الجريمة يختلف عن القصـــد الجنائي لدى المجرم التقليدي عند ارتكاب الجريمة التقليدية.

[1] – عفيفي عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط1، دار الكتب القانونية، القاهرة 2002، ص32

[2] – عبدو الشوا، المرجع السابق، ص 46

المطلب الثاني: تصنيف الجرائم المعلوماتية:

قسم الفقهاء ودارسو الجرائم المعلوماتية الى فئات متعددة تختلف حسب الاساس والمعيار الذي يستند اليه تقسيم المعنى، وبالتالي سنورد اهم هذه المعايير كالآتي:

الفرع الأول:

تصنيف الجرائم المعلوماتية تبعا لنوع المعطيات ومحل الجريمة

يعكس هذا التصنيف والتطور التاريخي لظاهره الجرائم المعلوماتية وهذا التصنيف كان سائد في مختلف كتابات الفقهاء، ولهذا نجد أن الجرائم المعلوماتية بحسب هذا المعيار تنقسم الى ما يلي :

اولا/الجرائم الماسة بقيمة معطيات الحاسوب :

تنقسم هذه الجرائم على فئتين :

الفئة الأولى الجرائم الواقعة على ذات المعطيات:

كإتلاف البيانات والمعلومات واتلاف برامج الحاسوب ذاتها بما في ذلك استخدام الفيروسات

الفئة الثانية: الجرائم الواقعة على ما تمثله هذه المعطيات اليا من اموال او أصول كجرائم غش الحاسوب التي تستهدف الحصول على المال او جرائم الاتجار بالمعطيات وجرائم التلاعب بالمعلومات المخزنة داخل الحاسوب واستخدامها دون وجه حق كتزوير المعالجة الآلية واستخدامها.

ثانيا/ الجرائم الماسة بالمعطيات الشخصية البيانات المتصلة بالحياة الخاصة:

وتشمل هذه الفئة الجرائم الاعتداء على المعلومات والبيانات الشخصية المتعلقة بالحياة الخاصة[1]

[1] – يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والأنترنت، ط1 ، دار العدالة ، عمان ، 2011 ، ص ص 26-27

وتعد هذه الجرائم من أخطر الصـــور لا نها تنطوي على الاعتداء على المعلومات المخزنة في الحاسوب واستغلالها بأمور مشروعة بصور مختلفة .

وقد تأخذ جرائم المعلوماتية الماسـة بالمعطيات الشـخصـية صـورة نقل او تسـجيل المحادثات الخاصـة وسـائط الاتصـال والتصـنت عليها وهذا يمثل اعتداء على الحياه الخاصـة، كذلك يعد انشاء البيانات الشخصية السرية سواء تم من قبيل الخطأ او بقصد التشهير او تهديد من صور الاعتداءات الحياه الخاصة؛ لان قيام شخص بإيداع بياناته لدى مؤسسه تحوز على ثقته وقيام تلك المؤسسة بإفشائها باي وسيله من الوسائل سالفه الذكر تعد من الجرائم التي تمس حياته الخاصـــة ولا يشـــترط القانون في بعض الدول ان تكون هذه البيانات حقيقيه او مزورة بل يكفي ان تمس بشرف.

اما بالنسبة للأشخاص الاعتبارية فانقسم الفقه بشأن وجوب حماية خصوصيتها الى رأيين:

الرأي الأول: أنكر عليها هذا نظرا لعدم تمتعها بالشـخصـية القانونية حيث حصـر الشـخصـية القانونية في الشخص الطبيعي.

الرأي الثاني: اقر لها بالحماية اســـتنادا الى ان هؤلاء الاشـــخاص تمنح لها حق الجنســـية كالشـــخص الطبيعي وبالتالي كل ما يتمتع بالجنســية يمكن اعتباره مواطن فله الحماية القانونية للمعلومات الخاصة به[1].

[1] – ممدوح بحر، حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر، عمان، 1996 ص 288.

ثالثا الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه:

تشـمل نسـخ وتقليد البرامج و اعاده انتاجها دون ترخيص وبالنظر في هذه الفئات نجد تداخل في ما بينها اذ ان الاعتداء على معطيات الحاسـوب بالنظر الى قيمتها الذاتية او ما تمثله هو اعتداء على امن المعطيات لكن الغرض المباشر الذي يستهدفه الاعتداء ينصب على قيمتها ، والاعتداء على حقوق الملكية الفكرية لبرامج الحاســـوب هو اعتداء على حقوق المالية واعتداء على الحقوق الأدبية لكنها تميزت عن باقي الفئات بأنها محلها هو البرامج فقط والاســـتخدام الغير مشـــروع لها، ومن جهة اخرى نجد ان الحماية الجنائية في القانون المقارن اعتمدت على نحو غالبا لتقســيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج وأيضـــا حماية البيانات الشـخصـية المتصـلة بالحياة الخاصـة وحماية المعطيات بالنظر الى قيمتها أو ما تمثله والذي عرف بحماية الأموال كل في ميدان وموقع مســـتقل ، وهو في الحقيقة تمييز ليس مطلقا بين حماية قيمة المعطيات وأمنها وحقوق الملكية الفكرية ولابدا من الاشـــارة الى أن حماية أمن المعطيات (الطائفة الثانية) انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة أو حماية البيانات والمعلومات الســـرية والمحمية ، فقد تم تناوله في نطاق جرائم الطائفة الســـابقة الماســـة بقيمة المعطيات ، وبالنظر الى أن الدافع الرئيســـي للاعتداء والغرض من معرفة أو افشـاء هذه المعلومات غالبا ما يكون الحصـول على مقابل مالي ، مما يعد من اعتداءات التي تندرج تحت نطاق الجرائم الماســـة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصـلة بالذمة المالية التي تسـتهدفها هذه الجرائم وقد تم التحدث عنها في المطلب الأول كما ذكرنا سابقا.[1]

[1] – يوسف المصري، المرجع السابق، ص 26 وما بعدها.

الفرع الثاني:

تصنيف الجرائم تبعا لدور الحاسب الالي في الجريمة

يلعب الحاسـوب والتقنية المعلوماتية دورا مهما في الجريمة المعلوماتية فقد يكون هدف سـلوك اجرامي استهداف المعطيات المعالجة او المخزنة او المتبادلة بواسطة الأجهزة التقنية والشبكات وهو ما يعبر عنه بالمفهوم الضيق لها وقد يكون الحاسوب وغيره من التقنيات الإلكترونية وسيله ارتكاب جريمة اخرى قد يكون الحاسـوب وغيره من التقنية الإلكترونية بيئة للجريمة وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور.

الأول: جرائم التخزين ويقصد بها تخزين المواد المستخدمة في ارتكاب الجريمة.

الثاني: جرائم المحتوى او ما يعبر عنه بالمحتوى غير القانوني او المحتوى غير المشروع

حيث أصبح المحتوى غير القانوني يرمز الى جرائم نشر مواد الإباحية والمقامرة وغيرها باعتبار ان مواقع الانترنت اصبحت تروج لهذه الأنشطة، والحقيقة المفهومين المفهومان يتصـلان بدور الحاسـوب وغيرها من التقنيات الإلكترونية كبيئة لارتكاب الجريمة وفي نفس الوقت كوسـيلة لارتكابها، ومن خلال هذا التقسيم فان الجرائم المعلوماتية تنقسم الى :

–تستهدف نظام المعلوماتية نفسه على المعلومات واتلافها وجرائم ترتكب بواسطه الحاسوب و غيره من التقنيات كجرائم احتيال الحاسـوب اما تقسـيمها كجرائم هدف ووسـيله ومحتوى فانه الاتجاه العالمي في ضـوء تطور التدابير القانونية والتشـريعية للجرائم المعلوماتية حيث انه هناك اتجاه الى وضـع اطار عام لتصـنيف الجرائم الإلكترونية و يمكن تقسـيمها تبعا لدور الحاسـوب والتقنية المعلوماتية في الجريمة كما يلي[1]:

1– اتفاقية بوداسـت لمكافحة الجريمة المعلوماتية، تم اعتمادها من قبل لجنة وزراء مجلس أوروبا في دورته التاسـعة بعد المائة بتاريخ8 نوفمبر لعام2001،وفتح باب التوقيع عليها في بودابست في 23نوفمبر،ودخلت حيز النفاذ في1يوليو لعام 2004.

الطائفة الأولى: الجرائم التي تستهدف عناصر السرية والسلامة الخاصة بالمعطيات والنظم:

وتضم هذه الطائفة الدخول غير القانوني أي غير المصرح به والاعتراض غير القانوني، وتدمير المعطيات والمعلومات واعتراض النظم أو إساءة استخدم الأجهزة الإلكترونية.

الطائفة الثانية: الجرائم المرتبطة بالحاسوب والتقنية المعلوماتية ونذكر من هذه الطائفة التزوير والاحتيال الإلكتروني.

الطائفة الثالثة: الجرائم المرتبطة بالمحتوى:

وتشمل طائفة واحدة وفق هذه الاتفاقية، وهي الجرائم المتعلقة بالأفعال اللاأخلاقية.

الطائفة الرابعة: وهي طائفة الجرائم المرتبطة بالإخلال بحقوق الفكرية كقرصنة البرمجيات[1].

الفرع الثالث تصنيف الجرائم المعلوماتية تبعا لمساسها بالأشخاص والأموال:

يمكن تقسيم الجرائم المعلوماتية طبقا لهذا المعيار الى ما يلي :

أولا الجرائم التي تستهدف الاشخاص:

وتضم هذه الفئة نوعين رئيسين من الجرائم :

النوع الأول: غير الجنسية ومنها التحريض عن الانتحار، الملاحقة عبر الوسائل الإلكترونية، بث المعلومات الزائفة، القتل بالكمبيوتر، التسبب بالوفاة، جرائم الاهمال، انشطه البريد الالكتروني الغير المرغوب فيه، الاحداث المتعمدة للفقر العاطفي عبر وسائل التقنية.

[1] – يوسف المصري، المرجع السابق، ص.ص28–29.

النوع الثاني: الجرائم الجنسية:

وتشمل: (حض وتحريض القاصرين على أنشطة جنسية غير مشروعة – إفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية – وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة – تلقي أو نشر المعلومات عن القاصرين عبر الحاسب الآلي – التحرش الجنسي بالقاصرين عبر الحاسب الآلي والوسائل التقنية الحديثة – نشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام وللقاصرين تحديدا – المساس بالحياء عبر الإنترنت – استخدام الإنترنت لترويج الدعارة بصورة قصرية أو للإغواء أو النشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم – الحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة خبيثة)، وبالتركيز في هذه الأوصاف نجد أنها تجتمع جميعا تحت صورة واحدة ألا وهي استغلال الإنترنت والحاسوب لنشر الدعارة واستغلال الأطفال و القصر في الأنشطة الجنسية غير المشروعة .

ثانيا طائفة جرائم الاموال عدا السرقة:

يقصد بذلك الاقتحام او الدخول غير المصرح به من خلال شبكه المعلومات اما مجردا أو لجهة ارتكاب فعل اخر ضد البيانات والبرامج والنظم المعلوماتية ضمن مفهوم تدمير الحاسوب واغتصاب الملكية وانتاج الفيروسات واستخدام الاسم التجاري الالكتروني دون ترخيص، واتلاف الغير مصرح به لنظم الحاسوب، وانشطه انكار الخدمة وايضا الحيازة الغير مشروعة للمعلومات واساءه استخدام المعلومات.[1]

[1] – غانم مرضي الشمري، الجرائم المعلوماتية، ط1 ، دار الثقافة ، عمان ، 2016 ، ص 58

ثالثا/ جرائم الاحتيال والسرقة:

تتفق جريمة النصـــب (الاحتيال) مع جريمتي الســرقة وخيانة الأمانة في أنها أيضـــا تطال مال الغير، إلا أنها تختلف عنهما في أن محلها يمكن أن يكون عقارا أو منقولا، أما جريمتي الســرقة وخيانة الأمانة فلا تردان إلا على مال منقول إضـافة إلى أن السـلوك في جريمة النصـب يتخذ صـورة للقيام بالطرق الاحتيالية، أما في جريمة خيانة الأمانة يتخذ صـورة الكتمان أو التبديد أو إتلاف مال سبق تسلمه بموجب عقد أمانة.

ومن بعض التعريفات الفقهية لجريمه الاحتيال: اســتعمال الجاني وســيله من وســائل التدليس المحددة على سبيل الحصر ودفع المجني عليه بذلك على تسليم الجاني مالا منقولا للغير.[1]

اما مصطلح التحايل المعلوماتي فهو مصطلح حديث النشأة فعرفته هيئة الامم المتحدة الاحتيال بانه " الادخال او المحو او التعديل للبيانات او برامج الحاســـوب او تدخل المؤثر في معالجه البيانات التي تسـبب خسـارة اقتصـادية او فقد حيز ملكيه شـخص اخر بقصـد الحصـول على كسب اقتصادي غير مشروع لها ولشخص اخر."[2]

وتشـــمل جرائم الاحتيال على التلاعب بالنظم المعلوماتية او اســـتخدام البطاقات بدون ترخيص وقرصنه البرامج هو سرقه خدمات الحاسوب.

[1] – فوزية عبد الستار، قانون العقوبات –القسم الخاص –، دار النهضة العربية، القاهرة، 1990، ص 817.

[2] – غانم مرضي الشمري، المرجع نفسه، ص 59.

رابعا/جرائم التزوير:

لقد انتشر استخدام الحاسوب انتشارا واسعا في شتى المجالات في التعامل بين الأفراد ويمكن القول أنه حل محل الأوراق العادية في أغلب نظم المعالجة الآلية للمعلومات ومع تزايد حجم الاعتداءات الواقعة على البيانات والمعلومات التي تمس الأفراد في حقوقهم وأموالهم، وفي مقابل ذلك تزايدت فرص الأشخاص للعبث والتلاعب في معطيات الحاسوب بتبديلها وتحويرها بالشكل الذي يفقد الثقة بالتقنية ويمس مراكز الأفراد، وبات من الواجب بسط الحماية لهذه المعلومات وضمان أمنها وسلامتها من هذا التبديل والتزوير، ويمكن التأكيد على أن التشريعات القانونية هي الضمانة الأبرز لحماية هذه المعلومات فبالاطلاع على أغلب التشريعات العربية نجد أنها بالرغم من بسطها الحماية القانونية للمحررات والمعلومات المتجسدة فيها من كل تزوير أو تبديل إلا أن هذه التشريعات تتباين فيما بينها ، فإذا كانت بعض التشريعات قد أوردت تعريفا للتزوير في نصوصها كالقانون العقوبات الفلسطيني رقم 74 لعام 1936مثلا الذي نص في المادة (332) على تعريف التزوير بأنه: تحريف معدل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي)، وغيرها من القوانين إلا أنه هناك تشريعات أخرى لم تورد تعريفا للتزوير كالقانون الجزائري والمصري فأنها تبقي الباب مفتوحة لدخول أنماط مستحدثة من الأفعال التي قد تعد تزوير بخلاف الاتجاه الأول الذي يعتبر مقيدا[1]. ويمكننا القول أن جريمة التزوير الإلكتروني يمكن أن تشمل تزوير البريد الإلكتروني الخاص بفرد أو مؤسسة معينة أو تزوير للوثائق والسجلات وأيضا تشمل تزوير الهوية.

[1] – محمد عقاد، جريمة التزوير في المحررات للحاسب الآلي، دراسة مقارنة، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، ص 394.

خامسا/ جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب وجرائم الحاسوب ضد الحكومة:

وتشمل جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب جريمة تملك وإدارة مشروع مقامرة على الإنترنت وتسهيل إدارة مشاريع القمار على الإنترنت وتشجيع المقامرة عبر الإنترنت لترويج الكحول ومواد الإدمان للقصر. وتشمل جرائم الحاسوب ضد الحكومة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون والإخفاق في الإبلاغ عن جرائم الكمبيوتر والحصول على معلومات سرية والأخبار الخاطئ عن جرائم الحاسوب والعبث بالأدلة القضائية أو التأثير فيها وتهديد السلامة العامة وبث البيانات من مصادر مجهولة، كما تشمل الإرهاب الإلكتروني[1].

المبحث الثاني:

اهم مجالات التعاون الدولي لمكافحه الجرائم المعلوماتية

ادى الانتشار الواسع والمتزايد للتقنية المعلوماتية وخاصة الحواسيب وشبكات الاتصال وتزايد الاعتماد عليها تنظيم نواحي الحياه الى وصول هذه التقنية الى بعض الاشخاص الذين قاموا باستخدام هذه التقنية ارتكاب الجرائم وقد اكتسبت الجريمة المعلوماتية اهتماما دوليا نظرا خطورتها وزيادة انتشارها على الصعيد الدولي فنجد قصور التشريعات الوطنية في مكافحتها فهذا الامر تطلب وجود تعاون دولي في عده مجالات لمكافحه الجريمة المعلوماتية، وعلى ضوء ما تقدم سنحاول من خلال هذا المبحث ان نتطرق الى اهم مجالات التعاون الدولي لمكافحه الجريمة المعلوماتية ضمن المطلب الأول التعاون القضائي اما المطلب الثاني سنتطرق الى التعاون الدولي في مجال التدريب لمكافحه الجريمة المعلوماتية.

[1] – يوسف المصري، المرجع السابق، ص33

المطلب الأول:

التعاون القضائي:

لتحديد ماهية التعاون القضـــائي ســـنتطرق الى التعاون الامني على المســـتوى الدولي في الفرع الأول اما في الفرع الثاني سنتطرق الى المساعدة القضائية الدولية.

الفرع الأول:

التعاون الامني على المستوى الدولي:

أولا/ تعريف التعاون الامني الدولي:

يعرف التعاون الامني الدولي بانه "تبادل العون والمساعدة وتظافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع او خدمة او مصـــلحة مشـــتركة في مجال تصـــدي بمخاطر الاجرام وما يرتبط به من مجالات اخرى مثل مجال العدالة الاجتماعية، ومجال الامن، أو لتخطي مشـكلات الحدود والسـيادة التي قد تعترض الجهود الوطنية لملاحقه المجرمين وتعقب مصـادر التهديد، سواء كانت مساعدة متبادلة قانونيه او قضائية او شرطية؛ وسواء اقتصرت على دولتين فقط او امتدت اقليميا او عالميا."[1]

ويعد التعاون الامني الدولي ثمره تطور العلاقات الدولية ونتيجة حتمية لما تشـــــهده الجريمة المعلوماتية من تطور وانتشار حيث اضحت ظاهره دولية.

[1] – خالد بن مبارك القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المعلوماتية عبر الوطنية، أطروحة داكتورة، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، دار النهضة العربية الرياض، 2006، ص 38.

ثانيا/ أهمية التعاون الامني الدولي وضرورته:

لعل شـــعور مجتمع الدولي بخطورة الجرائم المعلوماتية وتســـارع نمو الجريمة المعلوماتية جعل التعاون الامني لمكافحتها نقطه التقاء للجهود الدولية لاتخاذ تدابير تدعم ســـبل التعاون الدولي في مكافحتها، ويمثل التعاون الأمني الدولي بين أجهزة الشرطة الجنائية المتخصصة في مكافحة الجرائم المعلوماتية في الدول أحد الوســـائل الهامة التي يمكن من خلالها تفادي الجرائم المعلوماتية أو التقليل منها، وتؤكد التحقيقات في الجرائم عامة والمعلوماتية خاصـــة على أهمية التعاون الأمني الدولي، حيث يســـتحيل على الدولة بمفردها القضـــاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الأمن في هذه الدولة أو غيرها لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها، فملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة لتوقيع العقاب يستلزم القيام بإجراء التحريات خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها، ومن هذه الإجراءات معاينة مواقع الإنترنت في الخارج، أو ضـــبط الأقراص الصـــلبة، أو تفتيش نظم الحاسوب[1]،.. إلخ.

ومتى فر المجرم خارج حدود الدولة يقف الجهاز الأمني عاجز، لذا أصبحت الحاجة ماسة إلى وجود تعاون دولي يأخذ على عاتقه القيام بهذه المهمة.

[1] – فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية، رسالة دكتوراة، كلية الحقوق عين شمس، 2012، ص 514.

ويتضـــح أهمية التعاون الأمني من خلال تبني تكنيك متطور لإجراء التحريات والتحقيقات في مجال مكافحة الجريمة المعلوماتية، باســـتخدام التكنولوجيا الحديثة في الاتصـــال مثل الدوائر التليفزيونية، واستخدام أساليب خاصة للتحري والمراقبة، واستحداث قنوات للاتصال، والتنسيق الأمني والقضائي بين الجهات المختصة عن طريق الأقمار الصناعية وشبكة الإنترنت لتبادل المعلومات ســـريعا، وانتقال القاضـــي إلى الدول المعنية للتحقيق ولاتخاذ ما يلزم من إجراءات، ليس فقط في مرحلة التحقيق الابتدائي ولكن في مرحلة الحكم أيضـــا، ومراعاة تنفيذ الأحكام الأجنبية وفقا لضـــوابط تتفق عليها الدول فيما بينها، من خلال التوفيق بين الإجراءات الجنائية في كل من الدولتين، والاتفاق على معايير موحدة في هذا الشـــأن، كذلك الاتفاق على كيفية مصادرة الأموال محل الجريمة المعلوماتية عبر الحدود أو إرسال المسجونين[1].

ثالثا/ اسس التعاون الأمني الدولي لمكافحة الجرائم المعلوماتية:

نظرا للطبيعة الخاصـــة بالجرائم المعلوماتية فانه ينبغي ان يبنى هذا التعاون على اســـس معينة وهي كالآتي:

1- الدراســـة العلمية لبحث ظاهره الجرائم المعلوماتية و توفير البيانات الإحصـــائية المتعلقة بالجريمة بمرتكبيها بسير نظام القضاء الجنائي، حيث ان هذه المعلومات تساعد بصورة فاعلة على مكافحه جرائم المعلوماتية.

2- تحديد أساليب التعاون في مجال التدريب وتحقيق التكامل الامني بين اجهزه الشرطة على المستوى الدولي.

3- اعداد مشروع اتفاقية دولية تتضمن قانون موحد للجريمة المعلوماتية.

4- وضـــع اســـتراتيجيات وقائية واحترازية توفر الجو الملائم لمكافحه وأنهاء انشـــطه المنظمات الإجرامية، وزياده الوعي العام لدى الافراد بنشر البيانات اللازمة عن هذه الجرائم ومرتكبيها[1].

[1] – هدى حامد قشقوش، الجريمة المنظمة القواعد الموضوعية والاجرائية والتعان الدولي، دار النهضة العربية، القاهرة، 2002، ص 83.

5_التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في الساحات الأمنية الإقليمية والدولية، بما يحقق حصـــر معدلات الجريمة ويحول دون اســـتفحالها واســـتكمال أي نقص في المعلومات الأمنية، وذلك بالتعاون لتجميع عناصـــر تلك المعلومات، ليكتمل بها في النهاية كشـــف أبعاد الجرائم وخطط الإعداد لارتكابها، وإتاحة الفرصة لإمكان مدارسة الثغرات الأمنية الدولية والعمل على إيجاد أفضل أساليب التعدي لها منعا للجريمة، وضبطا للجناة وإتاحة الفرصة للتعرف على التجارب الأمنية الدولية في المؤسسات الأمنية لدى الدول الأخرى). ذلك لأن تبادل المعلومات والخبرات ونتائج البحوث والدراســـات بخصـــوص الجرائم المعلوماتية يتيح حصـــر الأســـاليب والوسائل الجديدة المستخدمة وارتكاب هذه الجرائم، ويوسع نطاق المعرفة بأنماط المجرمين فيها وأنشطتهم الإجرامية.

رابعا/ صور التعاون الأمني الدولي لمكافحة الجرائم المعلوماتية:

1-ربط شبكات الاتصال والمعلومات:

تحتاج الاتصـالات الشـرطية إلى وسـائل الاتصـال تحقق السـرعة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصـــل بين ســـلطات التحقيق والملاحقة المختلفة، لذا عمدت الدول والمنظمات الدولية تطوير الاتصال وتبادل المعلومات فيما بينها.

2-القيام ببعض العمليات الشرطية والأمنية المشتركة:

تعقب المجرم المعلوماتي وتعقب الأدلة الرقمية وضـــبطها، والقيام بعملية التفتيش العابر للحدود لمكونات الحاســب الآلي والأنظمة المعلوماتية وشـبكات الاتصـــال بحثا عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، كلها أمور تسـتدعي القيام ببعض العمليات الشـرطية والأمنية المشـــتركة، واشـــتراك الدول فيما بينها للقيام بعمليات شـــرطية وأمنية يؤدي إلى صـــقل مهارات وخبرات القائمين على مكافحة تلك الجرائم وبالتالي وضع حد لها.[2]

[1] – عادل عبد العال ابراهيم خراشـي، اشـكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسـبل التغلب عليها، ط1، دار الجامعة الجديدة، الاسكندرية، 2015، ص ص 23 .24.

[2] نفس المرجع السابق، ص24.

3-جهود المنظمة الدولية للشرطة الجنائية والإنتربول في مكافحة الجرائم المعلوماتية:

أولا/ تعريف الإنتربول:

الإنتربول هو أكبر منظمة شـرطية دولية، أنشـأت عام 1929، ومقرها الرئيسـي في مدينة ليون بفرنسـا، وكما هو معروف من دسـتور الإنتربول الدولي فهي تتكون من الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، المكاتب المركزية الوطنية، المستشارون، لجنة ضبط ملفات الإنتربول، وكانت تسمى هذه المنظمة باللجنة الدولية للشرطة الجنائية وتضم في عضويتها 182 دولة.[1]

وطريقة العمل داخل المنظمة تتم بتبادل أعضـــاء الشـــرطة الدولية المعلومات عن المجرمين الدوليين، ويتعاونون فيما بينهم في مكافحة الجرائم الدولية، مثل جرائم التهريب، وعمليات البيع والشـراء غير المشـروع للأسـلحة، والجرائم الإلكترونية، وقد ركز الإنتربول في السـنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأنشطة الإجرامية ذات الصلة بها، مثل غسل الأموال. ويحتفظ أفراد المنظمة بســجلات الجرائم الدولية وقد أنشـــأت المنظمة وحدة تحليل المعلومات الجنائية والتي تقضـي باسـتخلاص المعلومات الهامة عن المنظمات الإجرامية وتبويبها، بهدف وضع تلك المعلومات في متناول هيئة الشرطة، أو الدول الأعضاء في الإنتربول[2].

---

[1] – الشمري محمد غانم، المرجع السابق، ص 96.

[2] – بدأت ظهور الملامح الأسـاسـية لهذه المنظمة عبر العديد من المؤتمرات، ففي عام 1914انعقد المؤتمر الأول للشـرطة الجنائية الدولية في موناكو من ضـــباط شـــرطة ورجال قانون وقضـــاة من 14 دولة، وذلك للتباحث بشـــأن إجراءات التوقيف وأساليب التبيين والسجلات المركزية للمجرمين الدوليين واجراءات التسليم.

ثانيا/ أهداف الإنتربول:

تستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات البوليس في الدول الأطراف، وطبقا للمادة الثانية من ميثاق المنظمة تتمثل أهم أهداف هذه المنظمة في تحقيق الآتي:[1]

أ-جمع المعلومات المتعلقة بالجرائم والمجرمين، وذلك عن طريق المعلومات التي تتسلمها المنظمة-المكتب الرئيسي في اليون من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، ويتم ذلك عبر شبكة اتصالات حديثة.

ب-التعاون مع الدول الأعضاء في ضبط الهاربين والمطلوبين-أيا كانت جنسياتهم-والصادر ضدهم أحكام قضائية، أو أوامر بالضبط والإحضار لمثولهم أمام جهات التحقيق، وذلك من خلال إصدار النشرات الدولية المخصصة.

ج_ دعم جهود الشرطة في مكافحة الإجرام العابر للحدود، وتقديم الخدمات في مجال الأدلة الجنائية، كبصمات الأصابع، والحمض النووي

د-إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام.

هـ-تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان، وبروح الإعلان العالمي لحقوق الإنسان.

1 - نفس المرجع السابق ، ص 96

ثالثا: استراتيجية الإنتربول في مكافحة الجرائم المعلوماتية:

أنشـــأت المنظمة الدولية للشـــرطة الجنائية (الإنتربول) خلال عام 2004، وحدة خاصـــة لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع استراتيجيات لمواجهة هذا النوع من الجرائم، وذلك من خلال[1]:

أ-إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار (24) ساعة(7) أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف.

ب-اســتخدام وســائل حديثة في تلك المكافحة، كاســتخدام قاعدة البيانات المركزية للصــور الإباحية المحولة من قبل الدول الأطراف والتي تســتخدم برنامج Excalibur للتحليل والمقارنة الأوتوماتيكية لتلك الصور.

ج-تزويد شرطة الدول الأطراف بكتيبات ارشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها.

[1] – نبيلة هبة هروال، الجوانب الاجرائية لجرائم الأنترنت في مرحلة جمع الاســتدلالات، دراســة مقارنة، دار الفكر الجامعي، 2007، ص 153.

وهكذا يتولى الإنتربول إقامة العلاقات بين الدول والمنظمة، وتبادل المعلومات بين سـلطات التحقيق فيما يتعلق بالجرائم المتشـعبة في عدة دول، كتلك المتعلقة بالجرائم المعلوماتية. وبهذا فإن شـرطة الإنتربول تعد منظومة عالمية تختص بمكافحة الجرائم الدولية والعابرة للحدود الوطنية للدول، بما فيها الجرائم المعلوماتية، وذلك ما أكدته نتائج الدورة رقم (77) للجمعية العامة المنظمة الإنتربول، حيث دعا الأمين العام للإنتربول السيد "بونالد نوبل" جميع الحكومات والدول لدعم وتطوير نظم تبادل المعلومات حول المشتبه بهم ومحاربة الإرهاب المتنامي في كل أنحاء العالم بكل صـوره بما فيه الإرهاب المعلوماتي، وقد نجحت المنظمة الدولية للشـرطة الجنائية. الإنتربول خلال الأعوام الأخيرة في جعل اسـمها من أكثر الأسـماء التي يخشـاها المجرمون. وعلى المسـتوى العربي نجد أن مجلس وزراء الداخلية العرب أنشـأ المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.[1]

3-تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة:

تتعرض كافة دول العالم لاحتمالات وقوع كوارث ضخمة وأحداث جسيمة وبشكل لا يمكن توقعه أو يسـتحيل التنبؤ بتوقيت حدوثه أو يصـعب معه مواجهته بالإمكانيات القومية للدولة المنكوبة بمفردها هذه الكوارث أو الأزمات غالبا ما يكون عنصر الوقت من الأمور الحاسمة في المواجهة الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشـكل يصـعب تحقيقه إلا بتضافر الجهود ولذلك لا بد من التعاون بين الدول.[2]

[1] يوسف المصري ، المرجع السابق ، ص. ص 100، 102

[2]. الشمري مرضي غانم، المرجع السابق، ص95.

الفرع الثاني:

المساعدة القضائية:

أولا/ تعريف المساعدة القضائية:

تعرف المساعدة القضائية الدولية بأنها" كل اجراء قضائي تقوم به الدولة من شأنها تسهيل مهمه المحاكمة في دوله اخرى بصدد جريمة من الجرائم[1]"

ثانيا: خطوات المساعدة القضائية:

لا تتحقق المساعدة القضائية الدولية الا بواسطة ثلاث خطوات وهي كالآتي[2]:

أ. الطلب: وتقدمه الدولة صاحبة الاختصاص الجنائي بالمحاكمة، ويخضع هذا الطلب لقانون الدولة الطالبة وفي نطاق الاتفاقية التي تعقدها مع الدولة التي ستقدم المساعدة، ويتم تقديم الطلب بالطرق الدبلوماسية بحسب الأصل، ومع ذلك فإن بعض الاتفاقيات الدولية تسمح بالاتصال المباشر بين جهات العدل في الدولتين كسبا للوقت.

ب. فحص الطلب: وتقوم به الدولة التي ستقدم المساعدة، ويتم ذلك عن طريق التحقق من اعتبار الواقعة المطلوب تحقيقها تعد جريمة وفقا لقانون الدولة الطالبة، وفي ضوء مدى اختصاص الدولة المطلوب منها بإجابة هذا الطلب وفقا النصوص الاتفاقية التي تعقدها مع الدولة الطالبة.

---

[1] – سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات، رسالة دكتوراة، كلية الحقوق عين شمس، 1997، ص 425.

[2] – حسين صالح عبيد، القضاء الجنائي الدولي، ط1، دار النهضة العربية، 1977، ص 140.

ج. تنفيذ المساعدة القضائية: ويتم وفقا لقواعد الدولة المطلوب منها، حيث يتم تنفيذ الإجراء وفقا لقانون الدولة التي تنفذه والاتفاقيات الدولية هي وحدها الأداة التي يمكن أن تتبع عنها الالتزامات بين الدول، ومن ثم فإنه بدون الاتفاقيات الدولية، وخارج الشروط التي تنص عليها لا يمكن للدولة أن تعتمد على مساعدة الدولة المطلوب منها على أن ما ليس ملزما يظل مع ذلك ممكنا وفقا لما ينص عليه القانون الداخلي في كل من الدولتين.

ثالثا: صور المساعدة القضائية:

تتخذ المساعدة القضائية الدولية عدة صور، ولعل من أبرزها ما يلي:

1-تبادل المعلومات: يقصد بتبادل المعلومات تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم[1]، كما أن هناك مظهرا آخر لتبادل المعلومات يتعلق بالسوابق القضائية للجناة، من خلالها تتعرف الجهات القضائية بدقة على الماضي الجنائي للفرد المحال إليها، وهي تساعد في تقرير الأحكام الخاصة بالعود، ووقف تنفيذ العقوبة، إلا أن تدويل الصحيفة الجنائية مازال في مرحلة الأولى، وتقوم الدول بإعدادها بالنسبة لرعايا الدول التي ترتبط بها باتفاقيات تبادل معلومات[2].

[1] – جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالأنترنت، دار النهضة العربية، 2002، ص79.

[2] – عبد الرحمان فتحي سمحان، تسليم المجرمين في ظل قواعد القانون الدولي، دار النهضة العربية، 2012، ص5.

وقد قررت بتبادل المعلومات الاتفاقية الأوروبية حول الجريمة الافتراضـــية في المادة 23 والتي نصـــت صـــراحة على وجوب توافر التعاون الدولي بين الدول الأطراف وتعميقه وتقليل العوائق، بما يوفر أكبر قدر من السـهولة والسـرعة لتبادل المعلومات والأدلة بين الأطراف. كما نصت المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي على هذا التبادل بقولها تتبادل وزارات العدل لدى الأطراف المتعاقدة بصـفة منتظمة نصـوص التشـريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنتشر فيها الأحكام القضائية، كما تتبادل المعلومات المختلفة بالتنظيم القضـــائي..."،ومن أمثلة تبادل المعلومات في مجال التعاون القضـــائي الدولي الطلب المقدم من الســـلطات الاســـترالية إلى وزارة العدل الرومانية برســـالة إلكترونية بشأن ارتكاب جماعة رومانية جريمة سرقة معلومات واستنساخ واعتراض بيانات بشكل غير قانوني، تلك الجريمة التي كان ضـحاياها مواطنين اسـتراليين، وكان الطلب بشـأن تحديد هوية أصحاب البطاقات المستنسخة وأخذ إفادتهم من حيث قدر الخسائر التي تكبدوها ،وكذلك طلب الحصول على نسخ إليكترونية من الوثائق المستنسخة وتحديد وقت معين للرد على ذلك الطلب، وبعد إجراء مشاورات مع مكتب النائب العام الملحق بمحكمة النقض العليا أرسلت وزارة العدل الرومانية تلك المعلومات، كما قدمت عدة إيضـــاحات إضـــافية بشـــأن بعض عناصـــر التحقيق.[1]به حضور الشهود والخبراء: ويمثل حضور الشهود والخبراء من دولة الى أخرى صورة هامة من صور المساعدة القضائية الدولية في المجال الجنائي"، ويشترط أن يحضر الشاهد أو الخبير بمحض اختياره لهذا الغرض أمام الهيئات القضـــائية في الدولة التي تطلب حضـــوره، ويتمتع بحصـانة ضـد اتخاذ أية إجراءات جنائية بحقه أو القبض عليه أو حبسـه عن أفعال أو تنفيذ أحكام سابقة على دخوله إقليم الدولة طالبة حضوره، ويتعين عند إعلان الشاهد أو الخبير أن يتم إخطاره كتابة بهذه الحصانة قبل حضوره لأول مرة المادة 22 من اتفاقية الرياض العربية للتعاون القضائي.

[1]. عادل إبراهيم خراشي، المرجع السابق، ص34

2_نقل الإجراءات:

يقصـــد بنقل الإجراءات" قيام إحدى الدول باتخاذ الإجراءات الجنائية بشـــأن جريمة ارتكبت في إقليم دولة أخرى ولمصـــــلحة هذه الدولة بناء على اتفاقية"[1]، وذلك إذا توافرت شـــــروط معينة، أهمها:

1_أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها.

2_أن تكون الإجراءات المطلوب اتخـاذهـا مقررة في قـانون الـدول المطلوب منهـا عن ذات الجريمة.

3_أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصـــول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب منها،[2] ولقد أقرت العديد من الاتفاقيات الدولية والإقليمية هذه الصـــورة كإحدى المسـاعدة القضـائية الدولية، كمعاهدة الأمم المتحدة النموذجية بشـأن نقل الإجراءات في المســـــائل الجنائية، واتفاقية الأمم المتحدة المكافحة الجريمة المنظمة عبر الوطنية، 2000م، وكذلك معاهدة المؤتمر الإسلامي لمكافحة الإرهاب 1999م، وكذلك النموذج الارشادي لاتفاقية التعاون القانوني والقضـــائي الصـــادر عن المجلس التعاوني الخليجي 2003م، وكذلك الاتفاقية الفرنســـية المصـــرية المبرمة في 15/3/1982، وكذلك الاتفاقية المصـــرية الإيطالية الموقعة بالقاهرة في2001/02/15 ويحقق نقل الإجراءات الجنائية تقليص الآثار السلبية التي تنجم عن تنازع الاختصـاص بين الدول وتفوت الفرصـة على المجرمين الجاري التحقيق معهم في الإفلات من العقاب.[3]

[1] نفس المرجع السابق، ص34.

[2] الشمري مرضي غانم، المرجع السابق، ص95.

[3] عادل إبراهيم خراشي، المرجع السابق، ص35.

ولكن رغم ذلك فإن هذه الاتفاقيات تمثل آليات تقليدية في مكافحة الجرائم وملاحقة مرتكبيها، وهو ما قد لا يكون مجديا في إطار الجرائم الواقعة في بيئة الإنترنت، لما تســـببه هذه الفئة من الجرائم وفقا لســـماتها وطبيعتها العابرة للحدود الوطنية من صـــعوبات تتعلق بإقامة الدليل على ارتكابها، ومدى قبول التشـريعات لدى مختلف الدول للأدلة المسـتمدة من الحاسـوب، وكذلك ما يتعلق بمسائل الضبط والتفتيش فبالقضاء الرقمي وتتبع المسارات الإلكترونية ، كل هذه العوامل تؤدي إلى صـفوية إثبات جرائم الإنترنت ونسـبتها إلى مرتكبيها، لذا فقد دعت بعض التشـريعات إلى التعاون الدولي في مجال تفتيش أجهزة الحاســـوب).ومن أمثلة نقل الإجراءات كنوع من التعاون القضـائي الدولي تلقي السـلطات الأوكرانية عام 2009م، طلبا بالطرق الدبلوماسـية من محكمة لبناية بناء على المادة 18 من اتفاقية الجريمة المنظمة عبر الوطنية لاسـتصـدار أوامر اسـتدعاء لأربعة شـهود، وقد اسـتجابت أوكرانيا لهذا الطلب، وصـدر بالفعل أمر اسـتدعاء لأحد الشـهود، أما أوامر الاستدعاء الأخرى فلم تصـدر، لأن الشـهود لم يكونوا متواجدين على الأرض الأوكرانية.[1]

[1] نفس المرجع السابق، ص35.

3-الإنابة القضائية:

يقصد بالإنابة القضائية الدولية" طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها الضرورة ذلك للفصل في مسألة معروضة على السلطة القضائية في الدول الطالبة ويتعذر عليها القيام به بنفسها"[1]، وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الأخرى كسماع الشهود أو إجراء التفتيش وغيرها من الإجراءات ويكون التنسيق في موضوع الإنابة القضائية عبر البعثات الدبلوماسية والتي تتميز بالبطء والروتين في إجراءاتها، ونتيجة لذلك أبرمت العديد من الدول الاتفاقات الجديدة التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، وذلك مثل الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفوية في حالة الاستعجال، ونفس الشيء تجده في البند الثاني من المادة (30) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999م والمادة (15) من اتفاقية الرياض العربية للتعاون القضائي 1983م،والمادة (53) من اتفاقية شينغن 1990م والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف والفقرة (13) من المادة(46) من اتفاقية الأمم المتحدة لمكافحة الفساد.

[1] – عبد الرؤوف معدي، شرح القواعد العامة لإجراءات جنائية وفقا لآخر التعديلات، دار النهضة العربية، القاهرة، 2002، ص 102.

المطلب الثاني:

التعاون الدولي في مجال التدريب لمكافحة الجرائم المعلوماتية:

ادى ظهور اشـكال جديده من الجرائم المتمثلة في الجرائم المعلوماتية مثل القرصـنة و غيرها من الجرائم التقنية الاخرى حيث اصـبحت تشـكل عبئا على اجهزه العدالة بمختلف انواعها نظرا لخصـائص الجرائم المعلوماتية المتميزة عن غيرها من الجرائم التقليدية فلذلك يجب على الأجهزة الأمنية ان تتحمل كافه المســؤولية تجاه هذه الجرائم وتحقيق العدالة ومن اجل تحقيق ذلك كان لابدا ان تكون هذه الأجهزة على مختلف انواعها على درجه كبيره من الكفاءة والمهارة للكشــف عن غموض تلك الجرائم والتعرف على مرتكبيها بســرعه ودقه متناهيه وهذا لا يتحقق الا بالتدريب ولتحديد التعاون الدولي في مجال التدريب سوف نخصـص الفرع الأول لأهمية تأهيل القائمين على اجهزه مكافحه الجرائم المعلوماتية اما الفرع الثاني ســنتطرق لمظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية.

الفرع الأول:

أهمية تأهيل القائمين على أجهزة مكافحة الجرائم المعلوماتية:

بات التدريب في مجال مكافحة الجرائم المعلوماتية وسيلة للاستثمار الذي تلجأ إليه عادة المنظمات الإدارية لتحقيق أهدافها باعتباره عنصرا حيويا لابد منه لبناء الخبرات والمهارات المتجددة، والواقع أن التدريب أصبح يلعب دورا مهما في حياة الإنسانية المعاصرة[1]، فقد زاد الاهتمام بالتدريب بمختلف جوانبه التقنية وأضحي من ضروريات الحياة لدى أغلب أفراد المجتمعات ، سواء أكان متدربا أم بالنسبة للمنظمة التي تقوم بعملية التدريب أيضا، وسواء أكانت منظمة مدنية أم عسكرية أم حكومية أم خاصة أم كانت تعمل في قطاع العدالة أم في غيره فهو أحد العناصر الأساسية لزيادة كفاءة الكادر البشري ويرفع إنتاجيته ويحقق التنمية بمفهومها الشامل، والدافع من عملية التدريب هو إدخال وإحداث تعديلات جوهرية على سلوك المتدربين تبدو آثارها واضحة في سلوكهم لأداء الأعمال التي يكلفون بها كلا ومجاله بشكل

[1] الشمري مرضي غانم، المرجع السابق، ص.ص115-120.

أفضل بعد عملية التدريب[1]، كما أن التدريب يعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الآخرين من خلال أشخاص مؤهلين على ذلك، والمقصود بالتدريب هنا التدريب التقني وغير التقليدي الذي يكسب الأفراد خبرة فنية عالية في مجال الجريمة المعلوماتية. هذه الخبرة التقنية لا تتأتى دون تدريب تخصصي يراعى فيه القدرات الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية لتلقي التدريب[2]،وهنا يكون من السهل تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي الادعاء، ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات التي لها علاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الالي، ويجب أن يشمل المنهج التدريبي على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة معلومات وأجهزة الحاسب الآلي وأيضا ذكر مفاهيم وتعريفات للصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكاب الجرائم المعلوماتية ولابد أن يراعي في البرنامج التدريبي نوعه وصفته وما إذا كان رسميا من خلال حلقات دراسية أو حلقات نقاش ورش عمل حول هذه الجرائم المستحدثة، ويجب أن يكون هناك تفاعل مثمر بين المشاركين لتحليل الحالات الدراسية وتبادل الخبرة العلمية في كيفية التعامل مع الحاسب الآلي وكيفية استخدامها ، وقد يكون التدريب فردية أو يتم ضم مجموعة من المتدربين للعمل معا كفريق، ويتعين على الفرق أن تخوض تجارب عملية بحيث تعرض عليه عينة من الجرائم المعلوماتية التي تم التحقيق فيها على أن يراعي في هذه العينة التنويع لكي تؤدي دورها في إكساب المشاركين في البرنامج التدريبي الخبرة المطلوبة. وهذا يتطلب أن يقوم بالتدريب جهة مختصة ولها الخبرة الكافية في اختيار المتدربين ذوو الخبرة العلمية والفنية والصفات الشخصية المميزة[3].

[1] خراشي عادل إبراهيم، المرجع السابق، ص23.

[2] غانم راضي الشمري، المرجع السابق، ص22.

[3] المرجع نفسه، الصفحة نفسها.

ولابد لعملية التدريب أن تكون مستمرة؛ لأن الجرائم المعلوماتية في تطور مستمر وسريع، ولابد أيضا أن تسعى الأجهزة الأمنية التي تكون مسؤولة عن التحقيق أن تستعين بالمختصين والخبراء في مجال الحاسوب ويمكن ذلك عن طريق استعانة كلية الشرطة مثلا وقبولها بتعيين دفعات من الجامعيين من خريجي كليات تكنولوجيا المعلومات تخرجهم ضـــباط مؤهلين قانونيا وتقنيا وعلى الكليات التي تدرس القانون أن تعنى بتدريس الحاســـوب وعلومه، وذلك يؤدي إلى أن تكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة بالحاسوب.[1]

.

[1] - خراشي عبدالعال إبراهيم، المرجع السابق، ص23.

الفرع الثاني:

مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية:

أجهزة العدالة في الكثير من الدول ليست لديها الجاهزية لمواجهة جرائم الحاسب ومثيلاتها من الجرائم الحديثة ذات التطور المستمر، ومن هنا ولأننا نعلم أنه ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول كانت الدعوة إلى ضرورة وجود تعاون دولي في هذه الناحية، أي في مجال المساعدات القضائية المتبادلة وفي مجال تسليم المجرمين وفي مجال تدريب رجال العدالة وهناك بعض الاتفاقيات الدولية والإقليمية التي دعت صراحة إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينهما كما هو الحال في المادة 9 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود وقد يكون التعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكة الإنترنت بين الدول وأجهزة العدالة الجزائية لديها، ففي جمهورية مصر العربية نجد أن النيابة العامة تعقد الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقدت أو خارجها، بالإضافة إلى أنه يتم إرسال أعضاء النيابة من مختلف الدرجات في برامج خارجية، وذلك بالتعاون مع أجهزة النيابة العامة الأخرى والهيئات الدولية بهدف الاطلاع على أحدث النظم في هذا في الدول المجال. وقد يتحقق من عقد تلك اللقاءات والندوات تبادل الآراء والخبرات بين المشاركين وتبادل الرأي وطرح الأفكار والتصورات وتشجيع التعاون بين الدول والأطراف أو المعاهدات من أجل مقاومة تلك الجرائم.[1]

ومن فوائد تلك البرامج والندوات التدريبية التي تعود عليه أو المنظمات المشاركة أنها تمكنها من طرح ما تريد من موضوعات حيوية، كما أنها تعلن عن دورها الرائد لتزيد من ثقة الأطراف الأخرى في أدائها بما يشجع على إجراء المزيد من التعاون معها، ويمكن أيضا لهذه البرامج التدريبية أن تفيد متلقي التدريب عن طريق زيادة مهاراته وخبراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى، الأمر الذي ينعكس على الجهة التي ينتمي إليها بالفائدة.

[1] – بوربابة صورية، التعاون الدولي في مكافحة الجريمة المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد الأول، جويلية 2019، ص.ص 98.99.

ومن أهم التجارب تجربة الولايات المتحدة الأمريكية في مجال مكافحة الجرائم المعلوماتية فالولايات المتحدة الأمريكية تحرص على توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجزائية لدى الحكومات الأخرى مساعدة من لديها أجهزة شرطة وادعاء عام وقضاة أيضا ليصبحوا أكثر فعالية في مكافحة الجريمة، فمثل هذه المساعدة لا تؤدي إلى تيسير بناء إطار للتعاون الدولي في مجال تطبيق القانون وحسب، ولكنها تعزز أيضا قدرة الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة المعلوماتية لديها قبل أن يمتد ليتجاوز حدود بلدانها، وهناك مكتب للمساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج التابع لوزارة العدل الأمريكية، وهذا الجهاز مكلف بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى وتعزيز إدارة القضاء في الخارج، كما أن البرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي الذي كثيرا ما يعمل على توفير مساعدات الأجهزة الشرطة في البلدان العالم الثالث في مختلف أنحاء العالم. وفي الوقت الحاضر تقدم وزارة العدل الأمريكية مساعدات للقضاء الدول في أفريقيا ودول أخرى في آسيا وأوروبا الشرقية والوسطى وغيرها. ونجد أيضا أن أجهزة تطبيق القانون الأمريكية توفر أيضا تدريبا لنظيراتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهدة خاصة بالتدريب مثل كلا من المجر وتايلاند، وفي هذه المعاهدة يقوم خبراء أمريكيون في عمل أجهزة تطبيق القانون باطلاع المتدربين على أساليب وسبل مبتكرة للتحقيق، ويشجعون على تبادل الآراء مع نظرائهم في مختلف أنحاء العالم[1].

[1] – غانم مرضي الشمري، الجرائم المعلوماتية، المرجع السابق، ص.ص116–120.

خلاصة الفصل الأول:

تعتبر الجرائم المعلوماتية من الجرائم المستحدثة في الوقت الحاضر، حيث لم نجد لها تعريف جامع مانع سواء في الفقه أو في التشريعات الوطنية أو في إطار المنظمات الدولية، ولكن جميع التعريفات تتفق أن هذه جرائم ترتكب عبر تقنية المعلومات للحصول بطريقة غير مشروعة على معطيات وبيانات.

ولقد تسارع انتشار هذه الجرائم وكذا خطورتها حول العالم، نظرا لما تتمتع به من خصائص وكذا تعدد أنواعها، ونتيجة لذلك بذلت جهود دولية لمكافحة هذه الجريمة من خلال التعاون بين أشخاص القانون الدولي في العديد من المجالات أبرزها مجال التعاون الأمني، حيث يعتبر الانتربول أهم فاعل في هذا المجال، حيث نفذ العديد من المهمات الناجحة و نجح في ابرام العديد من الاتفاقيات المتعلقة بمكافحة الجرائم المستحدثة التي تعتبر الجرائم المعلوماتية احداها، ومجال المساعدة القضائية من خلال تبادل المعلومات بين الدول حول هذه الجرائم ومرتكبيها وكذا المساعدة في إجراءات وكذا تبادل الخبرات بين أجهزة المعنية بمكافحة هدا النوع من الجرائم.

المبحث الأول:

تحديات التعاون الدولي لمكافحة الجريمة المعلوماتية:

مع الدور الحيوي الذي يؤديه التعاون الدولي في مكافحة الجرائم المعلوماتية، الا أن ثمة تحديات ومعوقات تقف دون تحقيقه[1]، وبناء على ما تقدم سنفصل هذه التحديات الى المطالب الآتية:

في المطلب الأول التحديات الدولية لمكافحة الجرائم المعلوماتية وفي المطلب الثاني التحديات الداخلية لمكافحة الجرائم المعلوماتية

المطلب الأول:

التحديات الدولية لمكافحة الجرائم المعلوماتية:

يؤدي التعاون الدولي دورا فعالا في سبيل مكافحة الجرائم المعلوماتية الا أن هذا الدور يعترضه العديد من التحديات على الصعيد الدولي وسنفصل هذه التحديات في الفروع الآتية:

الفرع الأول:

القصور التشريعي للدول والتعارض بين مصالحها

يعتبر هذا الأمر أكبر تحدي يواجه مكافحة الجرائم المعلوماتية، لما يترتب على ذلك التعارض من مشاكل في تطبيق القانون من الناحية العملية، كما أن قصور التشريعات عن وضع مفهوم ونظام قانوني خاص بالجرائم المعلوماتية يجعل التعاون أمرا صعبا[2].

[1] بوربابة صورية، المرجع السابق، ص 28.

[2] - سامح أحمد، الجوانب الاجرائية الحماية الجنائية لجرائم الأنترنت، المرجع السابق، ص 538.

والناظر الى الأنظمة القانونية القائمة في العديد في الدول يتأكد من عدم وجود نظام قانوني خاص بمكافحة الجرائم المعلوماتية، فما يكون مباح في أحد الأنظمة يكون مجرما في نظام آخر، ويمكن ارجاع ذلك لعدة أسباب لعل أهمها ما يلي:

1 – اختلاف البيئات والعادات والديانات والثقافات من مجتمع الى مجتمع أخر وبالتالي اختلاف السياسة التشريعية

2 – كثرة المفاهيم القانونية المتعلقة بالجرائم المعلوماتية، فكل دولة تضع تعريفات حسب أنظمتها القانونية الجنائية[1]

ولكل هذه الأسباب انعكس ذلك سلبا على اجراءات التعاون الدولي، حيث أن عدم النص على جميع الجرائم المعلوماتية يؤثر على صانعي القرار في المجالات المختلفة[2]، كما أن القصور تشريعي للدول في وضع نظام قانوني خاص بالجرائم المعلوماتية يؤدي الى افلات المجرمين من العقاب واحضار الحقوق للأفراد المجني عليهم، وكذلك تعارض مصالح الدول فيما بينها يمثل تحدي كبير يعترض سبل التعاون الدولي، حيث تلجأ الدول الى تغليب مصالحها على حساب العدالة الجنائية وتنفيذ القوانين وخاصة لاسيما في اختلاف الأيديولوجيات.

[1] – عادل عبد العال خراشي، المرجع السابق، ص 57.

2– هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، ط1، دار النهضة العربية، القاهرة،2006،ص529.

الفرع الثاني:

تنوع واختلاف النظم القانونية الإجرائية

تختلف إجراءات ضبط ومتابعة الجرائم من دولة إلى أخرى، حيث نجد أن هذه الاجراءات المتمثلة في التحري والتحقيق والمحاكمة قد تثبت فاعليتها في دولة ما في حين تكون عديمة الفائدة في دولة أخرى، كما هو الحال بالنسبة المراقبة الإلكترونية[1]، والتسليم المراقب والعمليات المستترة وغيرها من الإجراءات الشبيهة. كما قد تعتبر طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة ؛قد تكون غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرم جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع، وهذا يعني غياب تنسيق إجرائي المتعلق بالجرائم المعلوماتية في كافة مراحلها في ظل عدم وجود قنوات اتصال فيما بين الدول ،مما أثر سلبا على التعاون الدولي في مجال مكافحة الجرائم المعلوماتية.

الفرع الثالث:

تنازع الاختصاص القضائي الدولي:

يقصد باصطلاح الاختصاص القضائي الدولي "مجموعة القواعد التي تبين حدود ولاية المحاكم فيما يخص العلاقات القانونية ذات العنصر لأجنبي إزاء محاكم الدول الأجنبية التي تنازع هذا الاختصاص"[2]

---

[1] مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة، دار الكتب، القاهرة، 2003، ص3.

[2] عكاشة محمد عبدالعال، القانون الدولي الخاص، دار الجامعة الجديدة، لإسكندرية، 1999 ص402

تثير مسألة الاختصاص في الجرائم المعلوماتية على المستوى المحلي والدولي مشكلة كبيرة، ففي المستوى الوطني أو المحلي تحدد عن طريق المعايير المحددة قانونا، لذلك فالمشكلة تكمن في الاختصاص على المستوى الدولي حيث تختلف التشريعات والنظم القانونية من دولة لأخرى، والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المعلوماتية التي تتميز بكونها عابرة للحدود[3]، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الاقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الاطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها.

الفرع الرابع:

التحديات الخاصة بتسليم المجرمين:

وتظهر التحديات الخاصة بتسليم المجرمين في جانبين وهما كالآتي:

أولا/ التجريم المزدوج:

يعتبر التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين[3] ويجد أساسه الفلسفي في أن التسليم إجراء يتضمن مساسا بالحرية الشخصية يستند إلى قضاء أجنبي، الأمر الذي يوجب أن يكون لهذا الإجراء ما

[3] غانم مرضي الشمري، المرجع السابق، ص126

يبرره في النظام القانوني الوطني، وأن يكون الفعل- مبنى الطلب- مجرما في القانون الوطني حتى لا تصطدم مشاعر الجماعة بالقبض على شخص أو اعتقاله لارتكابه فعلا تعتبره تلك الجماعة مباحا ومشروع.

وبالرغم من أهمية هذا الشرط إلا أنه غالبا ما يكون عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، لاسيما وأن بعض الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة تحديد ما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أم لا، يضاف إلى ذلك أن الدول قد تفسر بتوسع شرط ازدواج التجريم الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المعلوماتية.

ثانيا/ التزاحم في طلبات التسليم:

يقصد بالتزاحم في طلبات التسليم أو تنازع الطلبات:" تلك الحالة التي يصل فيها إلى الدول المطلوب منها التسليم أكثر من طلب تسليم من عدة دول تطلب ذات الشخص، سواء كان الطلب متعلق بنفس الجريمة أو بجرائم أخرى "[4]

وسبب تعلق هذه الصعوبة بالجرائم المعلوماتية أن الشخص المطلوب تسليمه قد يرتكب جريمة أو أكثر من الجرائم المعلوماتية تمس في نفس الوقت بمصالح أساسية لأكثر من دولة، ففي هذه الحالة قد تتزاحم طلبات التسليم المقدمة من الدول المضرورة إلى الدولة المطلوب إليها.

وللقول بوجود تزاحم في طلبات التسليم ينبغي أن تقدم الدولة الطالبة لأدلة التي تثبت قيام الشخص المطلوب بارتكاب الجريمة المعلوماتية وليس مجرد الادعاء، وكذلك إرسال طلبها بالفعل، حيث لا تكفي التصريحات الشفوية أو إبداء الرغبة في استلام الشخص. ولا يشترط في تزاحم الطلبات أن تتعاصر في وصولها إلى الدولة

[4] أحمد محمد السيد عبد الله، التعاون الدولي في الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراة، كلية حقوق المنصورة 2009، ص394.

المطلوب إليها، بل يكفي أن تتوالى إلى الدولة المطلوب إليها، طالما أن الشخص المطلوب ما زال متواجدة على إقليمها، ولم يتم تسليمه إلى أي من الدول التي تطالب بتسليمه.

الفرع الخامس:

التحديات الخاصة بالإنابة القضائية:

تظهر هذه التحديات في جانبين وهما كالآتي:

أولا/تحديات مرتبطة بفكرة السيادة:

يقصد بالسيادة: "السلطة العليا للدولة على رعاياها وإقليمها، وغير المقيدة بأية تبعية أو تأثير يأتي من خارج الدولة، وتستأثر بمباشرة جميع الاختصاصات داخل حدود الإقليم في مواجهة الرعايا، وتتصرف في الخارج على قدم المساواة مع غيرها من السيادات المماثلة"[5].

فعندما يرتكب فرد جريمة ما من الجرائم المعلوماتية في إحدى الدول، وتجري محاكمته في دولة أخرى، فمن المنطق بل من الواجب البحث عن كافة أدلة ثبوت تلك الجريمة أو نفيها في البلد الذي وقعت فيه بحسبان أنها البلد التي كانت مسرحا لتلك الجريمة، وهذا ما يعرف بالتعاون القضائي بين الدول المختلفة، غير أن هذا التعاون قد يصطدم بفكرة سيادة كل دولة على إقليمها، بحسبان أن كل دولة عادة تقوم بنفسها وعبر جهازها القضائي بالفصل في كافة المنازعات التي تثار على أراضيها لاعتبارات ترتبط بفكرة السيادة ، ومن هذا الجانب قد يبدو من غير المقبول أن تطلب – مثلا – محكمة جزائرية دولة أخرى أجنبية أن تقدم لها العون والمساعدة في القيام بإجراء أو أكثر من إجراءات التحقيق على إقليمها يكون اتخاذه لازما للفصل في الدعوى المنظورة أمام المحكمة الجزائرية، والعكس صحيح، وبالتالي فإن

[5] نسيب أرزقي، مستقبل السيادة والنظام العالمي الجديد، المجلة الجزائرية للحقوق والعلوم الإدارية والقانونية،ج36،1998،ص86.

الزج بفكرة السيادة قد يعوق التعاون القضائي بين الدول المختلفة في مكافحة الجرائم العامة.

ثانيا: التحديات المرتبطة بإجراءات الإنابة:

الأصل بالنسبة لطلبات الإنابة القضائية الدولية والتي تعد من أهم المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية، وهذا بالطبع يجعلها تتسم بالبطء والتعقيد والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة وهو الأمر الذي انعكس على الجرائم المتعلقة الإنترنت.[6]

وهناك صعوبة أخرى في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث إن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب.[7]

الفرع السادس:

التحديات الخاصة بالتدريب في مجال مكافحة الجرائم المعلوماتية:

وتتمثل هذه التحديات والصعوبات في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات، ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الافراد المتدربين سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال، حيث إنه يوجد بعض الأشخاص ممن لا يعني في هذا المجال شيء وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال. ومن الصعوبات

[6] خراشي إبراهيم عادل، المرجع السابق، 63.
[7] المرجع نفسه، ص64.

أيضا التي قد تؤثر على عملية التدريب وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العلمي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا من حيث ما يدور بها من وقائع وملابسات وإجراءات وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية.[8]

المطلب الثاني:

التحديات الوطنية التي تواجه التعاون الدولي في مكافحة الجرائم المعلوماتية:

لا تقتصر التحديات التي تواجه التعاون الدولي في مجال مكافحة الجرائم المعلوماتية على المستوى الدولي، بل تشتمل أيضا مجموعة من التحديات الوطنية، ولعل من أهمها ما يلي:

الفرع الأول:

عدم كفاية وملائمة القوانين القائمة:

قد شمل التطور التكنولوجي شتي نواحي الحياة، حيث أضحي الجميع يعتمد على التكنولوجيا في سائر أموره، ومنهم مجرمي الجرائم المعلوماتية حيث استغلوا التقنية لارتكاب جرائمهم، ولكن هذا التطور الهائل في عالم الجريمة لم يقابل بذات الدرجة في النصوص القانونية.

وبالتالي فإن العديد من القوانين الجنائية لبعض الدول يستحيل لها مواجهة تلك الصور المستحدثة من الجرائم، لتطلب غالبية النصوص الصفة المادية في الشيء محل ارتكاب الجريمة، وهو ما يتنافى مع طبيعة الجرائم المعلوماتية، وبالتالي تخرج تلك الصور من طائلة التجريم والعقاب.[9]

---

[8] الشمري مرضي غانم، المرجع السابق، 128.

[9] صالح منير محمد، الجرائم المعلوماتية (وطرق مواجهتها)، بحث منشور بمركز بحوث الشرطة، القاهرة، العدد الثالث، يوليو، 2005، ص179.

وعلى الرغم من إصدار العديد من الدول للتشريعات المتعلقة بالجرائم المعلوماتية وانضمامها للعديد من الاتفاقيات الدولية التي تجرم الأفعال المخالفة للمعاهدات المنظمة لهذه الجرائم، حيث نجد مثلا المشرع الجزائري قد سارع بتعديل سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث أنه بتعديلي 01/09 و 04/14 وضع قواعد و احكام خاصة لسلطة المتابعة والاختصاص، الغرض منها هو مواجهتها، وهذه الأحكام هي: جواز تمديد الاختصاص المحلي للمحكمة: حيث نصت المادة 329 من قانون الإجراءات الجزائية في قدرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محكم أخرى عن طريق التنظيم في جرائم المخدرات و الجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية المعطيات. وتوسيع مجال اختصاص النيابة العامة: حيث أنه بموجب المادة 37 من قانون الإجراءات الجزائية تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها من قبل حيث نصت هذه المادة على تمديد الاختصاص للمحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض لأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[10]

• العمل بنظام المشروعية في تحريك الدعوى العمومية: حيث سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، حيث يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعلم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر 144 مكرر 1و2 من قانون العقوبات المعدل والمتمم بالقانون 01/09 المؤرخ في 26 يونيو 2001. إضافة لما سبق ودائما في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام بأعراض المراسلات

[10] نص المادة 39 من قانون الإجراءات الجزائية الصادر بموجب أمر رقم 66/155 بتاريخ 8يونيو لعام1966.

وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرره في إطار تعديل قانون الإجراءات الجزائية بالقانون 06/22المؤرخ في 20/12/2006.

إلا أن هذه النصوص غير كافية لمعالجة سائر الجرائم المعلوماتية، الأمر الذي يؤدي لتقليل جهود رجال الشرطة عند ضبط الجرائم والكشف عن مرتكبيها، كما أن الكثير من التشريعات الداخلية للدول وإن كانت تحتوي على قواعد عامة يمكن تطبيقها على الجرائم التقليدية إلا أنه نظرا لاختلاف أركان وشروط الجرائم المعلوماتية عن أركان وشروط الجرائم التقليدية فإنه يترتب على ذلك عدم إمكان تطبيق هذه النصوص على هذه الجرائم، مما يصعب مهمة الأجهزة الشرطية والقضائية في ضبط هذه الجرائم وملاحقة مرتكبيها قضائيا.

الفرع الثاني:

صعوبة إثبات الجرائم المعلوماتية والتحقيق فيها:

يرجع ذلك إلى العديد من الأسباب نذكر منها:

1. الطبيعة الخاصة للدليل في الجرائم المعلوماتية فهو ليس بدليل مرئي يمكن فهمه بمجرد القراءة، ويتمثل حسب ما تنمية النظم أدلة على الجرائم التي تقع عليها أو بواسطتها –بيانات غير مرئية لا تفصح عن شخصية معينة عادة، وتظهر هذه المشكلة بصفة بالنسبة لجرائم الإنترنت مثل الجرائم التي ترتكز على البريد الإلكتروني في ارتكابها، إذ يكون من الصعب على جهات التحري تحديد مصدر الإرسال.[11]

[11] الشمري مرضي غانم، المرجع السابق، ص174

2. سهولة إزالة الدليل، فالجاني يستطيع أن يتوجه إلى أي متجر خاص بالإعلام الآلي والدخول على أحد المواقع وإرسال رسالة على إيميل شخص آخر تحوي عبارات سب وقذف، ثم يقوم بإزالة الدليل والمغادرة من المتجر كأن شيئا لم يحدث.

3. صعوبة الوصول إلى الدليل؛ وذلك نتيجة توفير المواقع العالمية على الإنترنت للبيانات المخزنة على خوادمها حماية أمنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الاطلاع عليها أو نسخها، هذا من جهة ومن جهة أخرى يمكن للجاني زيادة صعوبة عملية ضبط أي دليل يدينه وخاصة إذا كانت لديه خبرة بمجال الأمن المعلوماتي.

4. اعتماد مرتكبي الجرائم المعلوماتية على الخداع والتخفي عبر تغيير قناع الشبكة المعلوماتية؛ نتيجة لامتلاكهم خبرة عالية في الأمن المعلوماتي والبرمجي.[12]

5_اختلاف دوائر العرض وخطوط الطول عبر العالم، مع إمكانية تنفيذ الجريمة عن بعد وكذلك اختلاف النظم القانونية بين الدول؛ حيث أن القانون الواجب التطبيق يلعب دورا كبيرا في تثبيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم.

6_إحجام الكثير من الجهات عن التبليغ عن تلك الجرائم، حيث تحرص أكثر الجهات وخاصة البنوك أو المؤسسات الادخارية على عدم الكشف عما تعرض لها ، وعدم بيان عجزها عن تحقيق الأمان الكافي للمعلومات، وبالتالي لأصول الأموال التي تتعامل معها، فتكتفي الجهة عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عما تعرضت له للسلطات المختصة، تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها، وقد يكون السبب في ذلك أيضا هو محاولة إخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها، الأمر الذي يشجع الجناة على ارتكاب المزيد من الجرائم.[13]

[12] خراشي إبراهيم عادل، المرجع السابق، ص54.

[13] رستم فريد هاشم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، آسيوط، 1994، ص25.

المبحث الثاني:

آليات التغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية:

تناولنا في المبحث السابق أهم التحديات التي تعترض سبل التعاون الدولي في مكافحة الجرائم المعلوماتية وتقديم مرتكبيها للعدالة، وفيما يلي نعرض لأهم الآليات والإجراءات والتدابير التي يتعين اتخاذها للقضاء على تلك التحديات أو على الأقل محاولة الإقلال منها. وسوف نتناول هذا المبحث في المطلبين التاليين:

المطلب الأول: آليات التغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الوطني.

المطلب الثاني: آليات التغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الدولي.

المطلب الأول:

آليات التغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الوطني.

تتمثل أهم آليات التغلب على تحديات التعاون الدولي في مجال مكافحة الجرائم المعلوماتية على المستوى الوطني في اتخاذ التدابير الموضوعية (فرع أول) والتدابير الإجرائية (فرع ثان).

الفرع الأول:

التدابير الموضوعية:

يتوجب على كل دولة أن تتبع سياسة تشريعية تهدف إلى التعاون مع باقي الدول الأجل حماية المجتمعات من مخاطر وتداعيات الجرائم المعلوماتية وذلك من خلال تبني ما يتلاءم ويتناسب مع الطبيعة الخاصة لتلك الجرائم من تشريعات، وذلك حتى يمكن مواجهة مخاطر استخدام الإنترنت في ارتكاب الأفعال الإجرامية وإمكانية نقل وتخزين الأدلة المتعلقة بتلك الأفعال الإجرامية عبر شبكة الإنترنت، ولذا يتعين على كل دولة أن تتبع التدابير التشريعية وغيرها من التدابير الأخرى اللازمة للكشف المبكر عن عملية الدخول غير المشروع، والبقاء غير المصرح إلى كافة أجراء نظام شبكة الإنترنت وفقا لما تقضي به أحكام قوانينها الداخلية.[14]

[14] سامح أحمد بتأجيل موسى، المرجع السابق، ص.ص542-543.

وكذلك اتخاذ التدابير التشريعية اللازمة لإدراك أي استيلاء غير قانوني وجعله جريمة جنائية وفقا للأحكام المقضي بها في القانون الوطني، كما يجب على كل دولة من الدول أن تشمل قوانينها أعمال الإضرار أو الإتلاف أو المحو أو الإعاقة أو التعديل التي تستهدف بيانات الحاسوب جرائم جنائية يعاقب عليها القانون، كما يجب اعتبارها جرائم جنائية تقتضي العقاب تلك الأعمال التي تعوق دون حق وظائف شبكة الإنترنت والحواسيب المتصلة بها، من خلال إدخال أو نقل أو الإضرار أو محو أو إتلاف أو تعديل أو إعاقة بيانات الحواسيب المتصلة بالإنترنت سواء أكانت حواسيب المضيفة أو المستضيفة.

كما يجب على كل دولة أن تتبنى إجراءات تشريعية تتيح مساءلة الأشخاص المعنوية جنائيا عما ينشأ من جرائم تتعلق بالحاسوب والإنترنت، وذلك في أحوال قصور الإشراف والرقابة من الشخص الطبيعي الذي يؤدي إلى حدوث جرائم أو تسهيل حدوثها.[15]

وغالبا ما يطبق على الجرائم المعلوماتية خاصة في بعض الدول –العربية– القانون الجنائي التقليدي، غير أن تلك الجرائم هي جرائم جديدة ليس هناك ما يحكمها في القانون الجنائي العادي، والقاضي حين تعرض أمامه دعوى من الدعاوى في هذا الإطار هو مقيد بما هو نافذ من النصوص القانونية، مهما حاول الاجتهاد والقياس فإن حكمه غير محصن من الطعن فيه، خاصة عندما يتم التثبت بمبدأ "لا جريمة ولا عقوبة إلا بنص"، انطلاقا من هذا المعنى صار ضروريا لكل الدول –خاصة العربية– أن تعيد النظر في تشريعاتها القائمة، قصد تعديلها ووضع تشريعات مستقلة تحيط بجميع الجرائم الممكن ارتكابها بواسطة الإنترنت.

ولذا من الأجدر تعديل بعض الأحكام الموضوعية لقانون العقوبات ليكون النص فيه صريحة على تجريم كافة الجرائم المعلوماتية والحاسبات الآلية، بدلا من إدراج تلك الجرائم تحت النصوص القانونية القديمة، وتحت مسمى الجرائم التقليدية القديمة ،

[15] نفس المرجع، ص542.

فالتطور التقني الذي نعيشه حاليا، والذكاء الذي يكون عليه هؤلاء المجرمين يؤكد بأننا نواجه العديد من الجرائم شديدة التعقيد والتطور، والتي لا تجد لها نصا قانونيا تقع تحت طائلته من تلك النصوص القانونية التقليدية القديمة التي تضع الجرائم التي ترتكب حاليا في نطاقها.

فنحن في حاجة إلى نصوص قانونية جديدة بحيث تجرم تلك الجرائم المعلوماتية الجديدة وما قد يستجد معها من جرائم ومن تطور في أدوات وارتكاب مثل تلك الجرائم، حتى لا يأتي الوقت الذي تقف فيه يد القانون عاجزة عن أن تقتص حق المجتمع عن تلك الفئة المنحرفة التي تستغل التكنولوجيا الحديثة والتطور التقني في ارتكاب الجرائم بدلا من استغلالها فيما يفيد المجتمع، على أنه يجب أن تراعى أن تكون تلك النصوص قد صيغت من جميع الدول دون استثناء، وأن تستوعب أي تطوير قد يحدث في المستقبل.[16]

الفرع الثاني:

التدابير الإجرائية:

تتمثل أهم التدابير الإجرائية التي يتعين على الدول اتخاذها، بهدف التغلب على إشكاليات التعاون الدولي بشأن مكافحة الجرائم المعلوماتية في الآتي[17]:

1_تبني التدابير التشريعية الإجرائية التي تمكنها من تفتيش نظم وشبكات الحاسوب أو أجزائها، وفحص البيانات المخزنة بها، وكذلك المخزنة على مختلف وسائط التخزين الأخرى، سواء أكانت هذه الأجزاء محل التفتيش تقع داخل الدول أو خارجها، طالما كان ذلك الأمر يفيد التحقيق في الجريمة وتقتضيه مصلحته.

[16] منير محمد الجنبيهي-ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي، دار الفكر الجامعي، الإسكندرية، 2004، ص.ص136-137.

[17] سامح أحمد بلتاجي موسى، المرجع السابق، ص543.

2-على كل دولة أن تتخذ التدابير التشريعية التي تلزم لتخويل سلطاتها المعنية صلاحيات ضبط وإحضار الأشخاص المتورطين بالجريمة، سواء أكانوا متواجدين على إقليمها أو في أي مكان آخر، لكي يقدم ذلك الشخص ما يقع تحت يده من بيانات مخزنة في أحد أنظمة الحاسوب، أو أحد الوسائط التي تستخدم في عملية تخزين البيانات، وذلك بالكيفية التي تطلبها تلك السلطات المصلحة التحقيق، وعلى كل دولة أن تتعاون فيما بينها في شأن تسهيل ذلك.

3-إضفاء صفة الضبطية القضائية على العاملين في مجال المعلومات من غير رجال الشرطة، كمزودي الدخول وخدمات الإنترنت، إذ تبعا لأعمالهم فإنهم يقومون بالرقابة عبر المزود عن سير حركة العمل ومدى الخضوع للنظام والقانون من قبل العاملين والمتعاملين مع شبكة الإنترنت، بحيث إذا حدث ووجدت الجريمة باكتشافها بهذا الأسلوب فإنه ليس لهؤلاء سوى التحفظ على أدالة الجريمة إلى حين حضور رجال الضبط القضائي".

4-قيام أجهزة الشرطة داخل كل دولة بعمل دوريات المراقبة مؤسسات نتاج الحواسب، وذلك وقاية من كافة صور الإجرام المتعلقة بالكمبيوتر والإنترنت، مثل تقليد برامج الحاسب الآلي بطريقة غير مشروعة، وإساءة تصنيع مكونات الحاسب بطريقة تستهد لإضرار بمستخدميه[18].

5-ضرورة تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناءعلى اتفاقيات دولية ولهذا التعاون أهميته، بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أن إحدى الجرائم المعلوماتية قد تم ممارستها عبر شبكة الإنترنت من خلال موقع موجود في الخارج فإنها تقوم بالإبلاغ عن هذه الجريمة إلى سلطات البوليس بالدولة التي تم فيها البث[19].

[18] عفيفي كامل، المرجع السابق، 471.
[19] طارق إبراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، 2009، ص594

كما يجب أن تعين كل دولة الإدارة الأمنية بمكافحة هذا النوع من النشاط الإجرامي، فيوكل إليها تلقي البلاغات التي محورها جريمة معلوماتية، ويكون من اختصاصها اتخاذ الإجراءات القانونية المناسبة–حسب القوانين الوطنية وتنفيذ التدابير الأمنية الواقية من استفحال هذا الخطر الملاصق للتقنية الحديثة، والهادم للاستفادة الصحيحة من المعلوماتية.

6–على كل دولة أن تتخذ تدابير تشريعية ترمي إلى تمكين سلطاتها المعينة من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد أنظمة الحاسوب، بما يحقق مصلحة التحقيق، وخاصة إذا ما تبين أن تلك البيانات معرضة للتلف، أو النقد، أو التعديل، أو المحو.

7-على كل دولة أن تتبنى التدابير التشريعية التي تلزم لمد مجال اختصاصها القضائي على أي جريمة من جرائم الإنترنت إذا وقعت:[20]

أ. بشكل كامل أو جزئي على إقليمها، أو على متن باخرة، أو طائرة، أو قمر صناعي يحمل علمها أو مسجل لديها.

ب -من أحد مواطني الدولة إذا كانت الجريمة من الجرائم التي يعاقب عليها وفقا لأحكام قانون العقوبات الساري في محل وقوع الجريمة، أو إذا وقعت الجريمة خارج نطاق الاختصاص الإقليمي لأي دولة أخرى.

المطلب الثاني:

آليات التغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الدولي:

كما يوجد آليات وطنية للتغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية، توجد كذلك آليات دولية للتغلب عليها وهي كالآتي:

الفرع الأول:

آلية التغلب على تحدي القصور التشريعي للدول والتعارض بين مصالحها:

تختلف قوانين الدول بشكل كبير، وإذا كان بالإمكان لدولة ما أن تطبق قوانينها في إطار حدود إقليمها الجغرافي على ما يرتكب من جرائم تقليدية، فالأمر مختلف

[20] عادل عبد العال خراشي، المرجع السابق، ص73.

بالنسبة للجريمة المعلوماتية، حيث لا حدود بين الدول لأن مسرح الجريمة المعلوماتية افتراضي. وللتغلب على هذا التحدي فإن الأمر يتطلب إيجاد نظام القانوني موحد خاص بالجرائم المعلوماتية، ولصعوبة هذا الأمر فإنه لا مناص في البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة الخاصة للجرائم المعلوماتية، ويخفف من حدة الفوارق بين الأنظمة الجنائية الوطنية، وتتمثل هذه الوسيلة في تحديث الأنظمة القانونية الوطنية المنظمة للجرائم المعلوماتية، وإبرام معاهدات خاصة يراعى فيها الطبيعة الخاصة للجرائم المعلوماتية.

ولذا يتعين على الدول التفاوض فيما بينها للوصول إلى معاهدات واتفاقيات دولية أو إقليمية، تضع تشريعا موحدا لمكافحة الجرائم المعلوماتية[21]، و على كل دولة أن تستهدي به في تعديل أنظمتها القانونية أو استحداث قوانين جديدة بهدف تفعيل المواجهة القانونية لهذه الجرائم، ويشترط في هذه المعاهدات والاتفاقيات المواءمة والانسجام مع تشريعات مختلف الدول، لتنظيم التعاون الدولي في مكافحة الجرائم المعلوماتية، وتذليل كافة الصعوبات التي تعترض سبل ذلك التعاون، على أن تراعي هذه المعاهدات أهمية خاصة للمعاهدات الدولية السابقة، بغرض حماية الموضوعات التي أبرمت بشأنها، كالمعاهدات الأوربية بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، والاتفاقيات الدولية الخاصة بحقوق الطفل، وغيرها من الاتفاقيات[22].

وإذا كان التعاون الدولي هو السبيل الوحيد لمكافحة الجرائم المعلوماتية فإن هذا التعاون يقتضي التخفيف من تلك الفوارق بين القوانين العقابية الوطنية، لأن التنافر بين هذه الأنظمة يجعل المجرمين يبحثون عن الأنظمة القانونية التي تعاقبهم أو التي ترأف بحالهم[23].

ويعتبر التعاون الدولي خطوة نحو تدويل القانون الجنائي بشقيه الموضوعي والإجرائي، بالإضافة إلى أنه وسيلة من قبيل التدابير المانعة من إفلات المجرمين من العقاب عن الجرائم التي ارتكبوها، مما يحقق الردع العام والخاص.

---

[21] حسين بن سعيد الغافري، المرجع السابق، ص555.

[22] سامح أحمد بلتاجي موسى، المرجع السابق، ص544.

[23] محمد فتحي محمد أنور، تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف، دراسة مقارنة، رسالة دكتوراه كلية حقوق عين شمس ،2010، ص545.

لذلك يعتبر التعاون الدولي في مجال أنظمة العقابية من أهم أساليب مكافحة الجرائم المعلوماتية وملاحقة مرتكبيها، فبغير ذلك التعاون الدولي سيرتفع معدل ارتكاب تلك الجرائم، وذلك لعدم وجود اتفاقيات وآليات موحدة للقبض على مرتكبيها وكيفية التعامل معهم، مما يؤدي إلى إفلاتهم من العقاب. ولتكريس التعاون الدولي في هذا الميدان لابد من التركيز على العناصر الرئيسية التالية:

1-الانضمام إلى المعاهدات الدولية التي تكرس الجهود المبذولة دوليا في مجال مكافحة الجرائم المعلوماتية.

2-تنفيذ العملي لتلك المعاهدات الدولية، أي تنفيذ ما تنص عليه الاتفاقيات من إجراءات دون أي تأخير.

3-العمل على قدر إمكان على توحيد القوانين بين الدول المختلفة، والمتعلقة بمكافحة الجرائم المعلوماتية، مما يضمن عدم إفلات مرتكبيها من العقاب.

وتجدر الإشارة في هذا الشأن أن هناك فجوة بين الدول المتقدمة والدول النامية، حيث أن أغلب تشريعات الدول النامية تعد متأخرة في مواكبة المستجدات التشريعية العالمية المتعلقة بجرائم التقنية ، الهادفة إلى حماية المنظومة المعلوماتية من الجريمة المعلوماتية، لاسيما الحواسيب الآلية وشبكة الإنترنت، وقد يعزي ذلك إلى التأخر التقني في مجال المعلوماتية لهذه الدول[24]،وفي المقابل تزايدت خطط مكافحة هذه الجرائم في الدول المتقدمة، وانصبت الجهود على دراستها المتعمقة، وخلق آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية، خاصة المنظمات والهيئات الإقليمية الأوربية، وإدراكا لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية كان لابد للعديد من الدول من وضع قوانين وتشريعات خاصة أو العمل على جبهة قوانينها الداخلية للتعديلها، من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم[25].

[24] وليد الزبدي، القرصنة على الإنترنت والحاسوب، التشريعات القانونية، ط1، دار أسامة، عمان،2003، ص128.
[25] علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، دار الشاخوري العلمية، عمان ،2009، ص158.

ولعل أبرز ما يمكن أن يقال عن الجهود إقليمية –كآلية للتغلب على إشكالية القصور التشريعي في مجال مكافحة الجرائم

المعلوماتية–اعتمد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد قانونا نموذجية بموجب القرار رقم ٢٢٩ لسنة 1996، وبالرجوع إلى المذكرة الإيضاحية لهذا القانون وباستعراض الباب السابع الخاص بالجرائم ضد الأشخاص نجد أن هذا القانون قد احتوي على فصل خاص بالاعتداء على حقوق الأشخاص، حيث أشارت المواد ١٩١–وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية، وكيفية جمع المعلومات الإسمية، وكيفية الاطلاع عليها[26].

الفرع الثاني:

آلية التغلب على تحدي تنوع واختلاف النظم القانونية الإجرائية:

يعيش المجتمع الدولي في الوقت الحاضر موجة لإصلاح التشريعات الإجرائية لكي تواكب التطورات الحاصلة في عالم الجريمة المعلوماتية والتعديلات المتلاحقة في نصوص قانون العقوبات في شأنها، وتفعيل الإجراءات الجنائية وخاصة إجراءات الإثبات في مجال تقنية المعلومات.

وتميل الإصلاحات الإجرائية الحديثة إلى دمج كافة الابتكارات والتطبيقات الناتجة عن تقنية المعلومات في مجال الإجراءات الجنائية، وبصفة خاصة إثبات جرائم تقنية المعلومات، وتستجيب النصوص المستحدثة لاحتياجات الشرطة القضائية واستغلالها بالنسبة للتحقيقات في هذا المجال[27].

والناظر في المواثيق الدولية الصادرة عن الأمم المتحدة يجد أنها تشجع الدول الأطراف فيها على السماح باستخدام بعض تقنيات التحقيقات الخاصة، الشئ الذي

---

[26] نفس المرجع، ص159.

[27] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط1، دار النهضة العربية، القاهرة، 1999، ص59.

يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال، وقد أبرمت العديد من الاتفاقيات الدولية في مجالات التعاون الدولي، وتستهدف التقريب بين القوانين الجنائية الوطنية من أجل مكافحة الجرائم عابرة الحدود، وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة والاعتراف بالأحكام الجنائية الأجنبية[28].

فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام2000 تشير في هذا الشأن إلى التسليم المراقب، والمراقبة الإلكترونية، وغيرها من أشكال المراقبة والعمليات المستترة، والتي تعد من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها، وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف، في سياق نظم المساعدة القانونية المتبادلة.

وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتي، حيث نصت المادة ٢٩ على سرية حفظ البيانات المعلوماتية المخزنة، وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة، عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر، والذي ينوي الطرف طالب المساعدة أن يقدم طلبة للمساعدة بشأنها، بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، أو الحصول أو الكشف عن البيانات المشار إليها.

وكذلك يمكن التغلب على هذا التحدي الدولي من خلال إيجاد قنوات اتصال فعالة فيما بين الدول المختلفة، فهناك حالات خطرة وأخرى يكون عنصر السرعة فيها حاسم، ولذا فإن وجود مثل هذه القنوات يساعد في تحقيق وتعقب مثل هذه الجرائم[29].

[28] حسين سعيد الغافري، المرجع السابق، ص556.
[29] سامح أحمد بلتاجي موسى، المرجع السابق، ص545.

كما يجب تدعيم التعاون بين سلطات الشرطة في الدول المختلفة بناء على الاتفاقيات الدولية، حيث إن لهذا التعاون أهمية كبيرة، حيث يسهل في عملية تعقب الجرائم المعلوماتية والقبض على مرتكبيها[30].

الفرع الثالث:

آلية التغلب على تحدي تنازع الاختصاص القضائي الدولي:

يمكن التغلب على هذا التحدي من خلال اعتبار جميع الجرائم المعلوماتية من الجرائم الدولية، وتدخل في الاختصاص القضائي العالمي، أو ما يعرف بالولاية القضائية العالمية، ويعني هذا أن يعطي الحق للدول بملاحقة ومحاكمة مرتكبي الجرائم الدولية دون أي اعتبار لجنسية مرتكبيها، أو المكان الذي ارتكبت فيه الجريمة، بما مفاده أن ينعقد الاختصاص القضائي العالمي لأي دولة ترغب في ملاحقة مرتكبي الجرائم الدولية[31].

ويعتمد الاختصاص القضائي بجريمة ما في الأحوال العادية على الصلة بين الدولة التي ترفع الدعوى وبين الجريمة نفسها، وهي صلة إقليمية في العادة، أما في حالة الجرائم الدولية فيكفي أن تكون هذه الصلة أن هذه الجرائم تشكل تهديدا لأمن وسلم المجتمع الدولي.

ويعني مبدأ العالمية أن كل دولة بإمكانها أن تخضع لسلطتها كل جريمة ينص عليها قانونها العقابي، بغض النظر عن مكان ارتكابها أو شخص مرتكبها، أو المجني عليه، أو جنسيتهم، ودون نظر عما إذا كان القانون الأجنبي يعتبرها جريمة من عدمه، وبعبارة أخرى فإن هذا المبدأ يعني وجوب تطبيق القانون الجنائي الوطني

---

[30] جميل عبد الباقي الصغير، المرجع السابق، ص86.

[31] عمرو زكي عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة المؤتمر الجوانب القانونية للتجارة القانونية مقر الجامعة العربية، يناير2001، ص60.

على مرتكب أي جريمة يتم القبض عليه في الأراضي الوطنية، بغض النظر عن مكان ارتكابها، أو أيا كانت جنسية فاعليها[32].

وتنص بعض التشريعات الجنائية المقارنة على مبدأ العالمية في عدد من الجرائم ذات الخطورة، مثل جرائم الحرب، ونقض الالتزامات الدولية، والجرائم الإنسانية، لتمارس اختصاصها في الملاحقة الجنائية، وتعقب المجرمين لمحاكمتهم أمام محاكمها[33].

ويهدف مبدأ العالمية إلى التصدي لتنامي الظواهر الإجرامية، ذات الأبعاد الدولية، من خلال تجاوز القيود التي يفرضها مبدأ الإقليمية، فينعقد الاختصاص للقاضي الجنائي لأي دولة من دول العالم بغض النظر عن المكان الذي ارتكبت فيه الجريمة المعلوماتية أو جنسية من ارتكبها أو جنسية المجني عليه أو نوع الجريمة. ويؤسس هذا المبدأ على فكرة التضامن بين الدول في مكافحة الجرائم، فالتدخل الدولي وفقا لهذا المبدأ يهدف إلى تجنب إفلات المجرمين من العقاب، ولضمان محاكمة الجناة بغض النظر عن جنسياتهم أو جنسية المجني عليهم، أو مكان ارتكابه الجريمة أو نوع الجريمة، من أجل المصلحة المشتركة أو اعتبارات الإنسانية، ولقد نظر الفقه الجنائي إلى مبدأ العالمية بوصفه مكملا لغيره من المبادئ التي تحكم نطاق تطبيق العقوبات، لسد ما يترتب عليها من نقص. وتطبيقا المبدأ العالمية فإن دولة القبض تختص بمحاكمة الجاني عن الجرائم التي ارتكبها في الخارج، لأن القبض شرط لانعقاد الاختصاص العالمي في حالة تعذر تسليم المتهمين إلى الدولة التي وقعت فيها الجريمة.

ولا شك أن هذا المبدأ يعد أداة رئيسية لمكافحة الجريمة المنظمة عبر الوطنية، وبخاصة الجرائم المعلوماتية، لما تفتضيه هذه الجرائم من طبيعة خاصة ذات أبعاد

---

[32] أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، ط6، دار النهضة العربية، القاهرة، 1996، ص219.

[33] وتجدر الإشارة الى أن المشرع الجزائري لم يبين هذا المبدأ في قانون العقوبات، ومع ذلك يرى بعض الفقه في الجزائر أن هذا المبدأ واجب التطبيق في أي دولة لم تنص عليه بالنسبة لجرائم القرصنة عبد الرحمان خلفي، محاضرات في القانون الجنائي العام، دراسة مقارنة، دار الهدى، الجزائر، سنة 2013، ص 73 إلى ص 79.

مدمرة للمجتمع الدولي، كما أنه يلازم الجرائم ذات البعد الدولي، ويجد أساسه في المصلحة المشتركة للدول[34].

الفرع الرابع:

آلية التغلب على التحدي الخاص في مجال التدريب:

يمكن التغلب على هذا التحدي من خلال عدة أمور، وهي كالآتي:

1-إجراء المزيد من الحملات التوعوية للتنبيه بمخاطر جرائم المعلومات والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها.

2-التنسيق بين الأجهزة المعينة بتدريب رجال تنفيذ القانون وإيجاد برامج تدريبية مشتركة تناسب جميع الفئات.

3-القيام ببعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب

وجهات النظر بشأنها[35].

الفرع الخامس:

آلية التغلب على التحديات الخاصة بالإنابة القضائية الدولية:

أولا: آلية التغلب على التحدي المتعلق بفكرة السيادة:

مما لاشك فيه أن فكرة السيادة تمثل خاصية مهمة للسلطة السياسية ،التي تعتبر ركن أساسي للدولة ، فهي السند القانوني الذي تستند إليه الدولة لمباشرة صلاحيتها

[34] فائزة يونس الباشا الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية، رسالة دكتوراه، حقوق القاهرة، 2001، ص372.
[35] غانم مرضي الشمري، المرجع السابق، ص131.

الداخلية والخارجية[36]، لذا من غير المتصور قيام التعاون الدولي بين دول لا تتمتع بالسيادة الوطنية، ولكن إزاء حرص كافة الدول علي التمسك بسيادتها المطلقة والتي لا تقيدها أي قيود لتحقيق مصالحها القومية والتي قد تتعارض مع مصالح المجتمع الدولي وتصطدم بها، إذ ظهر أن التذرع باعتبارات السيادة من الممكن أن يتسبب في سهولة هروب المجرمين من العدالة وتهريب الأموال المتحصلة من الجرائم، ولاشك أن الضرر الناتج يكون عاما يشمل كل المجتمع الدولي ،لذا أصبح من الضروري لتحقيق التعاون بين دول العالم ، التخلي عن فكرة السيادة المطلقة للدول، حيث بدأ الطابع المطلق للسيادة في الانحسار في مواجهة التضامن والتعاون الدولي لمواجهة التهديدات التي تهدد المجتمع الدولي.[37]

وإذا كان إجراء الإنابة القضائية الدولية هو الوسيلة التي يتحقق بها وإذا كان إجراء الإنابة القضائية الدولية هو الأسلوب التي يتحقق به مصالح الجماعة الدولية في مكافحة الجريمة دون الإخلال بالسيادة الوطنية للدول، إلا أن هذا الإجراء تفتضيه ضرورات عملية أهمها أن سلطات الدولة كأصل عام لا تستطيع ممارسة اختصاصاتها مثل الملاحقة والاستدلال والتحقيق والاتهام ومحاكمة وأخير تنفيذ العقاب خارج إقليمها الوطني إلا بإجراء الإنابة القضائية فهي تساعد على التغلب على تلك التحديات، فتقوم الدولة التي يستلزم اتخاذ الإجراء في إقليمها بتنفيذ ذلك الإجراء عن طريق سلطاتها القضائية نيابة عن الدولة التي انعقد لها الاختصاص[38]

ويبرز احترام سيادة الدولة التي يتم اتخاذ إجراء الإنابة في إقليمها في الآتي:

1-أنها لا تتم إلا بناء على طلب يقدم من الدولة صاحبة الاختصاص الجنائي وفقا للأسلوب الذي تحدده الاتفاقية السارية بينها وبين الدولة المطلوب إليها، وفي حدود ما نصت عليه تلك الاتفاقية.

---

[36] ماهر عبد الهادي، نظرية السلطة السياسيــة في دولة، ط2، دار النهضة العربية، بيروت،1984، ص11.

[37] علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، دار النهضة العربية، القاهرة 2000، ص.ص230-231.

[38] طارق الحسيني منصور، المحكمة الجنائية الدولية كتطور لمفهومي المسؤولية والسيادة، مع التطبيق على قضية دارفور، رسالة دكتوراة، حقوق المنصورة،2009، ص913.

2_خضوع ذلك الطلب للفحص من قبل الدولة المطلوب إليها، للتحقق من استيفاء موجبات تنفيذ الإنابة وفقا للاتفاقية المبرمة بهذا الخصوص.

3–يتم تنفيذ الإجراء المطلوب وفقا لقانون الدولة المطلوب إليها، فعندما ترسل إنابة قضائية خارجية من قاض مصري إلى قاض أجنبي فإن تنفيذ هذه الإنابة يخضع للقواعد السارية في قانون دولة القاضي الأجنبي وليس القانون المصري. والإنابة بهذا المعنى لا تعني إنقاص من سيادة الدول، بل تعني تعاون بين سيادات الدول لأجل تحقيق مصالحها المشتركة[39]، لذلك اتجهت الدول الى إبرام اتفاقيات ثنائية وجماعية خاصة بمساعدة القضائية في ضوء مكافحة الجرائم المعلوماتية، ولعل أبرز ما استحدثه أسلوب التحقيق عن بعد والذي أسهم بتخفيف من حدة تأثير فكرة السيادة التي كانت تعرقل التعاون الدولي في مجال مكافحة الجرائم[40].

ثانيا/ آلية التغلب على البطء في الإجراءات:

*التواصل المباشر بين السلطات القضائية في الدولتين:

وهو يعد أحد الأساليب المهمة للتغلب على البطء في الإجراءات، حيث بمقتضى هذه الوسيلة يتم الاتصال مباشرة بين السلطة القضائية الطالبة والسلطة القضائية المطلوب إليها، ويعد هذا الطريق أكثر اختصارا وبالتالي أكثر سرعة ومرونة، وهو بالتالي يتلاءم مع أحوال الضرورة والاستعجال التي تتطلب سرعة اتخاذ إجراء من إجراءات التحقيق، خشية من استحالة اتخاذ الإجراء بفوات الوقت، ولهذا فقد نصت غالبية التشريعات الوطنية والاتفاقيات الدولية المعنية بتنظيم الإنابة القضائية الخارجية على جواز اتباع هذا الطريق في أحوال الاستعجال[41].

وهذا بالفعل ما اوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية والذي انعقد في بانكوك في الفترة من 18 – 4/25 2005م، حيث أكدت

[39] أمين عبد الرحمن عباس، الإنابة القضائية، رسالة دكتوراة، حقوق الإسكندرية، 2011، ص 233.
[40] عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة،2001، ص177.
[41] أمين عبد الرحمن عباس، المرجع السابق، ص298.

على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما وبغية ضمان تنفيذ الطلبات في الوقت المناسب[42].

حيث أن مرور إجراءات التعاون القضائي بالطريق الدبلوماسي يجعلها تتسم بالبطء وكثرة الشكليات، وهو ما يتعارض مع طبيعة الجرائم المعلوماتية التي تتميز بسرعة عبور وتبادل المعلومات من خلال شبكتها، لذلك فإن مكافحة الجرائم المتعلقة بالإنترنت تقتضي ردود سريعة، خشية التلاعب في البيانات التي قد تشكل دلي" ضد المتهم. وبالنسبة للرد على طلبات التماس المساعدة فإنه من الضروري استجابة الفورية و السريعة على هذه الطلبات لأجل ذلك تنص المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة، حيث أكدت على ذلك المادة25/03من اتفاقية بودابست، حيث نصت على ما يلي:" يمكن لكل طرف في حالة الاستعجال أن يقدم طلب المساعدة المتبادلة أو الاتصالات عن طريق وسائل سريعة للاتصال، كالفاكس أو البريد الإلكتروني، وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق بما في ذلك التشفير لو كان ضروريا– مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوبا بواسطة الدولة الموجهة إليها الطلب، ويجب على الدولة المقدم إليها الطلب أن توافق وأن ترد على الطلب المقدم إليها عن طريق أية وسيلة من الوسائل العاجلة للاتصال"[43]

[42] حسين الغافري، المرجع السابق، ص559.
[43] الفقرة 3 من المادة 25من اتفاقية بودابست لعام 2001.

الفرع السادس:

آلية التغلب على التحديات الخاصة بتسليم المجرمين في مكافحة الجرائم المعلوماتية:

أولا/آلية التغلب على ازدواجية التجريم:

يمكن التغلب على هذا التحدي من خلال التزام الدول بتجريم الأفعال الواردة في الاتفاقيات المبرمة فيما بينها ،فإن ذلك يوفر الأساس الكافي لتحقيق شرط ازدواج التجريم، حيث أكدت على ذلك اتفاقية الأمم المتحدة لمكافحة الفساد في نص المادة 2/23،حيث نصت على الآتي:" "في مسائل التعاون الدولي كلما اشترط توافر ازدواجية التجريم وجب اعتبار ذلك الشرط مستوفي، بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم التي تدرجه فيها الدولة الطرف الطالبة، أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة، إذا كان السلوك الذي يقوم عليه الجرم الذي تلتمس بشأنه المساعدة بعد يعتبر فعلا إجراميا في قوانين كلا الطرفين".[44]

ويمكن أيضا التغلب على هذا التحدي من خلال التخفيف من التطبيق الصارم لهذا الشرط وذلك إما برد الأفعال والتي تتطلب أن تجريم كجرائم أو أفعال مخلة بمقتضى قوانين الدولتين معا أو بمجرد السماح بالتسليم لأي سلوك تم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة، وهذا بالفعل ما ركزت عليه الاتجاهات والتطورات التشريعية الخاصة بنظام تسليم المجرمين[45].

ثانيا/ آلية التغلب على تحدي التزاحم في طلبات التسليم:

لم يستقر الفقه الدولي على تحديد وترتيب التسليم في حالة تزاحم طلبات التسليم، حيث توجد الاختلافات الكثيرة ترتيب في هذه الأولويات، بل إن هذا الاختلاف

---

[44]الفقرة 2من المادة 23 من اتفاقية الأمم المتحدة لمكافحة الفساد لعام 2016.

[45] غانم مرضي الشمري، المرجع السابق، ص130.

موجود أيضا على نطاق الدولة الواحدة في كل اتفاقية على حدة، وهذا كله يرجع بصفة أساسية إلى اختلاف مصالح وأولويات الدول ومصالحها مع أطراف المتعاقدة.[46]

حيث اعتمدت اتفاقية العربية الخاصة بالتسليم على معيار جسامة الفعل الإجرامي، ويظهر ذلك في المادة ١٣ منها، حيث تقضي بأنه "إذا قدمت إلى الدولة المطلوب إليها عدة طلبات من مختلفة بشأن تسليم متهم من أجل نفس الجريمة، فتكون الأولوية التسليم للدولة التي أضرت الجريمة بمصالحها، ثم الدولة التي ارتكبت الجريمة على أرضها، ثم للدولة التي ينتمي إليها المطلوب تسليمه، أما إذا كانت طلبات التسليم خاصة بجرائم مختلفة، فتكون الأولوية التي طلبت التسليم قبل غيرها".

ولكن يزداد هذا التحدي تعقيدا في حالة الشخص متعدد الجنسيات، حيث تتعدد أسباب تعدد الجنسية فمنها ما يتحقق وقت الميلاد، ومنها ما يتحقق في تاريخ لاحق على الميلاد، ومنها ذلك التعدد المعاصر للميلاد، وهو أكثر الحالات شيوعا[47]

ولاشك أن مشكلة التنازع بين الجنسيات تختلف حسب المبدأ الذي تتبناه الدولة المطلوب إليها، سواء كان مبدأ تسليم الرعايا أو حظر تسليمهم، ولم تعالج التشريعات هذا الأمر، وتركته لمبدأ العاملة بالمثل وقواعد المجاملات الدولية وفي حالة ما إذا كان الشخص المطلوب يتمتع بجنسية الدولة الطالبة إلى جانب دولة أخرى فإن هذه الدولة بالتأكيد ستتمسك بالقواعد العامة التي تطبقها في هذا الخصوص، فقد ترفض تسليمه للدولة الثانية حتى ولو كان يحمل جنسيتها، وقد توافق على التسليم في ضوء الضوابط والمعايير التي تحددها، انطلاقا من حقوقه كمواطن.

وتزيد المشكلة أكثر إذا لم يكن الشخص المطلوب يحمل جنسية الدولة المطلوب إليها، وبالتالي يخضع الأمر هنا كله إلى العلاقات الدبلوماسية، لأنه لا يمكن وضع

---

[46] أحمد محمد السيد عبد الله، التعاون الدولي في الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراه، حقوق، المنصورة، 2009، ص.ص394-395.

[47] فؤاد رياض، الوسيط في الجنسية ومركز الأجانب، ط5، دار النهضة العربية، القاهرة، ص80.

معيار محدد يفصل بين الدول التي يحمل جنسيتها شخص واحد، ويكون القرار في النهاية بيد الدولة المطلوب إليها، وهي التي ستملك ترجيح دولة على أخرى لإعادة الشخص المطلوب إليها، لكن من الممكن أن يخضع التسليم هنا لمبدأ المعاملة بالمثل ليفصل في التنازع بين الدول، بالإضافة إلى قواعد المجاملات الدولية التي تحددها طبيعة العلاقة بين الدول الأطراف في التسليم[48]

ولكن هناك عدة حالات يجوز فيها للدولة المطلوب إليها التسليم أن ترفض ذلك الطلب وتمتنع عن التسليم، وهذه الحالات كالآتي:

1_إذا توافرت أسباب جدية للتخوف من أن طلب التسليم قد قدم بغرض معاقبة الشخص المطلوب تسليمه لأسباب متعلقة بجنسيته، أو ديانته، أو أصله العرقي، أو توجهاته وآرائه السياسية، أو انتمائه لجماعة أو طائفة معينة.

2_إذا كانت هناك أسباب موضوعية تدعو للاعتقاد بأن الشخص المراد تسليمه سيتعرض للتعذيب، أو المعاملة أو العقوبة القاسية أو اللاإنسانية، أو الإحاطة بالكرامة أو المخالفة المبادئ وحقوق الإنسان، وهو عمل لا يليق بالدولة المطلوب إليها التسليم أن تساهم في تنفيذه[49]

3_عدم وجود اتفاقية تسليم مع الطرف طالب التسليم، أو أن المعاهدة المبرمة لا تشمل مثل هذا الطلب، وهذه الحالة نصت عليها اتفاقية بودابست في المادة 3/24.

ولكن من وجهة نظرنا نرى أن يستند رفض التسليم إلى ما يبرره منطقيا، وألا يكون عائقا أمام تحقيق العدالة وخاصة في مجال مكافحة الجرائم المعلوماتية، لما تكتنفه تلك الجرائم من خطورة وصعوبة، وبما تطلبه من تعاون دولي لتصدي لمرتكبيها ومكافحته.

[48] أحمد عبد الكريم سلامة ،المبسوط في شرح نظام الجنسية، ط1،دار النهضة العربية، القاهرة 1993،ص574.
[49] سامح أحمد بلتاجي موسى، المرجع السابق، ص521

هناك العديد من الأمثلة العملية للتعاون الدولي في مجال تسليم مرتكبي الجرائم المعلوماتية، ومنها:[50]

– عملية محطم الجليد، قامت بها بوروبول في 14 يونيو 2005، تم خلالها مداهمة وتفتيش أماكن في ثلاث عشرة دولة أوروبية هي: النمسا، بلجيكا، فرنسا، ألمانيا، المجر، أيسلندا، إيطاليا، هولندا، بولونيا، البرتغال، سلوفاكيا، السويد، بريطانيا، كما تم توقيف أفراد في كل من فرنسا، بلجيكا، المجر، أيسلندا، السويد، ثم تم تسليم المتهمين إلى بريطانيا التي قامت بتقديمهم للمحاكمة الجنائية، وحكم القضاء بإدانتهم

–عملية أوديسيوس التي تمت في 29 فبراير 2004، بمبادرة من يوروبول، وقامت قوات الشرطة خلالها بعمليات شملت 10 دول هي (استراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج، بيرو، اسبانيا، السويد، بريطانيا) وتم تسليم المتهمين إلى سلطات التحقيق في بريطانيا، حتى قضي بإدانتهم.

[50] http://www.pogar.org/publications/ruleoflaw/cybercrime تاريخ إعلان 6_1-2021،الساعة6:00am

خلاصة الفصل الثاني:

على الرغم من اعتبار التعاون الدولي حجر الأساس في مكافحة الجرائم المعلوماتية، الا أنه تواجه العديد من التحديات على الصعيد الدولي والوطني.

حيث تتمثل التحديات الدولية في العديد من العراقيل التي تنج سواء عن تعارض مصالح أشخاص القانون الدولي، أو التي تنج عن تنازع الاختصاص القضائي الدولي نتيجة صعوبة اتباث هذه الجرائم و صعوبة إجراءات المتابعة القضائية، وأما التحديات الوطنية تتمثل في العراقيل التي تنج عن عدم ملائمة غالب التشريعات الوطنية لطبيعة الخاصة بهذه الجرائم، وكذلك نتيجة صعوبة التحقيق فيها.

يمكن التغلب على كل هذه التحديات من خلال ابرام اتفاقيات دولية تزيل التعارض بين أشخاص القانون الدولي من خلال انشاء قانون نموذجي موحد لمكافحة الجرائم المعلوماتية.

الخاتمة:

يعد التعاون الدولي القاعدة الأساسية في مكافحة الجريمة المعلوماتية، إلا أن هذا التعاون يفقد فاعليته في ظل العديد من التحديات على المستوى الدولي والوطني، والتي عادة ما ترتبط بمصالح الدول وفكرة السيادة.

في نهاية الدراسة توصلنا إلى مجموعة من النتائج والتوصيات، كالآتي:

أولا/النتائج:

توصلنا خلال هذه الدارسة إلى مجموعة من النتائج، لعل من أبرزها ما يلي:

1-تمثل الجرائم المعلوماتية-وما يعتريها من تحديات خطرا يهدد الاستقرار الدولي، لذلك أهتم المجتمع الدولي بمكافحتها.

2- بعد مبدأ التعاون الدولي في الوقت الراهن من أهم المبادئ القانونية الدولية التي لا يتطرق إليها الشك، وقد ظهرت أهمية هذا المبدأ في مجال مكافحة الجريمة، مع تعدد وتشعب التطورات التي لحقت بظاهرة الجريمة وأساليب ارتكابها.

3-يعد مصطلح التعاون الدولي لمكافحة الجريمة من المفاهيم التي يصعب وضع تعريف جامع مانع لها، لعدة أسباب منها:

أ -اتساع المجال والصور والأشكال التي يمكن أن يتخذها هذا التعاون، عدم إمكان حصرها أو حصر الوسائل الجديدة والمتجددة التي تجعل هذا التعاون ظاهرة متغيرة ومتطورة بشكل مستمر.

ب-ارتباط هذا التعاون بمفاهيم الإجرام ومكافحته، وهي مفاهيم يصعب معها وضع تصور محدد وإطار ثابت لأي منها.

4-لا تستطيع أي دولة لوحدها مكافحة الجرائم المعلوماتية، لذلك لا بد من الدخول في اتفاقيات الدولية الخاصة بمكافحة الجرائم المعلوماتية.

5_يمثل التعاون الأمني الدولي بين أجهزة الشرطة الجنائية المخصصة لمكافحة الجرائم المعلوماتية في الدول أحد الوسائل الهامة التي يمكن من خلالها منع الجرائم المعلوماتية أو الإقلال منها.

6-يعد التعاون الدولي أسلوب فعال لمكافحة الجرائم المعلوماتية، نظرا لكونها غالبا ما تتم في أماكن مختلفة في العالم باستخدام تقنيات حديثة، غير أن ذلك التعاون تعترضه عدة تحديات، سواء على المستوى الوطني ،لعل من أهمها عدم كفاية وملائمة القوانين القائمة، صعوبة إثبات الجرائم المعلوماتية- أو المستوى الدولي أهمها القصور التشريعي للدول، تنوع واختلاف النظم القانونية الإجرائية، تنازع الاختصاص القضائي الدولي، التحديات الخاصة بالإنابة القضائية وتسليم المجرمين والتي يجب للتغلب عليها بذل المزيد من الجهد لتخطيها والقضاء عليها.

ثانيا/الاقتراحات:

من وجهة نظرنا المتواضعة يمكن تقديم مجموعة من التوصيات لجعل مكافحة الجرائم المعلوماتية أكثر فاعلية، وهي الآتي:

1-كآلية للتغلب على إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الوطني يتعين على كل دولة الآتي:

أ. أن تجرم في تشريعاتها جميع الأفعال التي تشكل انتهاك للحقوق المعلوماتية.

ب-اتخاذ التدابير التشريعية التي تلزم لتخويل سلطاتها المعنية صلاحيات ضبط وإحضار الأشخاص المتورطين في الجرائم المعلوماتية.

ج. إضفاء صفة الضبطية القضائية على العاملين في مجال المعلومات من غير رجال الشرطة، بحيث إذا حدث ووجدت الجريمة يسهل التعامل معها.

د-تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناء على اتفاقيات دولية.

2–ضرورة إيجاد أساس تشريعي موحد لمفهوم الجريمة المعلوماتية من أجل تحديد الأفعال التي تشكل جريمة معلوماتية، إضافة إلى عقد اتفاقيات ثنائية أو جماعية يكون هدفها التنسيق وتوحيد الجهود قصد محاربة هذه الجرائم.

3_للتغلب على إشكالية القصور التشريعي للدول في مكافح الجرائم المعلوماتية على المستوى الدولي يتعين توحيد النظم العقابية الخاصة بالإجرام الرقمي.

4–لتفعيل التعاون الدولي في مجال التشريع العقابي كآلية للتغلب على تحدي القصور التشريعي للدول في مكافحة الجرائم المعلوماتية–يتعين التركيز على العناصر التالية:

أ. الانضمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون والتنسيق بين الجهود التي تبذلها الدول في مكافحة الإجرام المعلوماتي.

ب. إدخال تلك المعاهدات حيز التنفيذ الفعلي.

ج–العمل على وجود أكبر قدر من التناسق والتطابق فيما بين قوانين الدول المختلفة والمتعلقة بمكافحة الجرائم المعلوماتية

5_للتغلب على تحدي تنازع الاختصاص القضائي الدولي في مكافحة الجرائم المعلوماتية على المستوى الدولي يتعين اعتبار جميع الجرائم المعلوماتية جرائم دولية تدخل في الاختصاص القضائي العالمي، وهو ما يعني إعطاء الحق للدول بملاحقة ومحاكمة مرتكبي الجرائم الدولية، دون أي اعتبار لجنسية مرتكبيها، أو المكان الذي ارتكبت فيه الجريمة.

6–للتغلب على إشكالية البطء في إجراءات الإنابة القضائية الدولية في مكافحة الجرائم المعلوماتية يتعين الاتصال المباشر بين السلطات القضائية الدولية الطالبة والمطلوب إليها.

7–كآلية للتغلب على التحدي الخاص بالتزاحم في طلبات التسليم في مكافحة الجرائم المعلوماتية يتعين عقد اتفاقية دولية تتضمن وضع ضوابط موضوعية وآليات محددة يتبعها المجتمع الدولي، على أن يتم وضع هذه الضوابط والآليات بصفة موضوعية مجردة وبعيدة عن مصالح دولة معينة.

قائمة المصادر والمراجع:

أولا: المصادر:

***المصادر الخارجية:**

1-الاتفاقية بودابست بشأن الجرائم الإلكترونية، الموقعة في بوداست في تاريخ23 نوفمبر2001.

2-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة في 21 ديسمبر2010.

ثانيا: المراجع:

***الكتب:**

1 -أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، ط6، دار النهضة العربية، القاهرة، 1996، عبد الرحمان خلفي، محاضرات في القانون الجنائي العام، دراسة مقارنة، دار الهدى، الجزائر، سنة 2013.

2-أحمد هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة 1997.

3-جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالأنترنت، دار النهضة العربية، 2002.

4-حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، ط1، دار الكتب القانونية، القاهرة، 2002.

5-حسين صالح عبيد، القضاء الجنائي الدولي، ط1، دار النهضة العربية، 1977.

6 –خالد ممدوح أمن الجريمة الالكترونية، الدار الجامعية الاسكندرية 2008.
7–رستم هشام فريد، الجوانب الاجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، أسيوط، 1994.

8 –سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط1، دار النهضة العربية، القاهرة، 1999.

9–سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات ط1 دار النهضة العربية القاهرة 1994 .5رستم فريد هاشم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994.
10–طارق إبراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، 2009.9وليد الزبدي، القرصنة على الإنترنت والحاسوب، التشريعات القانونية، ط1، دار أسامة، عمان،2003.

11–عادل عبد العال ابراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، ط1، دار الجامعة الجديدة، الاسكندرية، 2015.

12 –عبد الرحمان فتحي سمحان، تسليم المجرمين في ظل قواعد القانون الدولي، دار النهضة العربية، 2012.

13–عبد الرؤوف معدي، شرح القواعد العامة لإجراءات جنائية وفقا لآخر التعديلات، دار النهضة العربية، القاهرة، 2002.

14–عفيفي عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط1، دار الكتب القانونية، القاهرة 2002.

15 –عكاشة محمد عبدالعال، القانون الدولي الخاص، دار الجامعة الجديدة، الإسكندرية، 1999.

16–علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، دار النهضة العربية، القاهرة 2000.

17 –علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، دار الشاخوري العلمية، عمان، 2009.

18 –فؤاد رياض، الوسيط في الجنسية ومركز الأجانب، ط5، دار النهضة العربية، القاهرة،1999.

19–قورة نائلة جرائم الحاسب الاقتصادية، ط1 دار النهضة العربية، القاهرة، 2000.
20–لصغير جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، ط1، دار النهضة العربية، القاهرة 1992.

21 –ماهر عبد الهادي، نظرية السلطة السياسية في دولة، ط2، دار النهضة العربية، بيروت،1984.

22–مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة، دار الكتب، القاهرة، 2003.

23–ممدوح بحر، حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر، عمان، 1996.

24 –الرازي بن أبي بكر محمد، مختار الصحاح، إخراج دائرة المعاجم، مكتبة لبنان، بيروت ،1989

25 –منير محمد الجنبيهي –ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي، دار الفكر الجامعي، الإسكندرية، 2004.

–26 نبيلة هبة هروال، الجوانب الاجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي ،2007.

27 –هدى حامد قشقوش، الجريمة المنظمة القواعد الموضوعية والاجرائية والتعان الدولي، دار النهضة العربية، القاهرة، 2002.

28 –الهيثي محمد حماد، التكنولوجيا الحديثة والقانون الجنائي، ط1 دار الثقافة للنشر والتوزيع، عمان، 2004.

29 –يونس عرب، دليل أمن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والأنترنت، ط1، اتحاد المصارف العربية ،2002.

***المذكرات وأطروحات:**

1 –أحمد محمد السيد عبدالله، التعاون الدولي في الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراه، حقوق، المنصورة، 2009.

2 أحمد محمد السيد عبدالله، التعاون الدولي في الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراة، كلية حقوق المنصورة 2009.

3– خالد بن مبارك القحطاني ، التعاون الأمني الدولي في مواجهة الجريمة المعلوماتية عبر الوطنية ، أطروحة دكتورة ، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، دار النهضة العربية الرياض ، 2000

4– سالم محمد سليمان الأوجلي ، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات ، رسالة دكتوراة كلية الحقوق عين شمس ، 1997.

5– فهد عبد الله العبيد ، الإجراءات الجنائية المعلوماتية، رسالة دكتوراة، كلية الحقوق عين شمس، 2012

6-طارق الحسيني منصور، المحكمة الجنائية الدولية كتطور لمفهومي المسؤولية رسالة دكتوراة، حقوق المنصورة، 2009.

ثالثا/ المقالات:

1-أسماهان بوضياف، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، مجلة الشروق، العدد 11 سبتمبر 2018.

2-صورية بوربابة، التعاون الدولي في مكافحة الجريمة المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد الأول، جويلية 2019.

3 -محمد مرزوقي، جرائم الحاسب الآلي، المجلة العربية للفقه والقضاء تصدر عن الأمانة العامة لجامعة الدول العربية، العدد الثامن والعشرون، 2003.

4-محمد عقاد، جريمة التزوير في المحررات للحاسب الآلي، دراسة مقارنة، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي. حسني عصام الأطرش ة محمد عساف، معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الأجهزة الأمنية، مجلة جامعة الشارقة، المجل د16، العدد1، 16يونيو 2018.

5-عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة المؤتمر الجوانب القانونية للتجارة القانونية، مقر الجامعة العربية، يناير 2001.

6 -محمد مرزوقي، جرائم الحاسب الآلي، المجلة العربية للفقه والقضاء تصدر عن الأمانة العامة لجامعة الدول العربية، العدد الثامن والعشرون، 2003.

7-محمد عقاد، جريمة التزوير في المحررات للحاسب الآلي، دراسة مقارنة، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

مجلس أوروبا

سلسلة المعاهدات الأوروبية رقم 185

التقرير التفسيري لاتفاقية الجريمة الإلكترونية

بودابست، في ٢٣ نوفمبر/تشرين الثاني ٢٠٠١

أولا – تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (٨ نوفمبر/تشرين الثاني ٢٠٠١) وفتح باب التوقيع على الاتفاقية في بودابست، في ٢٣ نوفمبر/تشرين الثاني ٢٠٠١، بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية.

ثانيا – لا يشكل نص هذا التقرير التفسيري أداة توفر تفسيرا ذي حجية للاتفاقية، على الرغم من أنه قد يكون ذا طبيعة تسهل تطبيق الأحكام الواردة فيه.

أولا. المقدمة

١. غيرت ثورة تكنولوجيات المعلومات المجتمع بشكل جوهري، ومن المحتمل أن تستمر في تغييره في المستقبل القريب، علاوة على أنها يسرت إنجاز العديد من المهام. ولئن كانت بعض فئات المجتمع فقط قد نجحت، أصلا، في ترشيد إجراءات عملها بمساعدة تكنولوجيا المعلومات، فإن كافة فئات المجتمع لم تسلم من تأثيرها، حيث اجتاحت تكنولوجيا المعلومات بشكل أو بآخر تقريبا كل جوانب الأنشطة البشرية.

٢. لعل إحدى السمات البارزة لتكنولوجيا المعلومات تتلخص في الوقع الذي أحدثته وستحدثه على تطور تكنولوجيا الاتصالات السلكية واللاسلكية. وقد تجاوزت الاتصالات الهاتفية، التي تنطوي على نقل صوت الإنسان، تبادل كميات هائلة من البيانات، بما في ذلك الصوت، والنص، والموسيقى والصور الثابتة والمتحركة. لم يعد هذا التبادل يحدث سوى بين البشر، ولكن أيضا بين البشر والحواسيب، وبين أجهزة الكمبيوتر نفسها. فضلا عن ذلك، تمت استعاضة عن الاتصالات بدوائر التبديل بشبكات تبديل الرزم. ولم يعد الربط المباشر يكتسي أي أهمية؛ يكفي أن يتم إدخال بيانات في شبكة مع عنوان الوجهة أو إتاحتها لأي شخص يريد النفاذ إليها.

٣. يعتبر الاستخدام واسع النطاق للبريد الإلكتروني والولوج إلى العديد من المواقع الإلكترونية مثالا لهذه التطورات، التي غيرت مجتمعنا بعمق.

٤. أدت سهولة الولوج إلى المعلومات المضمنة في نظم الكمبيوتر وإمكانية البحث عنها، بالإضافة إلى الإمكانات غير المحدودة لتبادلها ونشرها بشمل عملي، بغض النظر عن بعد المسافات الجغرافية، إلى حدوث نمو هائل في حجم المعلومات المتاحة والمعرفة التي يمكن استخلاصها من منها.

الباب الأول: المبادئ العامة ذات الصلة بالتعاون الدولي

المبادئ العامة ذات الصلة بالتعاون الدولي (المادة ٢٣)

٢٤١.تحدد المادة ٢٣ ثلاثة مبادئ عامة فيما يتعلق بالتعاون الدولي بموجب الفصل الثالث.

٢٤٢.توضح المادة، في المقام الأول، أن التعاون الدولي سيقدم إلى الأطراف "على أوسع نطاق ممكن". ويقتضي هذا المبدأ من الأطراف أن تقدم تعاونا واسعا فيما بينها، وأن تقلل إلى أدنى حد من العوائق التي تحول دون التدفق السلس والسريع للمعلومات والأدلة على الصعيد الدولي.

٢٤٣.ثانيا، يرد النطاق العام للالتزام بالتعاون في المادة ٢٣: ينبغي توسيع نطاق التعاون ليشمل جميع الجرائم ذات الصلة بأنظمة وبيانات الكمبيوتر (أي الجرائم المشمولة بالفقرة ٢ من المادة ١٤، البندين "أ" و"ب")، فضلا عن جمع الأدلة في شكل إلكتروني عن جريمة جنائية. ويعني ذلك أن أحكام الفصل الثالث تنطبق سواء ارتكبت الجريمة باستخدام نظام كمبيوتر، أو انطوت جريمة عادية لم ترتكب باستخدام نظام كمبيوتر (مثل القتل) على أدلة إلكترونية. ومع ذلك، تجدر الإشارة إلى أن المواد ٢٤ (تسليم المجرمين) (المساعدة المتبادلة بشأن جمع بيانات الحركة في الوقت الحقيقي) و٣٤ (المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى) تسمح للأطراف بتوفير نطاق مختلف لتطبيق هذه التدابير.

٢٤٤.وفي الأخير، يجب إنجاز التعاون "وفقا لأحكام هذا الفصل" و "من خلال تطبيق الاتفاقات الدولية ذات الصلة بالتعاون الدولي في المسائل الجنائية، والترتيبات المتفق عليها على أساس التشريع الموحد أو المتبادل والقوانين المحلية " على حد سواء. وينص البند الأخير على المبدأ العام الذي مفاده أن أحكام الفصل الثالث لا تلغي أحكام الاتفاقات الدولية المتعلقة بالمساعدة القانونية المتبادلة وتسليم المجرمين، والترتيبات المتبادلة بين الأطراف في إطارها (والتي يرد وصفها بمزيد من التفصيل في مناقشة المادة ٢٧ أدناه)، أو والأحكام ذات الصلة في القانون المحلي والمتعلقة بالتعاون الدولي. ويعزز هذا المبدأ الأساسي بشكل صريح في المواد ٢٤ (تسليم المجرمين)، و٢٥ (المبادئ العامة المتعلقة بالمساعدة المتبادلة)، و٢٦ (المعلومات التلقائية)، و٢٧ (الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق)، و٢٨ (السرية والقيود على الاستخدام) و(٣١) (المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكمبيوتر المخزنة) و٣٣ (المساعدة المتبادلة ذات الصلة بجمع بيانات الحركة في الوقت الحقيقي) و٣٤ (المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى).

الباب الثاني – المبادئ ذات الصلة بتسليم المجرمين

المادة ٢٤ – تسليم المجرمين (المادة ٢٤)

٢٤٥.تنص الفقرة ١ على أن الالتزام بالتسليم لا ينطبق إلا على الجرائم المقررة طبقا للمواد من ٢ إلى ١١ من الاتفاقية التي يعاقب عليها بموجب قوانين الطرفين المعنيين بعقوبة سالبة للحرية لمدة أقصاها سنة واحدة على الأقل أو بعقوبة أشد. وقرر القائمون على الصياغة إدراج حد أدنى للعقوبة لأن الأطراف قد تعاقب، بموجب الاتفاقية، على بعض الجرائم بعقوبة حبسية تكون مدتها القصوى قصيرة نسبيا (مثلا، المادة ٢ – النفاذ غير القانوني – والمادة ٤ – التدخل في البيانات). وبالنظر إلى ذلك، لم يعتقد القائمون على الصياغة أنه من الملائم اشتراط اعتبار كل جريمة من الجرائم المنصوص عليها في المواد من ٢ إلى ١١ في حد ذاتها قابلة لتطبيق إجراء تسليم المجرمين. وبناء على ذلك، تم التوصل إلى اتفاق بشأن شرط عام يقضي بأن تعتبر الجريمة جريمة قابلة لتطبيق إجراء تسليم المجرمين عندما تكون العقوبة القصوى التي يمكن فرضها على الجريمة المطلوب التسليم من أجلها عقوبة حبسية لمدة سنة واحدة على الأقل – كما هو وارد في المادة ٢ من الاتفاقية الأوروبية لتسليم المجرمين (سلسلة المعاهدات الأوروبية رقم ٢٤). ولا يتوقف تحديد قابلية الجريمة لتطبيق إجراء تسليم المجرمين على العقوبة الفعلية المفروضة في القضية المعينة قيد النظر، ولكن بدلا من ذلك على المدة القصوى التي يجوز فرضها قانونيا على الجريمة المطلوب التسليم من أجلها.

٢٤٦.في الوقت نفسه، ووفقا للمبدأ العام الذي يقضي بأن التعاون الدولي في إطار الفصل الثالث ينبغي أن ينفذ عملا بالصكوك الجاري بها العمل بين الأطراف، تنص الفقرة ١ أيضا على أنه في حال وجود معاهدة بشأن تسليم المجرمين أو ترتيب على

الباب الأول – المساعدة المتبادلة بشأن التدابير المؤقتة

التعجيل في حفظ بيانات الكومبيوتر المخزنة (المادة ٢٩)

٢٨٢.تنص هذه المادة على آلية على الصعيد الدولي مطابقة لتلك المنصوص عليها في المادة ١٦ من أجل الاستخدام على الصعيد الوطني. وتخول الفقرة ١ من هذه المادة للطرف أن يقدم طلبا للحصول على التعجيل بحفظ البيانات المخزنة في إقليم الطرف متلقي الطلب، وتقتضي الفقرة ٣ أن يكون لكل طرف القدرة القانونية على تحقيق ذلك عبر نظام الكمبيوتر، بغية تفادي تغيير البيانات أو إزالتها أو حذفها خلال الفترة الزمنية اللازمة لإعداد وإرسال وتنفيذ طلب المساعدة المتبادلة للحصول على تلك البيانات. ويعتبر الحفظ تدبيرا مؤقتا محدودا تتوخى منه السرعة بشكل أكبر بكثير من تنفيذ المساعدة المتبادلة التقليدية. وكما أشير سابقا، تعتبر بيانات الكمبيوتر شديدة التقلب. ويمكن حذفها ببضع نقرات على لوحة المفاتيح أو عن طريق تشغيل برامج تلقائية، مما يجعل من المستحيل تتبع الجريمة للوصول إلى مرتكبها أو يؤدي إلى إتلاف الأدلة الهامة على الجريمة. يتم تخزين بعض أشكال بيانات الكمبيوتر لفترات قصيرة فقط قبل حذفها. وهكذا، تم الاتفاق على أن هناك حاجة إلى آلية لضمان توافر هذه البيانات ريثما يتم تنفيذ العملية الأطول والأشمل لطلب المساعدة المتبادلة الرسمية التي قد تستغرق أسابيع أو شهور.

٢٨٣.ولئن كان هذا التدبير أسرع بكثير من ممارسة المساعدة المتبادلة العادية، فإنه في الوقت نفسه أقل تطفلا. ولا يطلب من الموظفين المسؤولين عن المساعدة المتبادلة في الطرف متلقي الطلب الحصول على البيانات من الجهة الوديعة. ولعل الإجراء المفضل للطرف متلقي الطلب يتمثل في ضمان أن تقوم الجهة الوديعة (التي غالبا ما تكون مقدم خدمة أو طرفا ثالثا) بحفظ البيانات (أي، عدم حذفها) ريثما تصدر عملية تقضي بتسليمها إلى موظفي إنفاذ القانون في مرحلة لاحقة. وتتميز هذه العملية بالسرعة وحماية خصوصية الشخص الذي تخصه البيانات، حيث لن يتم الكشف عنها أو فحصها من قبل أي مسؤول حكومي حتى يتم استيفاء معايير الكشف الكامل وفقا لأنظمة المساعدة المتبادلة العادية. وفي الوقت نفسه، يسمح للطرف متلقي الطلب باستخدام إجراءات أخرى لضمان الحفظ السريع للبيانات، بما في ذلك التعجيل بإصدار وتنفيذ أمر التقديم أو أمر البحث عن البيانات. ويتمثل الشرط الأساسي في التوفر على عملية سريعة للغاية لتفادي ضياع البيانات بصورة لا رجعة فيها.

٢٨٤.تبين الفقرة ٢ محتويات طلب الحفظ عملا بهذه المادة. وإذ تضع اللجنة في اعتبارها أن هذا الإجراء تدبير مؤقت وأن يتعين إعداد الطلب وإرساله بسرعة، فإن المعلومات المقدمة تكون موجزة وتشمل فقط الحد الأدنى من المعلومات المطلوبة لتمكين حفظ البيانات. وبالإضافة إلى تحديد السلطة التي تسعى إلى الحفظ والجريمة التي يطلب من أجلها الحفظ، يجب أن يتضمن الطلب موجزا للوقائع، ومعلومات كافية لتحديد البيانات التي يتعين حفظها وموقعها، وأن يبين أن البيانات ذات صلة بالتحقيق في الجريمة المعنية أو ملاحقتها قضائيا، وأن حفظها ضروري. وفي الأخير، يتعين على الطرف مقدم الطلب أن يتقدم بعد ذلك بطلب للمساعدة المتبادلة حتى يتسنى له الحصول على البيانات.

٢٨٥.تنص الفقرة ٣ على أنه لا ينبغي فرض مبدأ ازدواجية التجريم كشرط لتوفير الحفظ. بشكل عام، يسفر تطبيق مبدأ ازدواجية التجريم عن نتيجة عكسية في سياق الحفظ. أولا، في إطار الممارسة الحديثة في مجال المساعدة المتبادلة، ثمة ميول إلى إلغاء شرط ازدواجية التجريم بالنسبة لكافة التدابير، ما عدا التدابير الإجرائية الأكثر تطفلا، مثل البحث والمصادرة أو الاعتراض. غير أن الحفظ، وفقا لتصور القائمين على الصياغة، لا يعتبر تطفلا بشكل خاص لأن الجهة الوديعة يحتفظ بحيازة البيانات التي بحوزته بصورة قانونية، ولا يتم الكشف عن البيانات للمسؤولين لدى الطرف المتلقي أو فحصها من قبلهم إلى أن يتم تنفيذ طلب المساعدة المتبادلة الرسمية الذي يلتمس الكشف عن البيانات. وثانيا، وكمسألة عملية، غالبا ما يستغرق تقديم التوضيحات اللازمة لإثبات وجود ازدواجية التجريم بصورة قاطعة وقتا طويلا لدرجة يمكن في غضونه حذف البيانات، إزالتها أو تغييرها. فعلى سبيل المثال، قد يدرك الطرف مقدم الطلب في المراحل المبكرة من التحقيق أنه قد تم اقتحام جهاز كمبيوتر في إقليمه، لكن قد لا يستوعب جيدا طبيعة الضرر ونطاقه إلا في وقت لاحق. وفي احتمال تأخير الطرف متلقي الطلب لحفظ بيانات الحركة التي من شأنها أن تتقفى مصدر الاقتحام في انتظار إقامة ازدواجية التجريم، فإن البيانات الهامة غالبا ما تحذف بصورة روتينية من قبل مقدمي الخدمات الذين يحتفظون بها لساعات أو أيام

الباب الثالث – المبادئ العامة ذات الصلة بالمساعدة المتبادلة

المبادئ العامة ذات الصلة بالمساعدة المتبادلة (المادة ٢٥)

٢٥٣.ترد المبادئ العامة التي تنظم الالتزام بتقديم المساعدة المتبادلة في الفقرة ١. وينبغي توفير التعاون "على أوسع نطاق ممكن". وهكذا، وكما ورد في المادة ٢٣ ("المبادئ العامة ذات الصلة بالتعاون الدولي")، تكون المساعدة المتبادلة من حيث المبدأ واسعة النطاق، والمعيقات التي تقيدها محدودة للغاية. ثم، وكما ورد في المادة ٢٣، ينطبق الالتزام بالتعاون من حيث المبدأ على كل من الأفعال الإجرامية المتعلقة بأنظمة وبيانات الكمبيوتر (أي الجرائم المشمولة بالفقرة ٢ من المادة ١٤، والبندين "أ" و "ب")، وبجمع أدلة خاصة بجريمة جنائية في شكل إلكتروني. وقد تم الاتفاق على فرض التزام بالتعاون فيما يتعلق بهذه المجموعة الواسعة من الجرائم لأن ثمة حاجة مماثلة إلى آليات مبسطة للتعاون الدولي فيما يتعلق بكلتا هاتين الفئتين. ومع ذلك، تسمح المادتان ٣٤ و٣٥ للأطراف بتوفير نطاق مختلف لتطبيق هذه التدابير.

٢٥٤.ستوضح أحكام أخرى من هذا الفصل أن الالتزام بتقديم المساعدة المتبادلة يتم عموما وفقا لأحكام معاهدات وقوانين وترتيبات المساعدة القانونية سارية التطبيق. وبمقتضى الفقرة ٢، كل طرف مطالب بالتوفر على أساس قانوني لتنفيذ أشكال التعاون المحددة المبينة في باقي الفصل، إذا كانت معاهداته وقوانينه وترتيباته لا تتضمن بالفعل أحكاما من هذا القبيل. ويعد توافر هذه الآليات، ولا سيما تلك الواردة في المواد من ٢٩ إلى ٣٥ (أحكام خاصة - الأبواب ١ و٢ و٣) أمرا حيويا للتعاون الفعال في المسائل الجنائية المتعلقة بالكمبيوتر.

٢٥٥.لن تقتضي بعض الأطراف أي تشريع تنفيذي لتطبيق الأحكام المشار إليها في الفقرة ٢، حيث أن أحكام المعاهدات الدولية التي تنشئ أنظمة مفصلة للمساعدة المتبادلة تعتبر أحكاما ذاتية التنفيذ بطبيعتها. ومن المتوقع أن تكون الأطراف قادرة على التعامل مع هذه الأحكام على أنها ذاتية التنفيذ، وأن تكون لديها بالفعل مرونة كافية في إطار تشريعات المساعدة المتبادلة القائمة لتنفيذ تدابير المساعدة المتبادلة المقررة بموجب هذا الفصل، أو أن تكون قادرة على سن أي تشريع مطلوب للقيام بذلك، على وجه السرعة.

٢٥٦.تعتبر بيانات الكمبيوتر شديدة التقلب. ويمكن حذفها ببضع نقرات على لوحة المفاتيح أو عن طريق تشغيل برامج تلقائية، مما يجعل من المستحيل تتبع الجريمة للوصول إلى مرتكبها أو يؤدي إلى إتلاف الأدلة الهامة على الجريمة. يتم تخزين بعض أشكال بيانات الكمبيوتر لفترات قصيرة فقط قبل حذفها. وفي حالات أخرى، قد يتأذى أشخاص أو يلحق ضرر جسيم بممتلكات إن لم يتم جمع الأدلة بسرعة. وفي مثل هذه الحالات العاجلة، يجب التسريع ليس فقط بالطلب، بل وكذلك بالرد. لذلك، تهدف الفقرة ٣ إلى تيسير التعجيل بعملية الحصول على المساعدة المتبادلة بحيث لا تضيع المعلومات أو الأدلة الهامة بسبب حذفها قبل إعداد طلب المساعدة وإرساله والاستجابة له. وتحقق الفقرة ٣ ذلك من خلال: (١) تمكين الأطراف من تقديم طلبات عاجلة للتعاون من خلال وسائل الاتصال السريعة، بدلا من الوسائل التقليدية البطيئة التي تنطوي على نقل الوثائق المكتوبة والمختومة عبر الحقائب الدبلوماسية أو البريد؛ و(٢) مطالبة الطرف متلقي الطلب باستخدام وسائل سريعة للاستجابة للطلبات في مثل هذه الظروف. ويطلب من كل طرف أن تتوفر لديه القدرة على تطبيق هذا التدبير في حال لم تنص معاهدات أو قوانين أو ترتيبات المساعدة المتبادلة على ذلك. يعتبر إدراج الفاكس والبريد الإلكتروني ذا طبيعة إرشادية؛ ويجوز استخدام أي وسيلة اتصال سريعة أخرى حسبما يكون ملائما في الظروف الخاصة المطروحة. ومع تقدم التكنولوجيا، سيتم تطوير المزيد من وسائل الاتصال السريعة التي يمكن استخدامها لطلب المساعدة المتبادلة. وفيما يتعلق بمتطلبات الصحة والأمن الواردة في الفقرة، يجوز للأطراف أن تقرر فيما بينها كيفية ضمان صحة الاتصالات وما إذا كانت هناك حاجة إلى حمايات أمنية خاصة (بما في ذلك التشفير) قد تكون ضرورية في الحالات الحساسة بشكل خاص. وفي

الباب الرابع – الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق (المادة ٢٧)

٢٦٢.تلزم المادة ٢٧ الأطراف بتطبيق بعض إجراءات وشروط المساعدة المتبادلة في حالة عدم وجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة سارية بين الأطراف المقدمة والمتلقية للطلب. ومن ثم، تعزز هذه المادة المبدأ العام القائم على أن المساعدة المتبادلة ينبغي أن تنفذ من خلال تطبيق المعاهدات ذات الصلة والترتيبات المماثلة للمساعدة المتبادلة. ورفض القائمون على الصياغة إنشاء نظام عام منفصل للمساعدة المتبادلة في هذه الاتفاقية يطبق بدلا من الصكوك والترتيبات الأخرى واجبة التطبيق، واتفقوا بدلا من ذلك على أنه سيكون من العملي أكثر الاعتماد على أحكام معاهدات المساعدة المتبادلة (MLATs) القائمة في هذا المجال كموضوع عام، وبالتالي السماح لممارسي المساعدة المتبادلة باستخدام الصكوك والترتيبات المستأنسين بها وتجنب الارتباك الذي قد ينجم عن إنشاء أنظمة متنافسة. وكما ذكر سابقا، فإن كل طرف مطالب، فقط فيما يتعلق بالآليات اللازمة بشكل خاص للتعاون الفعال والسريع في المسائل الجنائية المتصلة بالكمبيوتر، مثل الآليات الواردة في المواد من ٢٩ إلى ٣٥ (أحكام خاصة - الأبواب ١ و٢ و٣) بإنشاء أساس قانوني بغية تمكين تنفيذ مثل هذه الأشكال من التعاون إن لم تكن معاهدات أو ترتيبات أو قوانين المساعدة المتبادلة الراهنة تنص على ذلك بالفعل.

٢٦٣.بناء على ذلك، يتواصل تنفيذ معظم أشكال المساعدة المتبادلة بموجب هذا الفصل عملا بالاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية (سلسلة المعاهدات الأوروبية رقم ٣٠) وبروتوكولها (سلسلة المعاهدات الأوروبية رقم ٩٩) بين الأطراف في تلك الصكوك . وكبديل عن ذلك، تواصل الأطراف في هذه الاتفاقية التي تتوفر على معاهدات المساعدة المتبادلة (MLATs) ثنائية الأطراف سارية المفعول بينها، أو غيرها من الاتفاقات المتعددة الأطراف التي تنظم المساعدة المتبادلة في القضايا الجنائية (مثل الدول الأعضاء في الاتحاد الأوروبي) تطبيق شروطها، التي تكملها الآليات المتعلقة بالجريمة المرتكبة عبر الكمبيوتر أو ذات الصلة بالكمبيوتر الوارد وصفها في الجزء المتبقي من الفصل الثالث، ما لم توافق على تطبيق أي من أحكام هذه المادة أو كلها، بدلا منها. ويمكن أن تستند المساعدة المتبادلة أيضا إلى الترتيبات المتفق عليها على أساس تشريعات موحدة أو متبادلة، مثل نظام التعاون الذي وضعته بلدان الشمال الأوروبي، والذي تقبله أيضا الاتفاقية الأوروبية المعنية بالمساعدة المتبادلة في المسائل الجنائية (المادة ٢٥، الفقرة ٤)، وفيما بين أعضاء الكومنولث. وفي الأخير، لا تقتصر الإشارة إلى معاهدات أو ترتيبات المساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة على الصكوك السارية وقت بدء نفاذ هذه الاتفاقية، بل تشمل أيضا الصكوك التي يمكن اعتمادها في المستقبل.

٢٦٤.تنص المادة ٢٧ (الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق)، الفقرات من ٢ إلى ١٠، على عدد من القواعد لتقديم المساعدة المتبادلة في غياب أحكام معاهدات المساعدة المتبادلة (MLATs) أو ترتيب على أساس تشريعات موحدة أو متبادلة، بما في ذلك إنشاء سلطات مركزية، وفرض شروط وأسباب وإجراءات في حالات التأجيل أو الرفض، وسرية الطلبات، والاتصالات المباشرة. وفيما يتعلق بهذه المسائل المشمولة

٣٠٣.مع بعض الاستثناءات، تستند الأحكام الواردة في هذا الفصل، في معظمها، إلى "البنود الختامية النموذجية للاتفاقيات والاتفاقات المبرمة داخل مجلس أوروبا" والتي وافقت عليها لجنة الوزراء في الجلسة ٣١٥ خلال اجتماع النواب المنعقد في فبراير/شباط ١٩٨٠. وبما أن معظم المواد من ٣٦ إلى ٤٨ إما تستخدم اللغة الموحدة في البنود النموذجية أو تستند إلى ممارسة طويلة الأمد في مجال وضع المعاهدات في مجلس أوروبا، فإنها لا تدعو إلى تعليقات محددة. ومع ذلك، فإن بعض التعديلات في البنود النموذجية المعيارية أو بعض الأحكام الجديدة، تقتضي بعض التوضيح. ويلاحظ في هذا السياق، أن البنود النموذجية اعتمدت كمجموعة غير ملزمة من الأحكام. وكما وردت الإشارة في تقديم البنود النموذجية فإن "الغرض من هذه البنود الختامية النموذجية يتلخص في تسهيل مهمة لجان الخبراء وتجنب الاختلافات النصية التي لا يكون لها أي مبرر حقيقي. ولا يعتبر النموذج بأي حال من الأحوال ملزما ويمكن تكييف بنود مختلفة لتناسب حالات معينة ".

التوقيع والدخول حيز النفاذ (المادة ٣٦)

٣٠٤.صيغت الفقرة ١ من المادة ٣٦ وفقا لعدة سوابق وضعت في اتفاقيات أخرى أعدت في إطار مجلس أوروبا، ومنها مثلا اتفاقية نقل الأشخاص المدانين (سلسلة المعاهدات الأوروبية رقم ١١٢) والاتفاقية المعنية بمكافحة غسل الأموال، والبحث عن عائدات الجريمة وضبطها ومصادرتها (سلسلة المعاهدات الأوروبية رقم ١٤١)، والتي تسمح بالتوقيع عليها، قبل دخولها حيز النفاذ، ليس فقط من قبل الدول الأعضاء في مجلس أوروبا، بل أيضا من لدن الدول غير الأعضاء التي تشارك في صياغتها. ويهدف هذا الحكم إلى تمكين أكبر عدد ممكن من الدول المهتمة، وليس فقط الدول الأعضاء في مجلس أوروبا، من أن تصبح أطرافا في أقرب وقت ممكن. وهنا، يقصد من هذا الحكم أن ينطبق على أربع دول غير أعضاء هي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية التي شاركت بنشاط في صياغة الاتفاقية. وبمجرد دخول الاتفاقية حيز النفاذ، وفقا للفقرة ٣، يجوز دعوة دول أخرى من غير الأعضاء التي لا يشملها هذا الحكم إلى الانضمام إلى الاتفاقية وفقا للفقرة ١ من المادة ٣٧.

٣٠٥.تحدد الفقرة ٣ من المادة ٣٦ عدد التوقيعات أو القبول أو الموافقات اللازمة لدخول الاتفاقية حيز النفاذ، في ٥. ويعتبر هذا الرقم أعلى من العتبة المعتادة (٣) في معاهدات مجلس أوروبا ويعكس الاعتقاد بأن ثمة حاجة إلى مجموعة أكبر قليلا من الدول للشروع بنجاح في التصدي للتحدي للجرائم الدولية المرتكبة عبر الكمبيوتر أو ذات الصلة بالكمبيوتر. ومع ذلك، فإن هذا العدد ليس مرتفعا لدرجة قد تؤدي إلى التأخير غير الضروري لدخول الاتفاقية حيز النفاذ. ومن بين الدول الخمس الأولى، يجب أن تكون ثلاثة دول على الأقل من الأعضاء في مجلس أوروبا، ويمكن أن تكون الدولتان الأخريان من الدول

الأربع غير الأعضاء التي شاركت في صياغة الاتفاقية. وبطبيعة الحال، من شأن هذا الحكم أيضا أن يسمح بدخول الاتفاقية حيز التنفيذ بناء على التعبير خمس دول أعضاء في مجلس أوروبا عن الموافقة بالالتزام.

الانضمام إلى الاتفاقية (المادة ٣٧)

٣٠٦.صيغت المادة ٣٧ أيضا وفقا للسوابق المنصوص عليها في اتفاقيات أخرى لمجلس أوروبا، مع تضمنها لعنصر إضافي صريح. بموجب ممارسة معمول بها منذ عهد طويل، تقرر لجنة الوزراء، بمبادرة منها أو بناء على طلب، دعوة دولة غير عضو لم تشارك في وضع اتفاقية، للانضمام إلى الاتفاقية بعد التشاور مع جميع الأطراف المتعاقدة، سواء كانت دولا أعضاء أم لا. وهذا يعني أنه إذا اعترض أي طرف متعاقد على انضمام دولة غير عضو، فإن لجنة الوزراء لا تدعوها عادة للانضمام إلى الاتفاقية. غير أنه بموجب الصياغة المعتادة، يمكن للجنة الوزراء، نظريا، أن تدعو تلك الدولة غير العضو إلى الانضمام إلى اتفاقية حتى إذا اعترضت دولة طرف غير عضو على انضمامها. وهذا يعني أن حق النقض - من الناحية النظرية - لا يمنح عادة للدول غير الأعضاء بشأن عملية توسيع معاهدات مجلس أوروبا إلى دول أخرى من غير الأعضاء. ومع ذلك، تم إدراج شرط صريح يتمثل في تشاور لجنة الوزراء مع جميع الدول المتعاقدة – وليس فقط الأعضاء في مجلس أوروبا – والحصول على موافقتها بالإجماع – قبل دعوة دولة غير عضو إلى الانضمام إلى الاتفاقية. وكما هو مبين أعلاه، فإن هذا الشرط يتفق مع الممارسة ويعترف بأن جميع الدول المتعاقدة في الاتفاقية ينبغي أن تكون قادرة على تحديد الدول غير الأعضاء التي ترغب في بناء علاقات تعاهدية معها. ومع ذلك، يتم اتخاذ القرار الرسمي بدعوة دولة غير عضو إلى الانضمام، وفقا للممارسة المعتادة، من قبل ممثلي الأطراف المتعاقدة التي يحق لها حضور اجتماعات لجنة الوزراء. ويقتضي هذا القرار أغلبية الثلثين المنصوص عليها في المادة ٢٠(د) من النظام الأساسي لمجلس أوروبا وتصويت ممثلي الأطراف المتعاقدة الذين يحق لهم حضور اجتماع اللجنة بالإجماع.

٣٠٧.يطلب من الدول الاتحادية التي تسعى إلى الانضمام إلى الاتفاقية، والتي تعتزم إصدار إعلان بموجب المادة ٤١، أن تقدم مسبقا مشروع الإعلان المشار إليه في الفقرة ٣ من المادة ٤١، بحيث تتمكن الأطراف من تقييم كيفية تأثير تطبيق الحكم الاتحادي على تنفيذ الطرف المقبل للاتفاقية (انظر الفقرة ٣٢٠).

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الديباجـة :

إن الدول العربية الموقعة،

رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها،

واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات،

وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة،

وإلتزاماً بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها،

فقد اتفقت على ما يلي:

الفصل الأول

أحكام عامة

المادة الأولى: الهدف من الاتفاقية:

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المادة الثانية: المصطلحات:

يقصد بالمصطلحات التالية في هذه الاتفاقية التعريف المبين إزاء كل منها:

1- **تقنية المعلومات:** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة.

2- **مزود الخدمـة:** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.

3- **البيـانـات :** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها...

4- **البرنامج المعلوماتي:** مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.
5- **النظام المعلوماتي:** مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.
6- **الشبكة المعلوماتية:** ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.
7- **الموقـــع :** مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.
8- **الالتقـــاط :** مشاهدة البيانات أو المعلومات أو الحصول عليها.
9- **معلومات المشترك:** أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:
أ - نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.
ب- هويـــة المشـــترك وعنوانـــه البريـــدي أو الجغرافـــي أو هاتفـــه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.
ج - أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.

المادة الثالثة: مجالات تطبيق الاتفاقية:

تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية :

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.

المادة الرابعة: صون السيادة:

1- تلتزم كل دولة طرف وفقاً لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.
2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

الفصل الرابع

التعاون القانوني والقضائي

المادة الثلاثون: الاختصاص :

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت:

أ - في إقليم الدولة الطرف.

ب- على متن سفينة تحمل علم الدولة الطرف.

ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

د- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

3- إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم.

المادة الحادية والثلاثون: تسليم المجرمين:

1- أ- هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الاطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.

ب- إذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق.

2- إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبرجرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف.

3- إذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة.

4- الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة (1) من هذه المادة قابلة لتسليم المجرمين بين تلك الدول.

5- يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها لرفض تسليم المجرمين.

6- يجوز لكل دولة طرف من الأطراف المتعاقدة أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة أو بعقوبة أشد لدى أي من الطرفين المتعاقدين وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلباً بالملاحقة مصحوبا بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازتها وتحاط الدولة الطرف الطالبة علما بما يتم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم.

7- أ- تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإيصال اسم وعنوان السلطة المسؤولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي في

ظل غياب معاهدة إيصال هذه المعلومات إلى الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب.

ب- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل السلطات المعنية من قبل الدول الأطراف وعلى كل دولة طرف أن تضمن أن تفاصيل السجل صحيحة دائماً.

المادة الثانية والثلاثون: المساعدة المتبادلة :

1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم.

2- تلتزم كل دولة طرف بتبنى الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين.

3- يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك إستخدام التشفير) وتأكيد الإرسال حسبما تطلب الدولة الطرف ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات.

4- باستثناء ما يرد فيه نص في هذا الفصل فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها أن تمارس حقها في رفض المساعدة فيما يتعلق بالجرائم المنصوص عليها في الفصل الثاني فقط بناء على كون الطلب يخص جريمة يعتبرها من الجرائم المالية.

5- حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فإن هذا الشرط يعتبر حاصلاً بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة وذلك إذا كان الفعل الذي يمهد للجريمة التي تطلب المساعدة فيها يعتبر جريمة بحسب قوانين الدولة الطرف.

حررت هذه الاتفاقية باللغة العربية بمدينة القاهرة في جمهورية مصر العربية في 1432/1/15هـ ، الموافق 2010/12/21م من أصل واحد مودع بالأمانة العامة لجامعة الدول العربية (الأمانة الفنية لمجلس وزراء العدل العرب)، ونسخة مطابقة للأصل تسلم للأمانة العامة لمجلس وزراء الداخلية العرب، وتسلم كذلك نسخة مطابقة للأصل لكل دولة من الدول الأطراف.

وإثباتاً لما تقدم، قام أصحاب السمو والمعالي وزراء الداخلية والعدل العرب، بتوقيع هذه الاتفاقية، نيابة عن دولهم.

قائمة المحتويات

الـمـلـخص:

تناولنا في الفصل الأول ماهية التعاون الدولي لمواجهة الجرائم المعلوماتية، حيث تطرقنا خلاله الى ماهية الجريمة المعلوماتية من أجل بيان مضمونها وأهم أنواعها، وكذلك تتطرقنا فيه الى أهم مجالات التعاون الدولي في مكافحة الجريمة المعلوماتية من خلال إيضاح مدى الحاجة الماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بمهمة المكافحة وتنسيق بين الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين.

أما الفصل الثاني تناولنا الصعوبات التي تواجه التعاون الدولي وكيفية القضاء عليها، حيث تمثلت هذه الصعوبات في وجود تحديات على المستوى الوطني والدولي، ثم تطرقنا الى أهم أساليب المعالجة على المستوى الدولي والوطني.

ثم تضمنت الخاتمة جملة من النتائج والتوصيات الضرورة لمواجهة هذا النوع من الجرائم المستحدثة.

الكلمات المفتاحية:

التعاون الدولي، الجرائم المعلوماتية.

Summary

In the first chapter, we dealt with the nature of international cooperation to confront which we touched upon the nature of cybercrime in order to cybercrime, during clarify its content and the most important types, as well as the most important areas of international cooperation in combating cybercrime by clarifying the urgent need for an international entity to take upon itself Carrying out the task of combating and coordinating between different countries, especially with regard to the exchange of information related to crime and criminals.

As for the second chapter, we dealt with the difficulties facing international represented in the cooperation and how to eliminate them, as these difficulties are presence of challenges at the national and international levels.

Then the conclusion included a set of conclusions and recommendations necessary to confront this type of newly created crime.

Key words

International cooperation, cyber crime