السياسات الدولية والوطنية تجاه الجرائم الإلكترونية

د.نزيه محمد على عبد الغنى*

الملخص:

تتناول دراستنا السياسات الدولية والوطنية تجاه مواجهة الجرائم الإلكترونية، وبخاصة بعد أن ازدادت معدلات تلك الجرائم بصورة كبيرة في الآونة الأخيرة ،ونجم عن ذلك الأمر آثار خطيرة، وبعد إدراك تلك المجتمعات لأهمية مكافحة تلك الجرائم، فقد سعت إلى التوصل للعديد من الاستراتيجيات الفعالة بهدف التصديلمواجهة تلك الجرائم بجميع اشكالها، كما تتحقق المكافحة من خلال ترويج وتدعيم التدابير الرامية إلى منع ومكافحة تلك الجرائم، حيث تختلف وسائل مكافحتها ما بين تدابير وقائية وتشريعية وقضائية تساهم جميعها إلى حد كبير في مؤازرة كافة الجهود لمكافحة الجرائم الإلكترونية بهدف القضاءعليها.

وسوف تتطرق دراستنا في الفصل الأول إلى بيان الإطار القانوني للتعاون الدولي المتعلق بمكافحة تلك الجرائم سواء على المستوي التشريعي والمؤسسي، كما نبين دور المساعدات الأمنية والقضائية، وكذلك التدابير المتعلقة بتسليم المجرمين، كما نستعرض في الفصل الثاني موقف التشريعات الوطنية تجاه تلك الجرائم، حيث نستعرض الدور الوقائي لمواجهة تلك الجرائم ، مع بيان الاتجاهات العقابية المتعلقة بمكافحة تلك الجرائم

International and National Policies towards Cybercrime

Dr. Nazih Muhammad Ali Abdul-Ghani

Summary

Our study addresses international and national policies towards tackling cybercrime, particularly after the recent increase in the rates of such crimes, which have had serious consequences, and after recognizing the importance of combating such crimes, we have sought to find many effective strategies to address these crimes in all its forms. To support all efforts to combat cybercrime with the aim of eliminating them.

Our study will address in the first chapter the statement of the legal framework for international cooperation on combating these crimes, both at the legislative and institutional levels, as well as the role of security and judicial assistance, as well as measures related to the extradition of criminals.

* دكتور فى الحقوق قسم القانون الدولى العام

المقدمة:

ساهم ظهور الحاسبات الآلية إلى تغيير نمط الحياة في العالم، حيث أصبح الاعتماد بشكل رئيسي على الوسائل التقنية الحديثة، وازداد تأثير التكنولوجيا في المجتمعات المعاصرة، في العديد من المرافق العامة للدولة، أو المؤسسات المصرفية والمالية، وفي شتي المجالات التعليمية، والأمنية، أو غير ذلك من المسائل الأخرى .

وبالرغم من أن الوسائل والأدوات الإلكترونية الحديثة استخدمت في إسعاد البشرية، كما أنه ترتب على تلك التقنيات وجه أخر سلبي ذات خطورة كبيرة تسبب في شقاء البشرية، بما يعني أن تلك الوسائل الإلكترونية لديها العديد من الجوانب الايجابية المضيئة، بحيث توجد صعوبة كبيرة في حصر تلك الفوائد، بيد أن للتكنولوجيا وجه آخر سيء نتيجة الاستخدامات السيئة والضارة لتلك التقنيات الحديثة والمعاصرة، مما نجم عن ذلك ظهور جرائم مستحدثة أطلق عليها الفقه القانوني" الجرائم الإلكترونية"، وبخاصة أن الجرائم الأخيرة أصبحتمن الخطورةكونها تهدد العالم بأسره.

والجرائم الإلكترونية من الأتساع كونها تعتمد على التقنية الإلكترونيةالعالية؛ ويراد"بجرائم التقنية العالية"hi-tech crime استخدام الحاسوب وغيره من وسائل الاتصال الأخرى بهدف ارتكاب الجريمة. ولذلك فأن مصطلح"جرائم التقنية العالية"،يدخل ضمنياً جرائم الإنترنت تحت نطاقه[1].

في حين يذهب البعض بأن جرائم الإنترنت هي امتداد لما عرف بجرائم الكمبيوتر، ولقد وجدت العديد من المسميات لتلك الجرائم منها (جرائم عبر الكمبيوتر والإنترنت، جرائم تقنية المعلومات،وجرائم أصحاب الياقات البيضاء)[2].

وفي الوقت الحالي أمتد نطاق الجرائم الإلكترونية بظهور العديد من الانماط المستحدثة لتلك الجرائم، حيث أتسعت جسامة نطاق تلك الجرائم، واكتسبت الطابع الدولي، وذلك نتيجة تأثير تلك الجريمة على العديد من مصالح وقيم المجتمع الدوليالمشتركة، مما أصبحت الجرائم الإلكترونية تشكل خطورة كبيرة على السلم والأمن الدوليين، كونها تمثل مخالفة واضحة لما تضمنه ميثاق الأمم المتحدة .

وعلى صعيد المجتمعات الوطنية حيث تولدت العديد من الأضرار الناجمة عن تلك الجرائم، مما ظهرت جرائم الاعتداء على النفس، والاعتداء على المال، علاوة على تأثير تلك الجرائم لأنها تتعلق بأمن وسلامة الدولة على الصعيد الداخلي والخارجي.

وشهدت الجرائم الإلكترونية تطورات مذهلة بتطور الخدمات الإلكترونية، فظهرت العديد من صور تلك الجرائم، فإذا كان على المجتمع بأشخاصه ومؤسساته التعايش مع تلك الجرائم واتخاذ الإجراءات اللازمة لمواجهتها، وبخاصة عقب تطور

تلك الجرائم منذ منتصف التسعينات، وازدهارها، إلا أن القوانين الجنائية قد عجزت عن متابعة ذات التطورات[3].

ولقد تعددت تعريفات الجرائم الإلكترونية وتباينت فيما بينها ضيقا واتساعا، وقد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة تلك الجريمة، وما يتتبع ذلك من تسهيل الوصول إلى الحلول المناسبة لمواجهاتها [4]، كما أشار بعض الفقهاء إلى أن تلك الجريمة؛ هي التي ترتكب بأداة الكمبيوتر، بواسطة شبكة الإنترنت ومن قبل أشخاص لديهم دراية كبيرة باستخدام الإنترنت والكمبيوتر[5].

وإزاء ما تقدم ذكره؛فقد أحتلت مواجهة تلك الجرائمالخطيرة محور اهتمام أجهزة العدالة الجنائية والأمنية، والعديد من الحكومات والدول والأجهزة المعنية سواء كانت وطنية أو إقليمية أو دولية،بهدف صد هذا التيار الإجرامي المنظم والعابر للحدود الدولية،في سبيل إيجاد الوسائل والاساليب العلمية والتكنولوجية التي تحجمه وتقضي عليه ليتحقق الأمن ويسود الاستقرار على المستوى المحلى والعالمي[6].حيث تكاتف المجتمع الدولي لمجابهة تلك الجرائم، وتعزيز كافة سبل التعاون الدولي، وكذلك اتخاذ العديد منالتدابير الفعّالة بهدف الحد من تلك الجرائم ومعاقبة مرتكبيها، كما واجهت غالبية الدول المعاصرة ذات النوعيات المستحدثة من الجرائم .

اولاً- هدف الدراسة :

تسعى الدراسة الى تحقيق العديد من الأهداف التي تتمثل في التالي:

- الهدف الرئيسي من الدراسة هو إلقاء الضوء على موضوع السياسات الدولية والوطنية تجاه مواجهة الجرائم الإلكترونية،
- التطرق إلى الإطار القانوني للتعاون الدولي المتعلق بمكافحة الجرائم الإلكترونية، ببيان العديد من سياسات التعاون الدولي تجاه الجرائم الإلكترونية ،سواء كانت تلك الاستراتيجيات الدولية أمنية أو قضائية أو قانونية
- استعراض الموقف الذى سلكته بعض التشريعات والقوانين الوطنية المعاصرة تجاه الجرائم الإلكترونية.

ثانياً- أهمية الدراسة:

- تكمن اهمية موضوع دراستنا، وبخاصة بعد أن ساهمت التقنيات الرهيبة في الحاسبات الآلية إلى ظهور نوعية من الجرائم الالكترونية، مما احتلت الجرائم الإلكترونية دور له اهميته على صعيد المجتمعات الدولية والوطنية. ولا سيما أن كافة الإجراءات والتدابير التي تخذها الدول بمفردها غير كافية لمكافحة تلك الانماط من الجرائم، حيث ينبغي مواجهتها بالعمل على بتنسيق الجهود الدولية والوطنية .

- للدراسة اهمية كبيرة؛ نظرًالارتباط الجرائم الإلكترونية بالتطورالتقني والتكنولوجي مما يستوجب معه أن يكون القائمون على مكافحة تلك الجرائم على درجة عالية من المهارة في مواجهة تلك الجرائم ، وذات الأمر دفع المجتمع الدولي إلى اعتناق العديد من سبل التعاون الدولي لأهميته الكبيرة، كون أن ذات التعاون يهدف في المقام الأول إلى مواجهة كافة التهديدات الذي تشكلها الجرائم الإلكترونية، ويسعي نحو ضرورة اتخاذ سياسات فعالة ضد تلك الجرائم ، وبخاصة أن الأخيرة ذات جسامة كبيرة على المجتمع الدولي، وعلى الصعيد الوطني تعددت وسائل مكافحة الجرائم الإلكترونية، حيث استحدثت العديد من التشريعات الوطنية لكي تتلاءم مع ما يشهده المجتمع من تطورات تقنية وتكنولوجية، وكذلك تناسبها مع نوعية تلك الجرائم.
- المعالجة القانونية الدولية والاقليمية والوطنية لها أهمية كبري لأنها تعد بمثابة حجر الزاوية في مكافحة الجرائم الإلكترونية ؛ خاصة بعد أثبت الواقع فشل الجهود المبذولة داخل نطاق الدولة الواحدة أو الجهود الدولية غير الشاملة التي بذلت للحد من تلك الظاهرة في مجملها. مما تكمن اهمية موضوعنا في البحث والدراسة.

ثالثاً: إشكالية الدراسة:

- تتمثل صعوبة الدراسةنظرا لعدموجودقضاءدولي رادع ومتخصص تجاه مرتكبي الجرائم الإلكترونية، وبخاصة أن تلك الجرائم ازداد نطاقها واتسع نتاجا للتطورات العلمية والتكنولوجية الهائلة التي شهدها العالم في الوقت الحالي.
- كما تتجلي إشكالية الدراسة حول تأثير التطورات العلمية والتقنية على الفكر القانوني، وموقف الفقه القانوني من التقدم العلمي وتأثيره على القوانين، وبخاصة بعد أن ظهرتالكثير من المشكلات الجديدة تضاف إلى المشكلات التقليدية.
- كما تثاراشكالية دراستنا بالنظر الىالتطورالعلميوالتكنولوجي وما صاحبه من تقدم طرأ عليه تطورات شاسعة بفضل الطفرة العلمية الهائلة التي شهدها العلم في العصر الحديث، والتي لم تكن معروفة من قبل، ومدى تأثير ذلك التطور على التشريعات الوضعية التقليدية.

رابعاً: منهجية الدراسة :

أتبعنا في دراستنا المنهج الوصفي التحليلي الذي يهدف الي وصف وتشخيص موضوع البحث من مختلف جوانبه، عن طريق القيام بدراسة وتحليل النصوص الوضعية الدولية والوطنية المنظمة لذات الموضوع في ضوء اجتهادات الفقه القانوني، وما خلصت إليه الأحكام القضائية.

كما تطرقت الدراسة إلى المنهج المقارن فيما بين التشريعات الدولية والوطنية وذلك حتى يتم دراسة الموضوع بالشكل المطلوب.

خامساً: خطة الدراسة:

سنتناول في هذه الدراسة الحديث عن السياسات الدولية والوطنية تجاه مواجهة الجرائم الإلكترونية،حيث تنقسم إليمبحثين رئيسيين، يسبقهما مقدمة، ويعقبهما خاتمة تتضمن العديد من النتائج والتوصيات، وذلك على النحو التالي:

مقدمة وتشتمل على هدف البحث وأهميته ومشكلاته ومنهجه، **كما تشتمل الدراسة على التقسيم التالي :**

المبحث الأول-الإطار القانوني للتعاون الدولي المتعلق بمكافحة الجرائم الإلكترونية.

- المطلب الأول: التنظيم القانوني للتعاون الدولي على المستويالتشريعي والمؤسسي
- الفرع الأول: التعاون الدولي في إطار منظمة الامم المتحدة
- الفرع الثاني: التعاون الإقليمي تجاه الجرائم الإلكترونية .
- المطلب الثاني: تعدد سبل المساعدات الدولية
- الفرع الأول: تسليم المجرمين
- الفرع الثاني: التدابير المتعلقة بالمساعدات الأمنية والقضائية

المبحث الثاني - موقف التشريعات الوطنية تجاه الجرائم الإلكترونية.

- المطلب الأول: الاستراتيجيات التشريعية والوقائية تجاه الجرائم الإلكترونية
- الفرع الأول: المواجهة التشريعية تجاه الجرائم الإلكترونية.
- الفرع الثاني: الدور الوقائي تجاه الجرائم الإلكترونية
- المطلب الثاني: الاتجاهات العقابية المتعلقة بمكافحة الجرائم الإلكترونية
- الفرع الاول-: مكافحة الجرائم التي تمس بسرية وسلامة البيانات.
- الفرع الثاني: مكافحة جرائم غسل وتمويل الأموال.

خاتمة .

مراجع .

المبحث الأول

الإطار القانوني للتعاون الدولي المتعلق بمكافحة الجرائم الإلكترونية

تمهيد وتقسيم:

نجم عن العديد من الأوضاع المستحدثة التي شهدها العالم في النصف الثاني من القرن العشرين، بحدوث تقدم وتطور مذهل لقي صداه على كافة المستويات، وبخاصة

بعد استخدام الحاسوب، والطفرة التي شهدتها المجتمعات الرقمية والمعلوماتية، مما أصبحت الوسائط الالكترونية، ومنها شبكة الإنترنت بمثابة منتدي عام ومفتوح يتيح لجميع الأفراد ممارسة العديد من الحقوق المتعلقة بحرية التعبير بطريقة غير مسبوقة[7]، وبالرغم من ذلك فقد نجم عن استعمال الشبكة العنكبوتية ظهور انماط متعددة من الجرائم الإلكترونية .

وذات الأمر دفع العديد من الدول والحكومات في اطار المجتمع الدولي المنظم بوجوب التعاون فيما بينها مباشرة، بواسطة العديد من الهيئات الدولية العالمية والاقليمية والسياسية أو ذات الطابع الفني، بموجب العديد من النصوص القانونية التي تقرر مبدأ التعاون كأصل قانوني من أصول التنظيم الدولي المعاصر ،بحيث يمكن القول بأن مبدأ التعاون الدولي يعد اليوم احد المبادئ الرئيسية التي يقوم عليها التنظيم الدولي المعاصر ،والمجتمع الدولي المنظم الذى نعيش في أطاره[8].

ولذلك أصبحت مكافحة الجرائم بصفة عامة، احد الاهتماماًت الرئيسية للدول والحكومات، إذ إن الاستقرار في الحياة العامة والتقدم على كافة المستويات رهن بسلامة الأمن ومكافحة الجريمة، وذات الأمر تطلب اتخاذ العديد من الآليات التي تتعلق بالتعاون الدولي[9]. وبخاصة أن المجتمع الدولي يقوم على غايات مشتركة تتعاون الدول على تحقيقها [10].

ويتعين علينا لبيان الإطار القانوني للتعاون الدولي المتعلق بمكافحة الجرائم الإلكترونية تقسيم دراستنا على مطلبين على الوجه التالي:

- المطلب الأول- التنظيم القانوني للتعاون الدولي على المستويالتشريعي والمؤسسي.
- المطلب الثاني- تعدد سبل المساعدات الدولية .

المطلب الأول:

التنظيم القانوني للتعاون الدولي على المستويالتشريعي والمؤسسي

تمهيد وتقسيم:

شهد مفهوم "التعاون الدولي" تطوراً ملحوظاً خلال العقدين الأخيرين، وبخاصة أن هذا التطور يرتبط بالعديد من التطورات التي تشهدها قواعد التنظيم الدولي ودور المنظمات الدولية، وما طرأ على العلاقات الدولية من تطورات وتحولات في شتى المجالات؛ السياسية والاقتصادية والاجتماعية[11].

وعلى صعيد مواجهة الجرائم بصفة عامة أهتمت كافة الدول بضرورة تنسيق وتوحيد جهودها المشتركة في إطار "علاقات دولية تعاونية"، تهدف إلى زيادة

الفاعليات والقدرات– لمجابهة كافة المخاطر والتهديدات المتصاعدة لظاهرة الإجرام، فتعددت صور ووسائل التعاون وأغراضه ومدي قوة رابطته ونطاقه الجغرافي [12].

وفي إطار الجرائم الإلكترونية بات المجتمع الدولي المنظم يلتزم بوجوب التعاون فيما بين الدول ،مباشرة، ومن خلال الهيئات الدولية بكافة أنواعها ،العالمية والاقليمية.

ويتعين علينا لبيان التنظيم القانوني للتعاون الدولي على المستويالتشريعي والمؤسسي، تقسيم دراستنا على فرعين:

- الفرع الأول- التعاون الدولي في إطار منظمة الامم المتحدة .
- الفرع الثاني- التعاون الإقليمي تجاه الجرائم الإلكترونية .

الفرع الأول

التعاون الدولي في إطار منظمة الامم المتحدة

الأصل أنه توجد العديد من اجهزة في منظمة الأمم المتحدة المعنية بالتعاون الدولي لمكافحة الجريمة[13]، ولكنه بالنظر إلى خطورة الجرائم الإلكترونية فقد اهتمت المؤسسات الدولية ومنها- هيئة الأمم المتحدة-بمكافحة تلك الجريمة، وجعلته منأهم أولويات نشاطها نتيجة الأضرار والخسائرالكبيرة التي تولدها تلك الجريمة، كما ان منع هذه الجرائم يتطلب استجابة مشتركة على الصعيد الدولي بهدف التعاون للحد من انتشارها.

وعليه اهتمت منظمة الأمم المتحدة بمكافحة الجرائم الإلكترونية منخلال الإشراف على العديد من المؤتمرات الدولية الخاصة للقيام بردع الجريمة ومعاقبة المجرمين وفي ذات السياق نشير إلى أهم سبل التعاون الدولية في إطار المؤتمرات الدولية التي تتناول مواجهة هذا النوع من الجرائم ، على الوجه التالي:

ففي ظل المؤتمر السابع للأمم المتحدة الخاص بمكافحة الجريمة ومعاملة المجرمين لسنة 1985،الذى أشار إلى الجرائم الإلكترونية والصعوبات المتعلقة بها باعتبارها من الجرائم المتعدية الحدود، وفي أغسطس عام1995 عقد المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين في هافانا وكانت الجريمة الإلكترونية ، وكذلك حماية نظم المعالجة الآلية ومواجهة الاعتداءات التي تمس الحاسوب الآلي وملاحقة أحد الموضوعات التي تم بحثها [14].

وفي عام 1994، تولت منظمة الأمم المتحدة إصدار قانون نموذجي بهدف مساعدة الدول والحكومات في تحديث وتحسين القوانين الوطنية الداخلية المتعلقة بالجرائم الإلكترونية حتى تستطيع تلك التشريعات أن تواكب التطورات التي تشهدها الجرائم الإلكترونية وسبل وقاية ومكافحة تلك الجرائم [15].

كما ساهمت الاتفاقية المنشئة للمنظمة العالمية للملكية الفكرية[16]فيستوكهولم سنة 1967 والتي دخلت حيز النفاذ في 1970 إذتعتبرهذه المنظمة إحدى الوكالات المتخصصة في الأمم المتحدة، حيث ساهمت تلك المنظمة بواسطة المختصين والخبراء بتحقيق هدف مقتضاه حماية البرامج المتعلقة بالكمبيوتر، وإنفاذها إلى تشريعات الدول المتقدمة والنامية المتعلقة بحماية حق المؤلف، كما خلصت اتفاقية برن الدولية إلى أن برامج الحاسب الآلي "الكمبيوتر "سواء كانت بلغة المصدر أوبلغة الآلة تتمتع بالحماية [17].

كما عقدت منظمة الأمم المتحدة بدولة البرازيل في أبريل 2010مؤتمرهاالثاني عشر حول منع الجريمة والعدالة الجنائية، بهدف مكافحة الجرائم المستحدثة ومنها الجرائم الالكترونية، و التدابيراللازمة للتصدي لها.

وعلى صعيد الجمعيةالعامة للأمم المتحدة فقد لأصدرت العديد من القرارات والتوصيات المتعلقة بمجابهة الجرائم الإلكترونية ؛ منها قرار الجمعية المتعلق بمكافحة استغلال تكنولوجيا المعلومات لأهداف إجرامية والتي أصدرته الجمعية العامة للأمم المتحدة بموجب القرار رقم 63/55 بتاريخ الرابع من ديسمبر لسنة 2000، وبمقتضاه يحث الدول الأعضاء على تنسيق أعمال أجهزة الردع لديها، وكذلك تبادل المعلومات بشأن الصعوبات المتعلقة بمكافحة استغلال تكنولوجيا المعلومات لتحقيق أهداف إجرامية[18] .

كما أصدرت الجمعية العامة للأمم المتحدة القرار رقم A/RES/55/63 (عام 2001) متعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية[19].

وكذلك صدر القرار رقم A/RES/60/177 عام 2006،حيث يشجع ذات القرار على التعاون بهدف مكافحة الجرائم السيبرانية وتقديم كافة سبل المساعدات للدول الأعضاء[20].

وفي سنة 2010 أصدرت الجمعية العامة القرار رقم A/RES/64/211 متعلق بإرساء ثقافة عالمية تكفل أمن الفضاء الإلكتروني وتقييم الجهود الوطنية الرامية إلى حماية الهياكل الأساسية الحيوية للمعلومات، كما يدعو ذات القرار الدول الأطراف إلى تحديث التشريعات المتعلقةبالجرائم السيبرانية [21].

وفي سنة 2018 صدر قرار الجمعية العامة A/RES/73/266يدعو للارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي[22].

وفي يناير 2020 تضمن قرار الجمعية العامة A/RES/74/247الصادر في الدورة الرابعة والعشرون العديد من المسائل المتعلقة بمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية ،وذات القرار يدعو إلى إنشاء لجنة

حكومية دولية مفتوحة العضوية لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات[23]

تدعو الجمعية العامة في قراراتها المختلفة - التي غالبًا ما تكون مماثلة لقرارات الاتحاد الدولي للاتصالات - الدول الأعضاء، عند وضع القوانين الوطنية والسياسات العامة لمكافحة إساءة استعمال تكنولوجيا المعلومات، وأن تأخذ في الاعتبار أعمال لجنة منع الجريمة ولجنة العدالة الجنائية وغيرها من المنظمات الدولية والإقليمية.

وبالنسبة إلى مجلس الامن فقد أصدر العديد من القرارات منها القرار 2322لسنة 2016 ، والقرار لسنة 2016 2331،والقرار 2341 لسنة 2017 ،بمقتضاها دعا مجلس الأمن الدول الاعضاء إلى جمع الأدلة والمحافظة عليها حتى تتم التحقيقات والملاحقاتا لقضائية لمحاسبة الأشخاص المسؤولين عن الهجمات الإرهابية[24].

الفرع الثاني

التعاون الإقليمي تجاه الجرائم الإلكترونية

قد يأخذ التعاون الإقليمي مظهراً يتمثل في المنظمات الإقليمية التي تعمل على حماية مصالحها الاقتصادية و الثقافية و الاجتماعية ،بالتعاون فيما بين أعضاء المنظمات، تجاه الجرائم بصفة عامة التي تمثل خطرا يهدد مصالح جميع الدول وبالتالي أصبحت من أوليات اهتماماًت المنظمات الإقليمية مكافحة تلك الجرائم بجميع صورها وأشكالها الإجرامية والقضاء عليها[25]. ومنها الجرائم الإلكترونية

ولقد احتل التعاون الاقليمي بعد الحرب العالمية الثانية اهتماماً دولياً خاصاً، وشهد العالم نشوء منظومات للتعاون الاقليمي بدوافع عديدة، أهمها سياسية، أمنية، اقتصادية. وقد كانت الإخفاقات التيواجهت منظمة الأمم المتحدة كمنظمة دولية في تحقيق غاياتها، من أسباب هذا الاهتمام[26]، وغالباً ما يلعب الموقع الجغرافي أو التشابه الثقافي والمؤسسي دور في قيام التعاون الاقليمي[27].

وسوف نستعرض بعض سبل التعاون الإقليمي تجاه الجرائم الإلكترونية على وجه الايجاز :

أولا: اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية:

يرجع بداية الاتفاقية الاوربية المتعلقة بالجريمة الإلكترونية إلى عام1996، حيث كونت لجنة تتضمن العديد من الخبراء الأوربيين المتعلقة بالإجرام ، وفي الفترة ما بين عامي 1997 و 2000 صاغت نلك اللجنة اتفاقية تتعلق بمكافحة الجرائم السيبرانية (الإلكترونية) أطلق عليها اتفاقية بودابست لمكافحة الجرائم السيبرانية[28].

وتحظي اتفاقية مجلس أوروبا المتعلقة بشأن الجريمة المنظّمة ETS 185 بأهمية كبيرة لأنها أداة لها اهميتها، حيث أعدّ مجلس أوروبا هذه الاتفاقيةعلى مستوى الدول أعضاء مجلس الاتحاد الاوروبي بالتعاون مع كندا واليابان وجمهورية جنوب إفريقيا والولايات المتحدة الأميركية وعرضت للتوقيع في مدينة بودابست في 23 نوفمبر 2001 ودخلت حيّزالتنفيذفي الأول من يوليه 2004[29].

وتهدف تلك الاتفاقية إلى مكافحة الجرائم الإلكترونية التي تتم باستخدام / أو ضد الكمبيوتر و باستخدام شبكة الانترنت ،وكذلك العمل على توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية ، كما تضمنت هذه الاتفاقية في القسم الثالث منها بدور كبير في وضع إطار عام للتعاون الدولي في مجال مكافحة الجرائم الإلكترونية، حيث وضعت قواعد عديدة تتعلق بتسليم المجرمين ،وكذلك تنظيم سبل التعاون المتبادل المتعلق بتسليم المعلومة تلقائيا ،كما حددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية للدول الأعضاء[30]

ثانيا: جامعة الدول العربية :

تتميز الجامعة الدول العربية بأنها تشكل في حد ذاتها مشروعية قومية وليست اقليمية فقط[31]،ولقد تجلى التعاون على الصعيد العربي بإبرام جملة من المعاهدات الدولية من أجل الوقاية و الحد من الجرائم الالكترونية، حيث عقدت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010[32]؛ وتهدف هذه الاتفاقية الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات, لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[33]،كما تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك , على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها[34]،كما نص الفصل الثاني من الاتفاقية على تجريم انماط متعددة من السلوكيات، حيث قررت المادة الخامسة على أنه تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقا لتشريعاتها وأنظمتها الداخلية ، كما تضمن الفصل الرابع من الاتفاقية سبل التعاون القانوني والقضائي ، وكذلك صدر القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة لعام 2008[35]، حيث تناول الفصل السادس من ذات القانون الجرائم والعقوبات في المواد (من 33 إلى 39)، كما صدور كذلك القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية لعام 2009.[36]،وذات القانون متعلق بالمعاملات والتجارة التي تتم عبر الوسائط الالكترونية

ونري من جانبنا أنه بالرغم من مساهمة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذلك القوانين الاسترشادية في الحد من خطورة الجرائم الإلكترونية، والتصدي لها، بيد أنه يؤخذ علي تلك الاتفاقية والتشريعات الأسترشادية إلى أنها لم

واقع نظري بعيدة عن التطبيق والنفاذ الفعلي، كما لا تتطرق الاتفاقية بشكل واضح على مواد من شأنها أن تُحافظ على الحق في الخصوصية الفردية للمُستخدمين ومعلوماتهم وبياناتهم .

المطلب الثاني

تعدد سبل المساعدات الدولية

تمهيد وتقسيم:

تتعدد سبل المساعدات الدولية التي تساهم بدورها في مكافحة الجرائم الإلكترونية، وهو ما سوف نستعرضها على فرعين على الوجه التالي:

- الفرع الأول- تسليم المجرمين.
- الفرع الثاني- تعظيم الاجراءات الامنية وتقديم المساعدات القضائية.

الفرع الأول

تسليم المجرمين

استقر فقه القانون الدولي على اعتبار تسليم المجرمين من أهمسبل التعاون الدولي، والذى يهدف في المقام الأول إلى مكافحة الإجرام والجريمة والمجرمين.

وتسليم المجرمين أحد صور التعاون الدولي التي لها اهميتها ،كما أنها ترتبط بالتطورات التقنية والتكنولوجية وما يشهده المجتمع الدولي من طفرات في وسائل الاتصال والمواصلات.

ويراد بمفهوم تسليم المجرمين؛ بأنه هو الأجراء القانوني الذى تقوم به الدولة (دولة المطالبة / الطالبة) من أجل أن تحاكمه (تسليم لغاية المحاكمة) أو من اجل تنفيذ العقوبة عليه (تسليم لغاية التنفيذ) ، حيث إن التسليم المعرف على هذا المنوال هو وسيلة فعالة للتعاون الدولي لآنه يؤدى إلى الاعتقال الجسدي للفرد الذى تم تسليمه[37].

كما تعرفه المحكمة الجنائية الدولية التسليم في نظامها الأساسي تحت عنوان استخدام المصطلحات بأنه "يعنى نقل دولة ما شخصاً إلى دولة أخرى بموجب معاهدة أو اتفاقيه أو تشريع وطني"[38].

وعلى ذلك يجب على الدول تقوية إجراءات تسليم المجرمين من خلال التطبيق الفعال لذات النظام ، وبمقتضاه يفرض التزاماً على الدولة التي يتواجد على إقليمها المتهم بتطبيق قاعدة" التسليم أوالمحاكمة"، حيث يتم البحث والتحري عن هوية المجرم، ومكان تواجده، ثم القبض عليه وأدانته طبقا للتشريع الوطني الداخلي في حالة

امتناع الدولة عن القيام بتسليمه لدى دولة أخرى، كما يتعين على جميع دول العالم الالتزام بتنظيم القانون الدولي والتوفيق بين ضرورات التعاون القضائي الدولي ومقتضيات السيادة للحماية من جرائم القرصنة الإلكترونية[39].

وإجراء التسليم يقوم على أن الدولة التي يتواجد على اقليمها المتهم بارتكاب جريمة الكترونية عليها أما ان تقوم بمحاكمته إذا كانت تشريعاتها تسمح بذلك، أو القيام بتسليمه لمحاكمته بمعرفة دولة أخري مختصة، وذات الامر يحقق مصلحة الدولتين اطراف عملية التسليم [40].

ويعد تسليم المجرمين من التدابير التي لها اهميتها لمواجهة الجرائمالإلكترونية، ولا سيما أن تلك الجرائم الأخيرة تعتبر من الجرائم العابرة للحدود الدولية، فلم تعد الحدود القائمة فيما بين الدول تشكل عائقاً أمام ارتكاب تلك الجرائم، كما لم يقتصر الفعل الإجرامي على منطقة إقليمية محددة، بل أصبح يمتد اثره ليشمل العديد من الدول، من أجل ذات الأمر يتعين على الدول وضع العديد من الضوابط المتعلقة بنظام تسليم المجرمين، ومواجهة المجرم الإلكتروني.

الفرع الثاني

تعظيم الاجراءات الامنية وتقديم المساعدات القضائية

رغم أهمية الآليات المتعلقة بتسليم مجرمي الجرائم الإلكترونية في مواجهة نلك الجرائم ،إلا أن هناك العديد من التدابير والآليات الأخرى على الصعيد الأمني والقانوني والقضائي تهدف في المقام الأول إلى الحد من مخاطر الجرائم الإلكترونية، وسوف نستعرض بعض تلك التدابير على الوجه التالي: .

اولاً: تبادل المعلومات:

يتمثل ذلك في تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما أن هناك مظهر آخر من مظاهر تبادل المعلومات وهو مايتعلق بالسوابق القضائية للجناة من خلالها تتعرف الجهة القضائية بدقة على الماضي الجنائي للفرد المحال إليها، فهي التي تساعد في تطبيق الأحكام الخاصة بالعود ووقف تنفيذ العقوبة وعدم الأهلية(41).

وفي ذات الإطار فقد نصت الفقرة الثالثة من المادة 28 في الفقرة الثانية من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصيةعلى تأكيد أهمية تبادل المعلومات.

ثانياً: دور المؤسسات الامنية الدولية :

بالرغم من عدم وجود جهاز شرطة عالمية يتمتع أعضاؤه بصلاحية التحري عن الجرائم والبحث عن أدلتها والقبض علي مرتكبيها، يعد إحدى النتائج الأساسية التي تترتب علي مبدأ سيادة الدولة علي إقليمها .وكذلك بالرغم من أنه لا يجوز للشرطة في دولة معينة أن تقوم بإجراء علي إقليم دولة أخري ، ولا تلتزم بالقيام بعمل علي أراضيها بناء علي طلب دولة أجنبية. إلا أن الدول قد حرصت علي إرساء دعائم التعاون الأمني فيما بينها، واهتمت بتعزيز وسائله، بغية مكافحة الجريمة بصفة عامة، والجريمة المنظمة العابرة للحدود علي وجه الخصوص(42).

ولذلك قطع التعاون الشرطي الدولي شوطاً طويلاً سواء على مستوى التعاون الثنائي أو التعاون متعدد الأطراف ،إقليمياً أو عالمياً، وكان من ابرز العلامات على طريق هذا التعاون إنشاء منظمة الشرطة الجنائية "إنتربول "وظهور العديد من صور وأشكال ووسائل التعاون بين أجهزة الشرطة(43).

بالنظر إلى طبيعة جرائم الإنترنت كونها ذات طابع عالمي، حيث تتعدى آثارها العديد منا لدول؛ وعلى ذلك فيتم ملاحقة مرتكبي تلك الجرائم، وتقديمهم للمحاكمة، وكذلك توقيع العقاب عليهم، وذات الأمر يستلزم القيام بأعمال إجرائية خارج حدود الدولة، مثل المعاينة، أو ضبط الأقراص الصلبة التي توجد عليها معلومات أو بيانات غير مشروعة، أو تفتيش الوحدات الطرفية في حالة الاتصال عن بعد أو القبض على المتهمين أو سماع الشهود أو اللجوء إلى الإنابة القضائية أو تقديم المعلومات التي يمكن أن تسهم في تحقيق الجرائم .فكل ذلك لن يتحقق إلا بمساعدة الدول الأخرى(44).

وفي ذات الصدد أشار قرار مجلس الأمن رقم 2322لسنة 2016 بالتحديد إلى الزيادة الكبيرة في طلبات التعاون في جمع البيانات والأدلة الرقمية من الإنترنت، وشدد على أهمية النظر في إعادة تقييم الطرق وأفضل الممارسات، حسب الاقتضاء، على وجه الخصوص، فيما يتعلق بتقنيات التحقيق والأدلة الإلكترونية(45).

ثالثاً: المساعدات القضائية الدولية:

يشكل التعاون القضائي في حد ذاتها لقاعدة اللازمة لإقامة تعاون دولي فعّال . ومن شأن وجود التشريعات الإجرائية الفعّالة تساهم بدور بارز في عملية التعاون وسيرها بشكل آلي وسهل، حتى أنه من المفضل بالطبع اتخاذ إجراءات وتدابير لتسهيل عملية بناء هذا التعاون، وتعتبرعملية تجريم الفعل بين جميع الأطراف بمثابة أساس تشريعي يتحدد بناء عليه لتعاون بين الطرفين، بيد أنه قد يحدث خلاف عندما يكون القانون الجزائي للدولة متلقية الطلب بتسليم الجُناة لايعاقب على تلك السلوكيات الإجرامية(46).

ويرادبالمساعدة القضائية الدولية "" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخري بصدد جريمة من الجرائم"(47).

وفي إطار الجرائم الإلكترونية فأن فعالية الملاحقة القضائية تقتضي اتخاذ تدابير ذات فعالية كبيرة، وأكثر سرعة في ملاحقة مرتكبي تلك الجرائم، وتتخذ المساعدة القضائية في المجال الجنائي صور عدة منها:

1-**التعاون القضائي** يتحقق عند تقديم المشورة القضائية عندما يمكن لذلك القاضي أن يتوجه إلى زميله في موقعه بالبلد المعني لطلب المساعدة، فإنه يستطيع عندها تحرير طلبه أخذا بعين الاعتبار المقتضيات المخصوصة المتعلقة بالتعاون القضائي الجنائي الثنائي، ويمكن للقضاة أوضباط الاتصال أن يضطلعوا بدور" الميسّر"، بمعنى أن عددا من السلطات المختصة تنحو أكثر فأكثر إلى أن تُبّلغ القاضي أو ضابط الاتصال موضوع الإنابة قضائية تعتزم إرسالها إلى السلطات الأجنبية . وآنذاك، يكون زميلهم، في مركزعمله بالبلد(48).

2-الإنابة القضائية الدولية؛ هي أحد صور التعاون الدولي في مكافحة الجريمة والتي تتم على المستوى القضائي بين الدول، على اعتبار أنها تتعاون بين الأجهزة القضائية المختلفة للدول(49).

وبعض الفقه يري بأن الإنابة القضائية هي ناتجة عن الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة ، وبموجبها يعهد للسلطات القضائية – المطلوب منها اتخاذ إجراء – القيام بالتحقيق أو بالعديد من التحقيقات، لمصلحة السلطة القضائية المختصة في الدول الطالبة ، مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالمياً ، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل ،واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية(50).

وتعني الإنابة وفقاً للمادة (٦) من اتفاقية الإعانات والإنابات القضائية (51) أنه:" لكل من الدول المرتبطة بهذه الاتفاقية أن تطلب إلى أية دولة منها أن تباشر في أراضيها نيابـةعنها أيّ إجراء قضائي متعلق بدعوى قيد النظر، وفقاً لأحكام المادتين (٧ ،٦).

وتهدف تلك الصورة إلى تسهيل الإجراءات الجنائية فيما بين الدول بما يكفل إجراء التحقيقات اللازمة بهدف تقديم المتهمين للمحاكمة العاجلة والتغلب على عقبة السيادة الاقليمية(52).

3- نقل الإجراءات، إدراكا من الدول بضرورة اهمية التعاون على الصعيد الدولي لمواجهة الجرائم الالكترونية والتصدي لها ،فعقدت العديد من الاتفاقيات الثنائية بهدف تسهيل مهمة التحقيق لمواجهة الجرائم الالكترونية العابرة للحدود[53].والتحقيق يعتبر

أحد الإجراءات المتبعة لمواجهة الجرائم الإلكترونية فيقتضي لذلك التعاون القضائي بنقل الإجراءات

ويراد بمفهومنقل الإجراءات قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصددجريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الدولة مادام توافرت شروط معينة منأهمها التجريم المزدوج، بمعنى أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات. بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها أي أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة. وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدى دوراً مهماً في الوصول إلى الحقيقة[54].

ولقد أقرت العديد من الاتفاقيات الدولية والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية(55).

المبحث الثاني:
موقف التشريعات الوطنية تجاه الجرائم الإلكترونية

تمهيد وتقسيم:

الجرائم الإلكترونية تولدت بظهور الإعلام العالمي الجديد، ويسمي I Tunes من آبل، والفيس بوك، وتويتر، وجوجل، ومايكروسوفت، الذى يفرض من خلالها أنظمته على أجزاء كبيرة من العالم[56].

كان لظهور هذا النوع من الجرائم الأثر الهام في خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول وخاصة في ظل قصور قانون العقوبات عن مواجهة تلك الجرائم, الأمر الذي دعي الفقه والقضاء إلى أن الأمر يستدعي استحداث قواعد قانونية جديدة أو نصوص خاصة قادرة على احتواء هذا النوع من الجرائم تراعي طبيعتها وخصوصيتها[57]

علاوة على أن الجرائم الإلكترونية تتسع نطاقها، و تتعدد صورها في الوقت الحالي، ولقد شهدت على الصعيد الواقعي والعملي انتشاراً كبير، وبخاصة أن سمات الأدلة في قضايا جرائم الإنترنت تمتاز بسرعة انتقالها، بالإضافة إلى حساسيتها الشديدة، حيث يمكن أن تتعرض للتخريب والإتلاف، كذلك يمكن حفظها، ونسخها ونقلها في لحظة واحدة، مما توجد صعوبة كبيرة في تعقب البيانات غير المشروعة[58].

ويقتضي علينا لبيان موقف التشريعات الوطنية تجاه الجرائم الإلكترونية ، استعراضه على مطلبين:

- المطلب الأول- الاستراتيجيات التشريعية والوقائية تجاه الجرائم الإلكترونية.
- المطلب الثاني-الاتجاهات العقابية المتعلقة بمكافحة الجرائم الإلكترونية.

المطلب الأول:
الاستراتيجيات التشريعية والوقائية تجاه الجرائم الإلكترونية

تمهيد وتقسيم:

واجهت غالبية الدول الجرائم الإلكترونية بإجراءات تشريعية سواء بالانضمام للمعاهدات الدولية، وعقد العديد من الاتفاقيات الثنائية ، كما أن الجانب الوقائي ساهم بدوره في مكافحة تلك الجرائم، وهو ما سنوضحه على الوجه التالي في فرعين :

الفرع الأول- المواجهة التشريعية تجاه الجرائم الإلكترونية.

الفرع الثاني- الدور الوقائي تجاه الجرائم الإلكترونية.

الفرع الأول:
المواجهة التشريعية تجاه الجرائم الإلكترونية

اولاً: اتخاذ تدابير تشريعية رادعة :

يقتضي التأكيد على أن تجريم السلوكيات التي تمثل انتهاك في حماية المعلومات والاتصالات عبر الفضاء السيبراني، فيتعين ذات الأمر سن القوانين المتخصصة لمواجهة تلك السلوكيات، ولا يتم الاعتماد على التفسيرات التي قد تلتبس بالقواعد العامة(59).

علاوة على أن الطبيعة التقنية للمعلوماتية ، يتعين أن يفرد لها المشرع أحكام خاصة تحكمها، نظراً إلى طبيعتها الذاتية سواء على الصعيد الإجرائي أو الموضوعي، كما أن اللغة التقنية قد يضطر القاضي إلى استعمالها ،وذات الأمر مرهون بإجراء دورات تدريبية خاصة لجميع الفئات ذات الصلة بالقانون سواء تمثلت في رجال القضاء والمحققين ورجال الشرطة بهدف التعامل مع طبيعة تلك الجرائم والأدلة الثبوتية (60).

ونري من جانبنا بأن التشريع يعتبر هو خط الدفاع الأول لمواجهة الجرائم الإلكترونية، ولا سيما أنه بمثابة أداة لها فاعليتها المؤثرة بهدف تحقيق العدالة الجنائية، وكذلكالردع العام والخاص، وبخاصة أن الجرائم الإلكترونية لم تعد ذات شأن داخلي بكل دولة، بل اتخذت أبعادا متعدية الحدود الوطنية ، وعابرة للقارات .

ثانياً-الانضمام للمعاهدات الدولية والاتفاقيات الثنائية والتنسيق بينها:

لعبت المعاهدات والاتفاقيات باعتبارهم من صور التعاون الدولي دور كبير في إرساء قيمة التعاون الدولي ما بين الدول وحل الكثير من المشكلات(61).

كما حظيت المعاهدات والاتفاقيات في النظام الدولي بأهمية كبيرة، كونها مصدر رئيسي للالتزامات التعاقدية، بالإضافة إلى أنها أحد مصادر القانون الدولي المدون، ولذلك كان لصدور قانون المعاهدات أهميته القانونية، لأنه يعد تسجيلاً للقواعد التي تحكم وسيلة التدوين، وعليه يعتمد أيضا ما يرجى لهذه العملية من تقدم ونجاح(62).

وفي ذات الإطار يقسم التعاون الدولي إلى تعاون ثنائي الأطراف أو تعاون اقليمي ، وأخيراً قد يتحقق بواسطة الانضمام إلى المعاهدات الدولية الشارعة (63).

ويخول للمؤسسات الدولية مسؤولية تنسيق التشريعات الإلكترونية فيما بين الدول، وذات التنسيق من الممكن تحقيقه بفضل الاتفاقيات الدولية والتوصيات والقرارات ذات الشأن الدولي(64)

وعلى صعيد التطبيق الواقعي فلقد ابرمت العديد من الدول الوطنية، العديد من الاتفاقيات الثنائية التي تهدف في المقام الأول إلى مكافحة الجرائم الإلكترونية.

الفرع الثاني

الدور الوقائي تجاه الجرائم الإلكترونية

اولاً: وضع استراتيجيات تنفيذية متعلقة بمكافحة الجرائم الإلكترونية :

يتمثل سياسات المكافحة على الصعيد التنفيذي تجاه الجرائم الإلكترونية بوضع سياسات شاملة وعامة من قبل الحكومات تتولاها اجهزة الدولة المختصة، ويتعين أن تتضمن تلك الاستراتيجيات كافة المتطلبات اللازمة لمكافحة الجرائم الالكترونية وإجراءاته ،وكافة التدابير والإجراءات المتعلقة بالحماية التقنية والتنظيمية والتشغيلية، وكيفية التصرف في مكافحة الجرائم الالكترونية والتبليغ عنها وتقديم الدعم لضحايا تلك الجرائم، كما يتعين رفع الوعي التوعوي والتثقيفي بهذه السياسات وتعميمها على كافة إدارات الدولة وعلى جميع الأشخاص والمؤسسات(65)

ثانياً: التعاون والتنسيق وتبادل المعلومات بين السلطات:

تتحقق القدرة على التعاون من قبل السلطات ، حيث يمكن للقواعد والإجراءات التي تتخذها السلطات تحقيق الكثير؛ حيث أنه بواسطتها تمتلك صلاحيات كبيرة لتبادل المعلومات،كما يمكن لها أن تزيل كافة العوائق التي تحول دون تبادل المعلومات من خلال رفع السرية، علاوة على اتخاذ الإجراءات المناسبة للتعاون، وإنشاء كافة اللجان وتعيين منسقين، وغيرها(66).

وعلى ذلك يحث قرار مجلس الأمن الصادر عام 2019 على القيام، على الصعيد الوطني، بوضع أو تعزيز إطار عمل يتيح للسلطات الوطنية المختصة، وخصوصا وحدات الاستخبارات المالية، وأجهزة الاستخبارات، ووكالات إنفاذ القانون، ودوائر النيابة العامة و/أو السلطات القضائية، إمكانية جمع وتبادل المعلومات عن تمويل الإرهاب(67).

ومن جانبنا فنحن نوصي إلى انتهاج سياسات استراتيجية مشتركة تهدف إلى مواجهة الجرائم الإلكترونية سواء على الصعيد الوطني أو الثنائي أو دون الإقليمي، أوعلى المستوي القاري، أوالدولي

المطلب الثاني: الاتجاهات العقابية المتعلقة بمكافحة الجرائم الإلكترونية

تمهيد وتقسيم:

تعددت الاتجاهات العقابية المتعلقة بمكافحة الجرائم الإلكترونية، كما تباينت السياسات الجزائية على الصعيد الوطني المتعلقة بمواجهة تلك الجرائم واختلفت أحكامها من دولة إلى أخرى، ويكمن سبب ذات الاختلاف والتباين وذلك لتباين الأهداف والاستراتيجيات، و اختلاف الفلسفة التي تعتنقها كل دولة

وبالنظر إلى تعدد الجرائم الإلكترونية إلا أننا فسوف نتناول انماط محددة من تلك الجرائم ،وهو ما سنوضحه على الوجه التالي في فرعين :

- الفرع الاول- مكافحة الجرائم التي تمس بسرية وسلامة البيانات.
- الفرع الثاني- مكافحة جرائم غسل وتمويل الأموال.

الفرع الاول

مكافحة الجرائم التي تمس بسرية وسلامة البيانات

اولاً: بالنسبة إلى الجرائم التي تمس بسرية بيانات المستند:

واجهت العديد من التشريعات الوضعية جرائم الاختراق والدخول غير المشروع، وتقع جريمة الدخول غير المشروع، متنكان ذلك الدخول مخالف الإرادة صاحب النظام أو ممن له حق السيطرة عليه،كما تقوم كذلك جريمةالاختراق أوالدخول غير المشروع حين يضع مالك النظام قيود اعلى الدخول لذات النظام، ولايحترم الجاني تلك القيود، أو كان الأمر يتطلب سداد مبالغ من النقود لم يسددها الجاني الذي قام بالدخول غيرالمشروع إلى النظام (68).

فعلى صعيد التشريع المصري تطرقت المادة 14من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات(69)علىتلك الجريمة(70)، واعتبرها جنحة ،حيث أقر لها عقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن خمسين الف جنية ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

وذات التكييف القانوني بوصف الجريمة جنحة أقرته العديد من التشريعات المقارنة، ومنها التشريع العماني(71)، حيث تنص المادة الثالثة من قانون جرائم تقنية المعلومات الصادر بموجب المرسوم السلطاني العماني رقم 2001/12 بشان قانون مكافحة جرائم تقنيه المعلوماتبمعاقبة الجاني بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر، وكذلك عقوبة الغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين(72). علاوة على ذلك المشرع الإماراتي اعتبرها جنحة(73)، وأقر لها عقوبتي الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين(74).

ويتضح بذلك أن مسلك التشريعات تجاه مواجهة الجرائم التي تمس بسرية بيانات المستند الإلكتروني العديد من الملاحظات التي تتمثل في:

- استخدمت تلك التشريعات حرف العطف (و) في النص التجريمي مما يفيد انه توقع كلا العقوبتين.
- خولت تلك التشريعات للقاضي الجنائي سلطات تقديرية كبيرة ما بين توقيع العقوبة السالبة للحرية المقررة أو عقوبة الغرامة أو توقيع كلا العقوبتين.

ثانياً: مكافحة الجرائم التي تمس بسلامة بيانات المستند الإلكتروني:

تتعددالجرائم التي تمس بسلامة بيانات المستند الإلكتروني سواء كانت متعلقة

بجريمة اتلاف المستند الإلكتروني، أوجريمة التزوير الإلكتروني.

فبالنسبة لجرائم اتلاف المستند الإلكتروني، فأن تلك الجريمة تتحقق بصور مختلفة،فقد تكون وسيلة التعطيل مادية، كما لو وقع على الاجهزة عنف أو تخريب أو قطع وسائل الاتصال مما ادي الى تعطيلها،وقد يتحقق بوسيلة معنوية مثل إدخال فيروس في نظام التشغيل(75).

وفي ذات السياق تطرق المشرع المصري في المادة 21 على جريمة الاعتداء على سلامة الشبكة المعلوماتية ،واعتبرها جنحة، حيث أقر لها عقوبة الحبس لمدة لا تقل عن ستة أشهر وبغرامة لاتقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين(76).

وفي ذات الصدد نظر المشرع العماني إلى تلك الجريمة باعتبارها جنحة، وأقر لها عقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني أو بإحدى هاتين العقوبتين(77).

أما المشرع الإماراتي، فقد اعتبرها جناية، وأقر لها عقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين. ...." (78)، تأسيساً على ذلك تنص المادة 28 من قانون العقوبات الإماراتي على أن "الجناية هي الجريمة المعاقب عليها بإحدى العقوبات الآتية ومنها ...4-السجن المؤقت"، كما تنص المادة 68 من قانون العقوبات الإماراتي على أن" السجن هو وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة قانونا لهذا الغرض وذلك مدى الحياة ان كان السجن مؤبدا أو المدة المحكوم بها ان كان مؤقتا .ولا يجوز أن تقل مدة السجن المؤقت عن ثلاث سنوات ولا أن تزيد على خمس عشرة سنة ما لم ينص القانون على خلاف ذلك"

ومن جانبنا فنحن نؤيد مسلك المشرع الإماراتي في إقراره للعقوبة المقررة لتلك الجريمة لأنه يشدد الجزاء على مرتكبي تلك الجريمة، مما يصبح الجزاء الجنائي ذات اثر رادع، ولاسيما أن العقوبة تتناسب مع الجريمة المرتكبة، ومن ثم فنحن نوصي كلا المشرعين المصري والعماني بتشديد العقوبة على أن لا تقل عن خمس سنوات).

ومن ناحية أخري وبالنسبة لجرائم التزوير الإلكتروني، وبخاصة أن نصوص القانون الجنائي قد وضعت بهدف تنظيم المستند أو المحرر الورقي،وعليه لا يمكن القول بإعادة تفسير النصوص التقليدية، وسريانها على المستند الإلكتروني،فيتعين صدور تنظيم تشريعي للمستند الإلكتروني يراعى ضمانات يجب أن تتوافر في المستند حتى يكفل له الفاعلية في التعامل وقبول في التعاملات(79).

وتقع جريمة التزوير الإلكتروني على مخرجات الحاسوب، في صورته الرقمية أو أية بيانات أو معلومات عن طريق الكمبيوتر بشرط انفصالها عن الشرائط والتسجيلات المغناطيسية أو على شرائط F-Dأو أقراص مدمجة C.D(80).

ومن جانبنا فنحن نؤيد ذات الاتجاه وبخاصة أن طبيعة المستند الإلكتروني تختلف عن غيرها من المستندات الأخرى التقليدية ، ولذلك يتعين مراعاة ذلك تشريعياً، علاوة على أن قداسية مبدأ الشرعية الجرائم والعقوبات تقتضي عدم التوسع في النص القانوني أو القياس عليه

الفرع الثاني: مكافحة جرائم غسل وتمويل الأموال

ساهمت الشبكة العنكبوتية بدور كبير في انتشار جرائم غسل الأموال، وتمويل الجماعات الإرهابية؛ ويرجع السبب في ذلك إلى مزايا تلك الشبكة كونها وسيلة رخيصة وسريعة، وذات كفاءة كبيرة ، واستخدمت كأداة لارتكاب تلك الجرائم العملات الافتراضية [81].

ومن ذات المنطلق ساعدت الوسائط الإلكترونية– ومنها شبكة الإنترنت في اقتراف جرائم غسل الأموال[82]، وتمويل العمليات الإرهابية.

وفي ذات الصدد أشارت العديد من التقارير الأمريكية إلىأنّ جماعات الإرهاب يين ستعتمد على الإنترنت بصورة متزايدة، بهدف الحصول على الدعم المالي واللوجستي، وأشار التقريرأيضاًإلى أنّ التكنولوجيا والعولمة، مكّنتا الجماعات الإرهابية،من الاتصال ببعضها، بجانب توفير الدعم المادي اللازم للقيام بالهجمات دون الحاجةإلى تكوين منظمة إرهابية[83].

وذات الأمر دفع المشرع المصري إلى إيراد تعديلات تشريعية متعلقة بجرائم غسل الأموال، وجرائم تمويل العمليات الإرهابية[84]، ويراد بالأموال أو الأصول؛ جميع الأصول المادية والافتراضية والموارد الاقتصادية ، .... أياً كان شكلها بما في ذلك الشكل الرقمي أو الإلكتروني وجميع الحقوق المتعلقة بأي منها ....[85].

ولقد أحسن المشرع المصري صنعا كونه أقر بوقوع الجريمة على كافة الأموال المنقولة ذات الطابع المادي، كما يمتد التجريم إلى الأموال الافتراضية أوالمشفرة ، ولا سيما أن ارتكاب الجرائم المتعلقة بجريمة غسلالأموال أو تمويل العمليات الإرهابية قد يتحقق بواسطة العملات الافتراضيةإذا ارتكبت عبر شبكة الإنترنت .

ويطبق قانون مكافحة الإرهاب المصري رقم 94 لسنة 2015وتعديلاته [86] اقليميا على كافة الجرائم التي ترتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبا عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وذلك إذا تم الاعداد للجريمة أو التخطيط أو التوجيه أو الاشراف عليها أو تمويلها فيمصر [87].

والعقوبة المقررة لجرائم التمويل في التشريع المصري نصت عليها المادة 13من قانون مكافحة الإرهاب رقم 94 لسنة 2015 وتعديلاته [88]على أنه "يعاقب بالسجن المؤبد كل من ارتكب جريمة من جرائم تمويل الإرهاب إذا كان التمويل لإرهابي, وتكون العقوبة الإعدام إذا كان التمويل لجماعة إرهابية أو لعمل إرهابي....".

كما تناول المشرع العماني في المـــادة 20 من قانون جرائم تقنية المعلومات جرائم تمويل الإرهاب واعتبرها جناية[89]، حيث أقر لها عقوبة بالسجن المطلق وبغرامة لا تقل عن مائة ألف ريال عماني ولا تزيد على مائتي ألـف ريـال عماني[90]، في حين تطرقت المـــادة 21 من قانون جرائم تقنية المعلومات العماني الجرائم المتعلقة بغسل الأموال عبر الوسائط الإلكترونية[91]

وعلي صعيد التشريع الإماراتي تنص المادة 29 من القانون الاتحادي الإماراتي رقم 7 لسنة 2014 في شأن مكافحة الجرائم الارهابية على انه يعاقب بالسجن المؤبد أو المؤقت الذى لا تقل مدته عن عشر سنوات كل من :

1. قدم أموالا أو جمعها أو أعدها أو حصلها أو سهل للغير الحصول عليها بقصد استخدامها أو مع علمه بأنها سوف تستخدم كلها أو بعضها في ارتكاب جريمة

إرهابية .
2. قدم أموالا لتنظيم إرهابي أو لشخص إرهابي أو جمعها أو اعدها له أو حصلها أو سهل له الحصول عليها مع علمه بحقيقة أو غرض التنظيم أو الشخص الإرهابي
3. اكتسب اموالا أو اخذها أو ادارها أو استثمرها أو حازها أو نقلها أو حلولها أوو أودعها أو حفظها أو استخدمها أو تصرف فيها أو قام بأي عملية مصرفية أو مالية أو تجارية مع علمه بأن تلك الأموال كلها أو بعضها متحصلة من جريمة إرهابية أو مملوكة لتنظيم إرهابي أو معدة لتمويل تنظيم إرهابي أو شخص إرهابي أو جريمة إرهابية.

كما نص المشرع الإماراتي في المادة 37 من قانون مكافحة جرائم تقنية المعلومات الإماراتي على أنه "مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال، يعاقب بالحبس مدة لا تزيد على سبع سنوات وبالغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليوني درهم كل من أتى عمداً، باستخدام شبكة معلوماتية ، أو نظام معلومات إلكتروني ، أو إحدى وسائل تقنية المعلومات، أي من الأفعال الآتية:

(1) تحويل الأموال غير المشروعة أو نقلها أو إيداعها بقصد إخفاء أو تمويه المصدر غير المشروع لها.
(2) إخفاء أو تمويه حقيقة الأموال غير المشروعة أو مصدرها أو حركتها أو الحقوق المتعلقة بها أو ملكيتها .
(3) اكتساب أو حيازة أو استخدام الأموال غير المشروعة مع العلم بعدم مشروعية مصدرها ....."

ونري من جانبنا أن اختلاف توقيع الجزاء الجنائي بخصوص جريمة التمويل يخول للقاضي الجنائي توقيع العقوبة الأشد المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات الإماراتي، وذلك تأسيسا على ما تقرره المادة 87 من قانون العقوبات الإماراتي على أنه "إذا كون الفعل الواحد جرائم متعددة وجب اعتبار الجريمة التي عقوبتها أشد والحكم بعقوبتها دون غيرها".

خاتمة

تناولت الدراسة السياسات المتبعة على الصعيد الدولي والوطني تجاه مواجهة الجرائم الإلكترونية، حيث تم مكافحة تلك الجرائم بواسطة العديد من الاستراتيجيات الفعالةالتي تهدف إلى مواجهة تلك الجرائم بجميع اشكالها، والتصدي لها، كما تتحقق المكافحة من خلال تدعيم كافة التدابير والإجراءات سواء كانت وقائية، أو تشريعية، أو قضائية، وذلك بهدف منع ومكافحة تلك الجرائم والقضاءعليها. **وخلصت الدراسة إلى مجموعة من التوصيات**

1. زيادة نشر الوعي للتعريف بالجرائم الإلكترونية وخطرهامن خلال رفع الوعي التثقيفي عبر وسائل الاعلام ، وغيرها من الوسائل الاعلامية والثقافية دور كبير في الحد من الجرائم الإلكترونية، كما يتعين إقامة المؤتمرات والندوات المتعلقة بذات الموضوع.
2. ضرورة العمل على توحيد الجهود الدولية، ويتحقق ذلكبعقد مؤتمر دولي يتناول أحكام الجرائم الإلكترونية، وسبل مواجهتها تشريعياً، بالعمل على صياغة قانون موحد لمعالجة جرائم المعلوماتية يكون تحت رعاية الأمم المتحدة، وأن يكون هناك

أساليب رادعة ملزمة لمواجهة ذات الجرائم .

3. ضرورة تأهيل، وتكوين قضاة متخصصين في هذا النوع من الجرائم وإقامة محاكم مختصة في هذا المجال .
4. أولوية مكافحة الجرائم الإلكترونية عن طريق تبني استراتيجيات شاملة متعددة الجوانب تعتمد على مواجهة كافة مظاهر تلك الجريمة، وكافة أشكالها وصورها وأنماطها المختلفة .
5. أهمية مواءمة التشريعات القانونية لكافة المستجدات التي تشهدها الجرائم الإلكترونية، وبخاصة أن الجرائم الإلكترونية من الجرائمالمستحدثة والمتطورة وغير تقليدية مما يستوجب ضرورة الإسراع في وضع وتطوير تشريع جنائي يكفل حمايتها من خلال إيجاد آليات جديدة تتلائم و طبيعتها الموضوعية و الإجرائية
6. نوصي بالاستفادة من خبرات الدول التي نجحت في مكافحة الجرائم السيبرانية بصورة كبيرة، أو الحد من خطورة تلك الجرائم، كما أنه يتعين الاستفادة من المؤسسات الدولية التي تساهم في تقديم العون المادي والمعنوي في مكافحة تلك الجرائم.
7. ضرورة تفعيل التعاون الدولي من خلال إبرام المزيد من الاتفاقيات الدولية على المستوى الإقليمي والعالمي.

قائمة المراجع

اولا: المراجع باللغة العربية:

1-الكتب العلمية:

1. تيري ناردين، النظرية السياسية الدولية، بحث منشور في كتاب نظريات العلاقات الدولية، ترجمة محمد صفار ،سلسلة العلوم الاجتماعية للباحثين، المركز القومي للترجمة، القاهرة، العدد 2022،الطبعة الأولى، سنة 2014
2. عادل محمد السيوي، التعاون الدولي في مكافحة جريمتي غسل الأموال وتمويل الإرهاب ، نهضة مصر للطباعة والنشر والتوزيع ،الطبعة الاولي ،يوليو 2010
3. عادل يحيى، الأحكام العامة للتعاون الدولي في مكافحة الجريمة، دار النهضة العربية ،القاهرة، الطبعة الأولى، 2013،
4. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، سنة 2004
5. عبد الفتاح بيومي حجازي، جريمة غسل الأموال عبر شبكة الإنترنت ، دار النهضة العربية ،القاهرة ،الطبعة الاوى ،سنة 2009
6. علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، رؤية لاستراتيجية وطنية للتعاون الدولي في مجال مكافحة المخدّرات، القاهرة ،طبعة 2000
7. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، الطبعة الثانية، سنة 1995
8. فائزة يونس الباشا، الجريمة المنظّمة في ظل الاتفاقيات الدولية والقوانين الوطنية، دار النهضة العربية ، ط1 ،سنة 2001
9. ليندا بن طالب، غسل الأموال وعلاقته بمكافحة الإرهاب، "دراسة مقارنة"، دار الجامعة الجديدة، الإسكندرية، طبعة 2011
10. محمد محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، بدون دار نشر، طبعة 2007

2- الرسائل الأكاديمية:

(أ) رسائل الماجستير:

بوخافةسعاد،مبدأالتسليمو المحاكمةعلىضوءأعمالاللجنةالقانونالدولي،رسالةماجستير،كلية الحقوق،جامعةبنعكنون،الجزائر،2014

(ب)رسائل الدكتوراه :

1) أسماء حسن سيد محمد رويعي, الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه, كلية الحقوق, جامعة القاهرة، 2013م
2) دانا على صالح، المتغيرات المؤثرة في التعاون الدولي بعد الحرب الباردة "دراسة في تأثير ثورة الاتصالات"،رسالة دكتوراه، كلية القانون والسياسة بجامعة السليمانية، جامعة بغداد، 1432هـ
3) سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية ، رسالة دكتوراه،كلية الحقوق، جامعة عين شمس، 1997م
4) على فاروق على ،التعاون الدولي في مجال مكافحة غسل الأموال المتحصلة من الجريمة المنظَّمة وجرائم المخدرات في ضوء القانون الدولي العام ،رسالة دكتوراه مقدمة إلى كلية الحقوق بجامعة القاهرة ، بدون سنة نشر
5) عمار تيسير بجبوج، التعاون الدولي في مكافحة الإرهاب، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة ،سنة 2011م
6) نزيه محمد على عبد الغنى، وسائل الوقاية والتدابير الواجبة الإتباع في اتفاقية الامم المتحدة لمكافحة الفساد لعام 2003 ، رسالة دكتوراه ، كلية الحقوق ،جامعة بني سويف ،سنة 1437ه – 2016م

3-المجلات العلمية :

1. سامي حمدان الرواشدة، أحمد موسى الهياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلةالأردنيةفيالقانونوالعلومالسياسية– الأردن، المجلد الاول، العدد 3 ، تشرينالأولشوال سنة 2009
2. شيخهحسينالزهراني،التعاونالدوليفيمواجهةالهجومالسيبراني، مجلةجامعةالشارقةللعلومالقانونيةالمجلد

17العددالاول، يونيو2020م
3. شيرين دبابنة، الجرائم الإلكترونية القرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، المعهد العربي للدراسات المالية والمصرفية، الأردن، مجلد 23، العدد 1،سنة 2015
4. صورية بوربابة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، المركز الديمقراطي العربي، برلين، المانيا، العدد الاول ،سنة 2019
5. عبيد صالح حسن ،سياسة المشرع الإماراتي لمواجهة الجرائم الالكترونية ،بحث منشور في مجلة الفكر الشرطي ،الإمارات العربية المتحدة، المجلد الرابع والعشرين، العدد 95، أكتوبر 2015
6. ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية: الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وأبحاث، جامعة الجلفة، الجزائر، العدد الأول ،سنة 2009
7. مجدي حماد، المنظمات الإقليمية ومسألة الوحدة ، مركز دراسات الوحدة العربية ،لبنان، المجلد 11، العدد 121، مارس 1989م

4-الدراسات وأوراق العمل:

1- الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، توصيات سياساتية، الاسكوا، اللجنة الاقتصادية والاجتماعية لغربي آسيا، الامم المتحدة، نيويورك، 9 فبراير2015
2- مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، ٢٧ آب/أغسطس– ٧ أيلول/سبتمبر ١٩٩٠: تقرير أعدته الأمانة العامة، منشورات الأمم المتحدة.

5- المؤتمرات :

1. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني "دراسة مقارنة"، بحوث مؤتمر الاعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة ،في الفترة من 9-11 ربيع الأول 1424 هـ،الموافق 10-12 مايو 2013 م
2. محمد الامين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى المؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون ،الإمارات العربية المتحدة الفترة من 1-3 مايو سنة 2000

6-المراجع الإلكترونية :

- موقع منظمة الأمم المتحدة على العنوان الإلكتروني التالي:
  http://www.un.org/Depts/dhl/dhlara/events/south/index.html
- قرار الجمعية العامة للأمم المتحدة رقم **63/55**
  http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/55-63%20French.pdf
- قرار الجمعية العامة للأمم المتحدة رقم **A/RES/55/63**
  https://undocs.org/pdf?symbol=ar/A/RES/55/63
- قرار الجمعية العامة للأمم المتحدة رقم **A/RES/60/177**
  https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2005/General_Assembly/A-RES-60-177.pdf
- قرار الجمعية العامة للأمم المتحدة رقم **A / RES/64/211**
  https://undocs.org/ar/A/RES/64/211
- قرار الجمعية العامة للأمم المتحدة رقم**A / RES/73/266**
  https://undocs.org/ar/A/RES/73/266
- قرار الجمعية العامة للأمم المتحدة رقم **A / RES/74/247**
  https://undocs.org/ar/A/RES/74/247
- اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية على الرابط التالي
  https://rm.coe.int/budapest-convention-in-arabic/1680739173

II. References English:

I- Books:

1. Daniel Suter,EUROMED JUSTICE Legal and Gaps Analysis Cybercrime, CrimEx, UK, November 2017

2. Goans(J.),"Intellectual Property Principles and Practice", Nathan Associates Inc., 2014
3. Huet. A/Koering –Joulin.R: Droit Pénal International, presses Universitaires De France, ler Edition Paris, Juin 1994.
4. Nunziato(D.),Virtualfreedom ,Net Neutrality and Free Speech in the Internet Age, Stanford, California,U.S,A,2009

II- Articles and Researches:

1) Christina Schulman, Specific Crimes: Offences Related to Child Pornography and Those Related to Infringements of Copyright and Related Rights: Definition and Forms Programme on "Strengthening the Rule of Law in the Arab States –Project on the Modernization of Public Prosecution Offices", Regional Conference Booklet on "CyberCrime", Kingdom of Morocco, 19-20 June, 2007
2) Henrotte, (Jean.), L'importance de la collaboration internationale et l'expérience belge dans l'échange d'informations policières et de coopération judiciaire, Programme on "Strengthening the Rule of Law in the Arab States –Project on the Modernization of Public Prosecution Offices", Regional Conference Booklet on "CyberCrime", Kingdom of Morocco, 19-20 June, 2007
3) Manuel pour la cooperation internationale en matière pénale contre le terrorisme, OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME Vienne, Nations UNIES, New York, 2009
4) Matthew Levitt and Michael Jacobson, The Money Trail:Finding, Following, and Freezing Terrorist Finances, the Washington Institute for Near East Policy, United States of America , November 2008
5) Russell,(T.), Cybercrime: The Challenge for Law Enforcement ,Programme on "Strengthening the Rule of Law in the Arab States –Project on the Modernization of Public Prosecution Offices", Regional Conference Booklet on "CyberCrime", Kingdom of Morocco, 19-20 June, 2007.

III-Web sites:

- KALINA(L.),lutte contre la cybercriminalité, vers la construction d'un modèle juridique normalize

http://www.adie.sn

- Schjolberg,(S.),The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva, December, 2008

https://www.cybercrimelaw.net/documents/cybercrime_history.pdf

الحواشي

1)يُقصد"بجرائم الإنترنت**cyber crime**"استخداماالإنترنتإماكوسيلةلارتكابجريمةجنائيةأوكأداة للجريمة
Russell,(T.), Cybercrime: The Challenge for Law Enforcement ,Programme on "Strengthening the Rule of Law in the Arab States –Project on the Modernization of Public Prosecution Offices", Regional Conference Booklet on "CyberCrime", Kingdom of Morocco, 19-20 June, 2007,P.73.

2)العقيد الدكتور، عبيد صالح حسن ،سياسة المشرع الإماراتي لمواجهة الجرائم الالكترونية ،بحث منشور في مجلة الفكر الشرطي ،الإمارات العربية المتحدة، المجلد الرابع والعشرين، العدد 95،أكتوبر 2015 ـ ص30 اشار اليه:

د.عمادمجديعبدالملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية،الإسكندرية،سنة 2011،ص 31 .

3)راجع في ذلك

Schjolberg,(S.),The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva, December, 2008,P.1.

https://www.cybercrimelaw.net/documents/cybercrime_history.pdf

4)د. أسماء حسن سيد محمد رويعى, الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه, كلية الحقوق, جامعة القاهرة، 2013م، ص 10 اشار اليه د. نائلة عادل محمد فريد قورة،جرائم الحاسب الاقتصادية،رسالة دكتوراه،كلية الحقوق، جامعة القاهرة،سنة 2003، ص 19.

5)د. شيرين دبابنة، الجرائم الإلكترونية القرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، المعهد العربي للدراسات المالية والمصرفية، الأردن، مجلد 23 ،العدد 1،سنة 2015،ص 19 .

6)د. محمد محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، بدون دار نشر، طبعة 2007، ص 4-5.

7)Nunziato(D.),Virtualfreedom ,Net Neutrality and Free Speech in the Internet Age, Stanford, California,U.S,A,2009,P.23.

8)د. على فاروق على ،التعاون الدولي في مجال مكافحة غسل الأموال المتحصلة من الجريمة المنظمة وجرائم المخدرات في ضوء القانون الدولي العام ،رسالة دكتوراه مقدمة إلى كلية الحقوق بجامعة القاهرة ، بدون سنة نشر، ص186.

9)د. نزيه محمد على عبد الغنى، وسائل الوقاية والتدابير الواجبة الإتباع في اتفاقية الامم المتحدة لمكافحة الفساد لعام 2003، رسالة دكتوراه مقدمة إلى كلية الحقوق ،جامعة بني سويف،سنة 1437ه – 2016م، ص243-244.

10)تيري ناردين،النظرية السياسية الدولية، بحث منشور في كتاب نظريات العلاقات الدولية، ترجمة محمد صفار ،سلسلة العلوم الاجتماعية للباحثين، المركز القومي للترجمة، القاهرة، العدد 2022،الطبعة الأولى، سنة 2014، ص 441.

11)د. عادل يحيى، الأحكام العامة للتعاون الدولي في مكافحة الجريمة،دار النهضة العربية ،القاهرة، الطبعة الأولى، 2013، ص18، د . عمار تيسير بجبوج،التعاون الدولي في مكافحة الإرهاب، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة ،سنة 2011م،ص2.

12)القاضي الدكتور. عادل محمد السيوي، التعاون الدولي في مكافحة جريمتي غسل الأموال وتمويل الإرهاب ، نهضة مصر للطباعة والنشر والتوزيع ،الطبعة الاولي ،يوليو 2010، ص16.

13)تحث الجمعية العامة جميع لجان ووكالاتومنظمات الأمم المتحدةوالمؤسسات المتعددة الأطراف ذات الصلة على أن تكثف جهودها من أجل أن تعمم بشكل فعال استخدام التعاون بين بلدان الجنوب في تصميم برامجها العادية وصياغتها وتنفيذها، وأن تنظر في زيادة المخصصات من الموارد البشرية والتقنية والمالية لدعم مبادرات التعاون فيما بين بلدان الجنوب، وقررت الجمعية العامة، وبموجب القرار (58/220) بتاريخ (23 كانون الأول/ديسمبر 2003)، أن تعلن يوم (19كانون الأول/ديسمبر) "يوم الأمم المتحدة للتعاون بين بلدان الجنوب"؛ وهو التاريخ الذي أقرت فيه الجمعية العامة "خطة عمل بوينس أيريس لتشجيع التعاون التقني وتنفيذه فيما بين البلدان النامية. يراجع:
موقع منظمة الأمم المتحدة على العنوان الإلكتروني التالي:

http://www.un.org/Depts/dhl/dhlara/events/south/index.html

وهناك العديد من الأجهزة التي تحث على التعاون الدولي ومن قبيل ذلك 1-المجموعة الاستشارية لمنع الجريمة ومعاملة المجرمين. 2-صندوق تمويل الدفاع الاجتماعي. 3-قسم العدالة الاجتماعية ومنع الجريمة
4-لجنة منع الجريمة والعدالة الجنائية . 5-مركز منع الإرهاب .

14)مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، ٢٧ آب/أغسطس– ٧ أيلول/سبتمبر ١٩٩٠:تقرير أعدته الأمانة العامة، منشورات الأمم المتحدة،

15)راجع في ذلك :

KALINA(L),lutte contre la cybercriminalité, vers la construction d'un modèle juridique normalize **http://www.adie.sn**

16)حقوق الملكية الفكرية كانت محل اهتمام منذ القرن التاسع عشر حيث صدرت العديد من الاتفاقيات الدولية ومنها، اتفاقية باريس لحماية الملكية الصناعية 1883، ثم اتفاقية برن لحماية المصنفات الأدبيَّة عام 1886، ثم صدرت بعد ذلك اتفاقية روما عام 1961 لحماية الأداء والإنتاج والفني، ثم اتفاقية واشنطن 1989 لحماية الدوائر المتكاملة.

Goans(J.),"Intellectual Property Principles and Practice", Nathan Associates Inc., 2014.,p.24.

17)راجع: د. ليندةشرابشة،السياسةالدوليةوالإقليميةفيمجالمكافحةالجريمةالالكترونية :الاتجاهاتالدوليةفيمكافحةالجريمةالالكترونية، مجلةدراساتوأبحاث،جامعةالجلفة،الجزائر، العدد الأول ،سنة 2009، ص 246.

18)للاطلاع تفصيليا على ذات القرار :
http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/55-63%20French.pdf

19)القرار **A/RES/55/63**
https://undocs.org/pdf?symbol=ar/A/RES/55/63

20)القرار **A/RES/60/177**
https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2005/General_Assembly/A-RES-60-177.pdf

21)القرار **A / RES/64/211**
https://undocs.org/ar/A/RES/64/211

22)القرار **A / RES/73/266**
https://undocs.org/ar/A/RES/73/266

23)القرار **A / RES/74/247**
https://undocs.org/ar/A/RES/74/247

24)راجع في ذلك:
Daniel Suter(D.),EUROMED JUSTICE Legal and Gaps Analysis Cybercrime, CrimEx, UK, November 2017,p.17.

25) د. نزيه محمد على عبد الغنى، المرجع السابق، ص 292-293.

26)د. دانا على صالح،المتغيرات المؤثرة في التعاون الدولي بعد الحرب الباردة "دراسة في تأثير ثورة الاتصالات"،رسالة دكتوراه، كلية القانون والسياسة بجامعة السليمانية، جامعة بغداد، 1432هـ ،ص58.

27)د. نزيه محمد على عبد الغنى، المرجع السابق، ص 276.

28)Daniel Suter,OP.CIT,p.18.

Explanatory Report of the Convention on Cybercrime (185), No. 10

29)Christina Schulman, Specific Crimes: Offences Related to Child Pornography and Those Related to Infringements of Copyright and Related Rights: Definition and Forms Programme on "Strengthening the Rule of Law in the Arab States –Project on the Modernization of Public Prosecution Offices", Regional Conference Booklet on "CyberCrime", Kingdom of Morocco, 19-20 June, 2007,P.35.

30)راجع نص الاتفاقية تفصيلا على الرابط التالي
https://rm.coe.int/budapest-convention-in-arabic/1680739173

31)د. مجديحماد،المنظمات الإقليمية ومسألة الوحدة ، مركز دراسات الوحدة العربية ،لبنان، المجلد 11، العدد 121، مارس 1989م، ص 109.

32)ابرمت تلك الاتفاقية في مدينة القاهرة في جمهورية مصر العربية في 15 /1 /1432هـ، الموافق 12/21 /2010م،وانضمت مصر إلى الاتفاقية بموجب قرار رئيس الجمهورية الذى نشر في الجريدة الرسمية في العدد ٤٦ الصادر في ١٣ نوفمبر ٢٠١٤م

33)المادة الاولى من الاتفاقية .

34)المادة الثالثة من الاتفاقية .

35)اعتمده مجلس وزراء العدل العربيقرار رقم 771/د24 – 2008/11/27

36)اعتمد بموجب قرار مجلس وزراء العدل العربيرقم 812/د25 تاريخ 2009/11/19

37)Huet. A/Koering –Joulin.R: Droit Pénal International, presses Universitaires De France, ler Edition Paris,Juin 1994, P. 356.

38)راجع في ذلك : النظام الأساسي للمحكمة الجنائية الدولية المادة 102 تنص على
:**For the purposes of this Statute**

(a) "Surrender" means the delivering up of a person by a State to the Court,pursuant to this Statute.

(b) "Extradition"means the delivering up of a person by one State to another as provided by treaty, convention or national legislation.

39)أ. بوخافة سعاد، مبدأ التسليم والمحاكمة على ضوء أعمال لجنة القانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة بنعكنون، الجزائر،2014،ص 71ومابعدها

40)د. صورية بوربابة، التعاون الدولي في مكافحة الجرائم المعلوماتية،مجلة القانون الدولي للدراسات البحثية، المركز الديمقراطي العربي، برلين، المانيا، العدد الاول ،سنة 2019 ،ص 97-98.

41) د. شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية المجلد 17العدد الاول، يونيو2020م ، ص 749

42)د . عادل يحيى، المرجع السابق ،ص55.

43)د. علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، رؤية لاستراتيجية وطنية للتعاون الدولي في مجال مكافحة المخدّرات،القاهرة ،طبعة 2000، ص110.

44)د. شيخه حسين الزهراني، المرجع السابق، ص 748.

45)Daniel Suter,OP.CIT,p.17.

46)راجع تفصيليا :

Henrotte, (Jean.), L'importance de la collaboration internationale et l'expérience belge dans l'échange d'informations policières et de coopération judiciaire, Programme on "Strengthening the Rule of Law in the Arab States –Project on the Modernization of Public Prosecution Offices", Regional Conference Booklet on "CyberCrime", Kingdom of Morocco, 19-20 June, 2007,P.87.

47) د.سالم محمد سليمان الأوجلي : أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية ، رسالة دكتوراه،كلية الحقوق، جامعة عين شمس، 1997م ص 425.

48)Manuel pour la cooperation internationale en matière pénale contre le terrorisme, OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME Vienne, Nations UNIES, New York,(2009)., P.138.

49)د. عمار تيسير بجبوج، المرجع السابق،ص 387.

50)د. فائزة يونس الباشا، الجريمة المنظّمة في ظل الاتفاقيات الدولية والقوانين الوطنية، دار النهضة العربية ، ط1 ،سنة 2001، ص221.

51)اتفاقية الإعلانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين بين حكومة المملكة المغربية وحكومة المملكة الليبيةالمتحدة، الموقعة في ديسمبر ١٩٦٢م.

52) د. صورية بوربابة، المرجع السابق، ص 97.

53)د. محمد الامين البشري، التحقيق في جرائم الحاسب الآلي ،بحث مقدم إلى المؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون ،الإمارات العربية المتحدة الفترة من 1-3 مايو سنة 2000، ص 78.

54)د.سالم محمد سليمان الأوجلي، المرجع السابق، ص٤٢٧.

55)راجع في ذلك معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية التي اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/118 بتاريخ 1990/12/14، والمادة 21 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م ، وأيضا المادة 16 من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م.

56)George Ritzer,OP.CIT,p.286.

57)د. سامي حمدان الرواشدة ، د. أحمد موسى الهياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم السياسية – الأردن، المجلد الاول، العدد 3، تشرين الأول، شوال سنة 2009،ص 119.

58)Henrotte, (Jean.),OP.CIT,,P.86.

59)راجع في ذلك

Stein Schjolberg,OP.CIT,P.2.

60)الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، توصيات سياساتية، الاسكوا، اللجنة الاقتصادية والاجتماعية لغربي آسيا، الامم المتحدة، نيويورك، 9 فبراير2015، ص 26.
61)د. نزيه محمد على عبد الغنى، المرجع السابق، ص 273.
62)د.علاء الدين شحاته، المرجع السابق، ص 103.
63)د. نزيه محمد على عبد الغنى، المرجع السابق، ص 273.
64)Stein Schjolberg,OP.CIT,P.1.
65)الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية ،المرجع السابق، ص 15.
66)د. لينذا بن طالب، غسل الأموال وعلاقته بمكافحة الإرهاب، "دراسة مقارنة"، دار الجامعة الجديدة، الإسكندرية، طبعة 2011، ص 179.
67) ينظر الفقرة (18) من قرار مجلس الأمن، الوثيقة **S/RES/2462 (2019)**
68)د. عبد الفتاح بيومي حجازي،المرجع السابق ، ص79.
69)منشور في الجريدة الرسمية، العدد 32 مكرر (ج) في 14 أغسطس 2018
70)نصت تلك المادة على انه يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين الف جنية ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه....."
71)تنص المادة (٢٢)من قانون الجزاء العماني على أن " تنقسم الجرائم إلى ثلاثة أنواع : الجنايات والجنح والمخالفات ويحدد نوع الجريمة بمقتضى الحد الأقصى للعقوبة المقررة لها في القانون . وإذا كانت الجريمة معاقبا عليها بالسجن والغرامة، فيتحدد نوعها بحسب عقوبة السجن" .
في حين أن الجنحة نصت عليها المادة (٢٥) من قانون الجزاء العماني بالنص على أن الجنح هي الجرائم المعاقب عليها بالسجن مدة لا تقل عن (10) عشرة أيام، ولا تزيد على (٣) ثلاث سنوات، وبالغرامة التي لا تقل عن (100) مائة ريال عماني، ولا تزيد على (1000) ألف ريال عماني، أو بإحدى هاتين العقوبتين.
72)ينص المشرع العماني في المادة 3 من قانون جرائم تقنية المعلومات على أنه" يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك....."
73)تنص المادة 29 من قانون العقوبات الاتحادي الاماراتي لسنة 1987 على أن "الجنحة هي الجريمة المعاقب عليها بعقوبة أو أكثر من العقوبات الآتية: 1-الحبس. 2-الغرامة التي تزيد على ألف درهم.3-الدية.4-الجلد في حدي الشرب والقذف.
74)راجع الفقرة الأولى من المادة الثانية من القانون الإماراتي الاتحادي رقم (12) لسنة 2016في شأن مكافحة جرائم تقنية المعلومات.
75)د. أشرف توفيق شمس الدين،الحماية الجنائية للمستند الإلكتروني "دراسة مقارنة "،بحوث مؤتمر الاعمال المصرفية الإلكترونية بين الشريعة والقانون،كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة ،في الفترة من 9-11 ربيع الأول 1424 هـ، الموافق 10-12 مايو 2013 م، ص543.
76)تنص المادة سالفة الذكر بقولها "يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لاتقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها، أو الحد من كفاءة عملها، أو التشويش عليها، أو إعاقتها، أو اعتراض عملها، أو أجرى بدون وجه حق معالجة الكترونية للبيانات الخاصة بها....."
77) راجع المـــادة التاسعة من قانون جرائم تقنية المعلومات العماني .
78)انظر: المادة العاشرة من قانون مكافحة جرائم تقنية المعلومات الإماراتي
79)د.عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، الطبعة الثانية، سنة 1995، ص 79.
80)د.عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، سنة 2004، ص 154.
81)عرفت السلطة المصرفيّة الأوروبيّة العملة الافتراضية ؛ بأنها هي تمثيل رقمي لقيمة يمكن تحويلها أو تخزينها أو تداولها إلكترونيّاً لاتصدرعن البنك المركزي أو السلطات العامة وليست بالضرورة متعلّقة بعملة ورقيّة سواء (الدولار،اليورو)، ويقبل الأشخاص العاديّون والأشخاص القانونيّون بها كوسيلة للدفع ويمكن تحويلها أوتخزينها

أوتداولها إلكترونيّاً
EBA Opinion on "Virtual Currencies, July 4, 2014.

82)د. عبد الفتاح بيومي حجازي،جريمة غسل الأموال عبر شبكة الإنترنت، دار النهضة العربية،القاهرة ،الطبعة الاولى،سنة 2009، ص4.

83)تشير التقارير الى وجود مؤشرات لاستخدام نظام **M-payment**، وبعض الخدمات المتعلقة بالهواتف المحمولة ليتم عن طريقها نقل الأموال الكترونيا، وهذه العمليات تزداد في الدول التي لا يوجد فيها نظام مالي وحازم، وبصفة خاصة في مجال استخدام الهواتف الجوالة التي تستخدم في تحويل الأموال .
انظر التقرير التالي:
Matthew Levitt and Michael Jacobson, The Money Trail:Finding, Following, and Freezing Terrorist Finances, the Washington Institute for Near East Policy, United States of America , November 2008,P.21.

84)تطرقت المادة الثالثة من قانون مكافحة الإرهاب المصري، على بيان مفهوم جريمة التمويل بأنه "يقصد بتمويل الإرهاب كل جمع أو تلق أو حيازة أو إمداد أو نقل أو توفير أموال أو أصول أخرى أو أسلحة أو ذخائر أو مفرقعات أو مهمات أو آلات أو بيانات أو معلومات أو مواد أو غيرها لأي نشاط إرهابي فردي أو جماعي منظم أو غير منظم في الداخل أو الخارج, بشكل مباشر أو غير مباشر, أيا كان مصدره وبأي وسيلة كانت بما فيها الشكل الرقمي أو الإلكتروني, وذلك بقصد استخدامها كلها أو بعضها في ارتكاب جريمة إرهابية أو العلم باستخدامها, سواء وقع الفعل الإرهابي أم لم يقع, أو بتوفير مكان للتدريب أو ملاذ آمن لإرهابي أو أكثر أو تزويده بأسلحة أو مستندات أو غيرها, أو بأي وسيلة مساعدة أخرى من وسائل الدعم أو التمويل أو السفر مع العلم بذلك ولو لم يكن لها صلة مباشرة بالعمل الإرهابي.
النص الساري للمادة منذ صدور القانون 15 لسنة 2020

85)راجع المادة الاولى/(أ)من قانون رقم ١٧ لسنة ٢٠٢٠ بتعديل بعض أحكام قانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢.

86)أحدث تعديل بالقانون رقم 15 لسنة 2020 بتاريخ 3 مارس 2020بموجب رار رئيس جمهورية مصر العربية بالقانون رقم 94 لسنة 2015 بإصدار قانون مكافحة الإرهاب.

87) الفقرة الثالثة من المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات المصري.

88)أحدث تعديل بالقانون رقم 15 لسنة 2020 بتاريخ 3 مارس 2020.

89)ينص قانون الجزاء العماني على أن "الجنايات هي الجرائم المعاقب عليها بالإعدام أو السجن المطلق أو السجن المؤقت من (٣) ثلاث سنوات إلى (15) خمس عشرة سنة."

90)تنص المادة المذكورة على انه" يعاقب بالسجن المطلق وبغرامة لا تقل عن مائة ألف ريال عماني ولا تزيد على مائتي ألف ريال عماني، كل من أنشأ موقعا إلكترونيا على الشبكة المعلوماتية لتنظيم إرهابي أو استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات لأغراض إرهابية أو في نشر أفكار ومبادئ تنظيم إرهابي والدعوة لها أو في تمويل العمليات الإرهابية والتدريب عليها أو في تسهيل الاتصالات بين تنظيمات إرهابية أو بين أعضائها وقياداتها أو في نشر طرق صناعة المتفجرات والأسلحة والأدوات التي تستخدم خاصة في عمليات إرهابية.

91)ينص المشرع العماني على انه" يعاقب بالسجن المؤقت مدة لا تقل عن ثلاث سنوات ولا تزيد على خمس عشرة سنة وبغرامة لا تقل عن خمسين ألف ريال عماني ولا تزيد على ما يعادل قيمة الأموال محل الجريمة إذا كانت أكبر من ذلك، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في تحويل الأموال غير المشروعة أو نقلها أو إخفاء أو تمويه مصدرها أو في اكتساب أو حيازة الأموال أو الممتلكات مع علمه بأنها مستمدة من مصدر غير مشروع أو في طلب المساعدة في عملية غسل أموال أو في نشر طرق القيام بذلك".