



المحاضرة العاشرة

المسئولية الجنائية للوسطاء والتعاون الدولي والشرعية الإسلامية في الجرائم السيبرانية

تمهيد وتقسيم:

من الناحية التقنية، لا يمكن الوصول إلى الإنترنت دون خدمات من أحد وسطاء خدمة الإنترنت، وبالتالي فإن دور مقدمي خدمات الإنترنت محوري، وفي نطاق المسئولية الجنائية، تثار إشكالية مقدمي خدمات الإنترنت، سواء كان شخص طبيعة أو اعتباري، وذلك لأن المعلومات والبيانات وسائر العمليات التي تنساب عبر شبكة الانترنت تمر ما بين إنتاجها ووصولها إلى المستخدم النهائي بعدة ادوار لان تشغيل الشبكة يقتضي تضافر جهود عدة أشخاص تتنوع أدوارهم في النشاط الإلكتروني يتولون تقديم الخدمات الوسيطة في الشبكة بدءاً من مورد منافذ الدخول إلى الانترنت، ومروراً بمقدم خدمات الاستضافة على الانترنت وكذلك مقدم خدمات سحابة الكمبيوتر، ويتميز دورهم بأنه دور تقني بحت من خلاله يتمكن المستخدم من الاتصال بالموقع الإلكتروني المراد الدخول إليه والحصول على المعلومات المنشورة فيه، ولهذا الدور الفني أهمية في تحديد مسئولية وسطاء مقدمي الخدمات المعلوماتية عبر شبكة الإنترنت، ويعتبر من أهم المصادر الرئيسية التي يستمد منه عناصر المسئولية الجنائية هو أجهزة ومعدات مقدمي الخدمات المعلوماتية عبر الإنترنت.

ويثور التساؤل معانا في المحاضرة عن موقف الشريعة الإسلامية في مواجهة الجرائم السيبرانية، ودور التعاون الدولي في مواجهة الجريمة السيبرانية.

ولذلك سوف نقسم المحاضرة علي ثلاثة محاور رئيسية علي النحو التالي:

المحور الأول : المسئولية الجنائية للوسطاء في خدمات الإنترنت :

المحور الثاني: الشريعة الإسلامية والتعاون الدولي في مواجهة الجرائم السيبرانية:

• عناصر المحاضرة:

المحور الأول: المسؤولية الجنائية للوسطاء في خدمات الإنترنت :

أولاً: تعريف وسطاء الانترنت:

ثانياً: أنواع وسطاء الإنترنت حسب التصنيف الوظيفي:

ثالثاً: حالات اعفاء وسطاء الإنترنت من المسؤولية:

رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:

١. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية.

٢. المسؤولية الجنائية لمقدم خدمة الاستضافة.

٣. المسؤولية الجنائية لمقدم خدمة الاتصال بالإنترنت.

المحور الثاني: الشريعة الإسلامية والتعاون الدولي في مواجهة الجرائم السيبرانية:

أولاً : موقف الشريعة الإسلامية في مواجهة الجرائم السيبرانية:

ثانياً : أهمية التعاون الدولي لمكافحة الجرائم السيبرانية:

ثالثاً: أنواع التعاون الدولي:

١. التعاون الدولي غير الرسمي:

٢. التعاون الدولي الرسمي:

رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:

١. وثائق الجمعية العامة للأمم المتحدة بشأن الجرائم السيبرانية:

٢. قرارات المجلس الاقتصادي والاجتماعي:

٣. مؤتمر الأمم المتحدة الثامن لمنع الجريمة معاملة السجناء ... هافانا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر:

٤. إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية :

خامساً : الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية:

١. معاهدة بودابست لمكافحة جرائم الإنترنت :

٢. توصيات المجلس الأوروبي :

سادساً : جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية:

١. الاتحاد الدولي للاتصالات :

٢. المنظمة العالمية للملكية الفكرية :

٣. منظمة حلف شمال الأطلسي:

المحور الأول

المسؤولية الجنائية للوسطاء في خدمات الإنترنت

وينحصر دور وسطاء خدمة الإنترنت في تمكين المستخدم من الدخول على شبكة الإنترنت والتجول والإبحار فيها والاطلاع على ما يريد، فمنهم من ينقل الخدمة للمستخدم ومنهم من يمكن المستخدم من الوصول إلى الموقع، ومنهم من يقوم بتخزين المعلومات أو إنتاجها أو توزيعها.

وسوف نتناول في هذا المجال تعريف وسطاء الإنترنت وأنواعهم والمسؤولية الجنائية القانونية الواقعة عليهم، وذلك على النحو التالي:

أولاً: تعريف وسطاء الإنترنت:

يعرف بعض الفقه وسيط الإنترنت بأنه هو " أي شخص يوفر الوصول إلى خدمة المعلومات في شكل الكتروني". كما عرف جانب آخر من الفقه وسيط الإنترنت بأنه " هو مزود خدمات عبر شبكة الإنترنت". كذلك أشار البعض إلى أن وسطاء الإنترنت هم "هي الكيانات التي توفر للمشاركين الأفراد والمؤسسات إمكانية الوصول إلى الإنترنت".

ثانياً: أنواع وسطاء الإنترنت حسب التصنيف الوظيفي:

يشير مصطلح وسطاء "الإنترنت" بشكل عام، إلى مجموعة واسعة ومتنوعة وسريعة التطور من مقدمي الخدمات الذين يسهلون التفاعلات على الإنترنت بين الأشخاص الطبيعيين والاعتباريين ، ولكن يمكن إن ندرج وسطاء الإنترنت في فئتين واسعتين:

الفئة الأولى : وتسمى فئة القنوات، وهي مقدمي الخدمات التقنية للوصول إلى الإنترنت أو خدمات الإرسال ولا تتداخل القنوات مع المحتوى الذي تنقله، فكل ما تقوم به هذه الفئة هو التخزين التلقائي أو اللازم لنقل المحتوى.

والفئة الثانية: المضيفون Hosts، وهم مقدمو خدمات المحتوى وتمكين معالجة البيانات واستضافة الخدمات المستندة إلى الويب، بما في ذلك التحليلات التي ينشئها المستخدمون، على سبيل المثال، المنصات عبر الإنترنت وخدمات التخزين.

ويقوم المضيفون أيضا بتعديل المحتوى وترتيبه، وذلك بشكل أساسي من خلال المعالجة الإلكترونية، أو جمع المعلومات، أو المساعدة في عمليات البحث، أو تسهيل بيع السلع والخدمات، أو تمكين المعاملات التجارية الأخرى وقد يؤدون وظائف أخرى تشبه وظائف الناشرين.

ومن الأمثلة على وسطاء الإنترنت ما يلي:

١. موفرو البنية التحتية للشبكة Network infrastructure providers الذين يقومون بإنشاء وصيانة شبكات لمشغلي الشبكات مثل شركات Ericsson Huawei Cisco.

٢. متعهد خدمات الوصول لشبكة الإنترنت Internet access providers (IAPs) هم الشركات التي توفر الوصول إلى الإنترنت مثل شركة كومكاست Comcast في الولايات المتحدة، وشركة فرانس تليكوم France telecom في فرنسا، وشركة MWeb في جنوب أفريقيا، وكذلك، على نطاق أصغر، مقاهي الإنترنت ومقدمي نقاط اتصال Wi-Fi

ويشترط في متعهد الوصول والنفاز للإنترنت إن يتوافر فيه ثلاثة شروط: الأول: يربط كمبيوتر المستخدم النهائي بالإنترنت باستخدام الكابلات أو التكنولوجيا اللاسلكية، أو ييسر أيضا المعدات اللازمة للوصول إلى الإنترنت، والثاني: أن يكون هو الذي يقوم بالوصول إلى الإنترنت، والثالث: أن يقوم بخدمة الإنترنت.

٣. مقدمو خدمات الإنترنت (ISP) Internet service providers: يعتبر من أهم الشركات التي تقدم خدمات الإنترنت، ومنهم على سبيل المثال، مقدمي خدمات البريد الإلكتروني، كما أن العديد من مشغلي الشبكات هم أيضا من شركات خدمات الإنترنت.

٤. مقدمو خدمات الاستضافة Hosting providers: هي الشركات التي تقدم خدمات الاستضافة والتخزين عبر الإنترنت، يقدم مزود الاستضافة تقنيات لعرض المحتوى على الويب، الإرسال واستقبال وإدارة رسائل البريد الإلكتروني وتخزين الملفات، وما إلى ذلك، حيث يكون لديها العديد من أجهزة الكمبيوتر والخوادم مزودة بمساحة متاحة للإيجار.

ويمكن التمييز بين التخزين المؤقت، حيث يكون الغرض من الاستضافة هو تيسير عمل الشبكة من خلال التخزين التلقائي والمتوسط والعابر للمعلومات، واستضافة التخزين التجاري أو التخزين الآخر الدائم أو أكثر من مجرد تخزين مؤقت.

٥. ناقل المعلومات transit provider : هو الذي يسمح بالتفاعل بين الكمبيوتر ومتعهد خدمات الوصول للإنترنت، ومقدمي خدمات الاستضافة ووظيفته هي مجرد نقل البيانات، أي يعتبر مجرد قناة لعبور المعلومات.

٦. الشبكات الاجتماعية Social networks : يدخل ضمن شبكات التواصل الاجتماعي فيس بوك Facebook ، وتويتر Twitter ولينكد إن LinkedIn وجوجل بلس Google Plus ومنصات المحتوى Content platforms الذي ينشئه المستخدم مثل منصات التدوين ومواقع مشاركة الفيديو ومواقع مشاركة الصور .

ثالثا: حالات اءفاء وسطاء الإنترنت من المسؤولية:

عندما بدأت شركات الإنترنت في تقديم خدمات الإنترنت في الثمانينيات من القرن المنصرم، كان هناك بالفعل نقاش فقهي بشأن موقف وسطاء الإنترنت، في البداية، غالبًا ما كان يُنظر إلى المزود على أنه المكافئ الرقمي digital equivalent لشركة بريدية، لم يكن لديها معرفة أو سيطرة على المحتوى الذي تم تسليمه من قبلها، وبالتالي لا يمكن من حيث المبدأ، أن تتحمل المسؤولية من أي محتوى غير قانوني وغير مشروع .

والأصل أنه تقوم مسؤولية وسطاء خدمات الإنترنت، بالإضافة إلى القواعد العامة، عند وقوع خطأ أو غلط أو تحريف في إبلاغ الرسالة الإلكترونية إلى المرسل إليه ناتج عن سبب راجع إليه أو أحد العاملين لديه، كما تقوم مسؤوليته إذا انتهك سرية المراسلات والمكاتبات والاتصالات الإلكترونية ما لم يكن تدخله تبرره الضرورة الفنية لتشغيل الشبكة.

وهناك حالات يتم فيها اءفاء مقدمي الخدمات الوسيطة للإنترنت من المسؤولية منها ما جاء في التوجيه الأوروبي للتجارة الإلكترونية لسنة ٢٠٠٠ ، وتحدد المواد أرقام ١٢ ، ١٣ ، ١٤ من التوجيه الأوروبي للتجارة الإلكترونية لسنة ٢٠٠٠ حالات مقدمي الخدمات الوسيطة للإنترنت من المسؤولية، والتي يشار إليها أيضا باسم الموانئ الأمانة Safe ports والتي تحتوي على الشروط التي بموجبها يُعفى بعض مزودي خدمات الوسطاء من المسؤولية عن المحتوى غير المشروع.

وهناك ثلاث أنواع من مقدمي الخدمات الوسيطة منحها التوجيه الأوروبي الاعفاء المشروط من المسؤولية وهم على وجه التحديد، إذا كان مقدم الخدمة:

١. ناقل للمعلومات أو مجرد قناة ناقلة للمعلومات.

٢. يقوم بالتخزين المؤقت للمحتوي.

٣. أو يقوم بالاستضافة.

وهو ما يعني أنه عندما تدرج الخدمة فقط وحصرها ضمن أحد هذه الأنشطة المحددة يمكن إعفاؤها من المسؤولية.

رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:

ويعتبر مقدم خدمة الاتصال بالإنترنت ومقدم خدمة الاستضافة ومقدم خدمة الحوسبة السحابية هم مجرد مقدمي خدمات تكنولوجيا لا علاقة لهم بالمحتوى الذي ينقل عبر شبكاتهم، فوظائفهم تتميز بأنها ذات طابع تقني بحت، وبالتالي من المفترض إن لا يسألون جنائياً عن المحتوى غير المشروع فهم مجرد ناقل للمعلومات، إلا إن العديد من التشريعات وضعتهم في إطار المسؤولية الجنائية وذلك في حالات وشروط معينة، على نحو ماسري إن شاء الله تعالى، ومن هذا المنطلق سوف نتناول المسؤولية الجنائية لمقدمي الخدمة على النحو التالي:

١. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية.

٢. المسؤولية الجنائية لمقدم خدمة الاستضافة.

٣. المسؤولية الجنائية لمقدم خدمة الاتصال بالإنترنت.

وذلك على النحو التالي:

١. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية:

أ. تعريف الحوسبة السحابية ومقدم خدمة الحوسبة السحابية:

ويمكن تعريف الحوسبة السحابية بأنها " تقنية تقوم بتحويل موارد الكمبيوتر من برمجيات وعتاد إلى خدمات على شبكة الإنترنت، وذلك عن طريق تقنية تعتمد على استبدال المعالجة ومساحة التخزين الخاصة بالكمبيوتر إلى ما يسمى بالسحابة".

ويعتبر Google Drive مثلاً للحوسبة السحابية التي بدأت في الانتشار لما تقدمه من خدمات وتطبيقات المستخدمين عبر شبكة الإنترنت.

ولذلك فإن الحوسبة السحابية هي تكنولوجيا تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالكمبيوتر إلى ما يسمى السحابة، وهي مركز بيانات يتم الوصول إليه عن طريق الشبكة، وبهذا تتحول برامج تكنولوجيا المعلومات من منتجات إلى خدمات حيث تساهم هذه التكنولوجيا في إبعاد مشاكل الصيانة وتطوير الأنظمة عن الشركات المستخدمة لها، وبالتالي يتركز مجهود الجهات المستفيدة على استخدام هذه الخدمات فقط.

ومن أهم شركات مزود و خدمة الحوسبة السحابية شركة أمازون Amazon شركة مايكروسوفت، Microsoft شركة جوجل Google.

وقد عرفت وثيقة هيئة الاتصالات وتقنية المعلومات بالسعودية المعنية بتنظيم خدمة للحوسبة السحابية مقدم خدمة بأنه "أي شخص يقدم خدمات حوسبة سحابية إلى العموم من خلال مراكز معلومات يمتلكها، ويديرها بنفسه بشكل جزئي أو كلي".

أما القانون الأمريكي بشأن سحابة الكمبيوتر Cloud Act لسنة ٢٠١٨ فلم يضع تعريفاً لمقدم الخدمة، ولكنه أشار إليه في نصوص القانون بمصطلح مقدم خدمة الحوسبة عن بعد .

ونذهب مع الرأي القائل بأننا نهيب ونأمل من المشرع المصري أن يصدر قانون خاص ينظم خدمة الحوسبة السحابية، تكون أهدافه ضمان حقوق والتزامات كل من مقدمي ومستخدمي خدمات الحرسية السحابية، من خلال وضع إطار تنظيمي لعقد الحوسبة السحابية، وكذلك وضع أسس تنظيمية واضحة لإدارة المخاطر على أمن المعلومات المحتملة المرتبطة باستخدام خدمات الحوسبة السحابية.

ب. التزامات مقدم خدمة الحوسبة السحابية:

- القانون الأمريكي:

نص القانون الأمريكي بشأن سحابة الكمبيوتر Cloud Act لسنة ٢٠١٨ على عدة التزامات تقع على عاتق مقدم خدمة الحوسبة السحابية، ونعرض لأهم هذه الالتزامات:

١- يلتزم مقدم خدمة الاتصالات الإلكترونية أو خدمة الحوسبة عن بعد بالتزامات هذا الفصل بالحفاظ على محتويات الاتصالات سلكية كانت أو إلكترونية أو عدم الكشف عنها وعن أي سجل أو معلومات أخرى تتعلق بعمل أو مشترك في حيازة هذا المزود أو تحت سيطرته، بغض النظر عما

إذا كانت هذه الاتصالات أو السجلات أو المعلومات الأخرى موجودة داخل الولايات المتحدة أو خارجها.

٢- يلتزم مقدم خدمة الحوسبة السحابية بالكشف عن البيانات والمعلومات المخزنة لديه وفي حيازته بناء على الأمر الصادر من المحكمة أو جهة التحقيق المختصة.

- القانون السعودي:

الالتزامات في القانون السعودي (وثيقة هيئة الاتصالات بالسعودية):

١. يلتزم مقدم خدمة الحوسبة السحابية أن يضمن عدم نقل أي محتوى غير مشروع مستخدم خارج المملكة، مهما كان الغرض سواء من أجل التخزين المؤقت، أو التخزين الاحتياطي، أو أي، أغراض مماثلة، وبأي صيغة كانت.

٢. يلتزم خدمة الحوسبة السحابية أن يخطر هيئة الاتصالات بالمملكة ودون تأخير غير ضروري بأي انتهاكات أمن معلومات أو تسرب بيانات المستخدمين.

٣. يلتزم مقدمي خدمة الحوسبة السحابية بحذف أي محتوى مخالف للنظام، أو يخل بحقوق الملكية الفكرية للغير، إذا أمرت هيئة الاتصالات، أو أي جهة مختصة في المملكة مقدمي الخدمة بعمل ذلك.

٤. يتعين على مقدم خدمة الحوسبة السحابية الذي يحمل ترخيص تشغيل وخدمات الحوسبة السحابية أن يفصح للهيئة عن الموقع والخصائص الرئيسية لمراكز المعلومات التابعة له الواقعة في المملكة وكذلك التي تقع خارج المملكة إذا كانت تلك المراكز مؤثرة في عملية معالجة، أو تخزين، أو عبور، أو نقل بيانات المستخدم، أو محتوى المستخدم الذي يغطيه هذا الإطار التنظيمي.

٥. يجب على مقدم خدمة الحوسبة السحابية أن يبلغ مستخدمي الخدمة التابعين له مقدماً، إذا ما كان سوف يتم نقل، أو تخزين، أو معالجة محتوى المستخدم الخاص بهم خارج المملكة بشكل دائم أو مؤقت.

٢. المسؤولية الجنائية لمقدم الخدمة أو الإستضافة:

من الجرائم السيبرانية التي من الممكن أن تقع عبر المواقع الإلكترونية جريمة وضع علامة تجارية مقلدة لعلامة تجارية مشهورة أو مشابه لها مما قد تؤدي إلى خداع أو تضليل الجمهور، وكذلك جريمة الغش التجاري عن طريق بيع بضاعة مقلدة، أو جريمة عرض أثر مهريّة للبيع عبر الموقع.

وللحصول على الأدلة الرقمية المرتبطة بمثل هذا النوع من الجرائم فإنه يتم الاستعانة بمقدم خدمة استضافة المواقع الإلكترونية، الذي غالباً ما يحتفظ بنسخة احتياطية من بيانات الموقع الإلكتروني، ولعل هذا ما يدعوننا إلى بيان مفهوم مقدم خدمة الاستضافة، ثم بيان الالتزامات القانونية الواقعة على عاتقه وذلك على النحو التالي:

أ. تعريف مقدم خدمة الاستضافة Hosted service provider:

يعرف بعض الفقه مقدم خدمة الاستضافة، أو المضيف The host، بأنه هو " كل شخص طبيعي أو معنوي يعرض استضافة صفحات الويب web على الخوادم للمملوكة له مقابل أجر ..".

وخدمة الاستضافة ، أو الإيواء ، عرفها القانون الفرنسي حول الثقة في الاقتصاد الرقمي Confiante dans l'économie numérique بأنها عبارة عن " نشاط يمارسه شخص طبيعي أو معنوي، يهدف إلى تخزين مواقع إلكترونية وصفحات ويب web pages على أجهزة الخوادم التابعة له بشكل مباشر ودائم مقابل أجر أو بالمجان، ويضع من خلالها، تحت تصرف عملائه الوسائل التقنية والمعلوماتية التي تمكنهم في أي وقت من بث ما يريدون على شبكة الإنترنت من نصوص وصور وأصوات وتنظيم المؤتمرات والحلقات النقاشية وإنشاء روابط معلوماتية مع المواقع الإلكترونية الأخرى.

ويمكن القول إن متعهد الاستضافة هو شخص طبيعي أو معنوي، يعرض استضافة صفحات الويب على أجهزة الخوادم التابعة له مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة، للمستأجر الذي ينشر عليه ما يريد من نصوص أو صور أو ينظم مؤتمرات مناقشة أو ينشئ روابط معلوماتية من المواقع الأخرى.

وهناك نوعين أساسيين من مقدمي خدمة الاستضافة، الأول مقدم خدم استضافة مواقع الويب، والثاني مقدم خدمة استضافة البريد الإلكتروني.

ب. التزامات ومسئولية مقدم خدمة الاستضافة:

وفي هذا الصدد نجد أن القضاء الفرنسي ومن بعده المشرع الفرنسي، وأسوة بالمشرع الأوروبي، وضع حداً معقولاً من الالتزامات على مقدمي خدمة الاستضافة، كالالتزام بالحِطة والحذر في متابعة محتويات المواقع الإلكترونية، والالتزام بالإعلام، والالتزام بوقف بث المضمون المعلوماتي غير المشروع.

وطبقاً لقانون الثقة حول الاقتصاد الرقمي الفرنسي رقم ٥٧٥ لسنة ٢٠٠٤ فإن المسؤولية الجنائية لمقدم خدمة الاستضافة تقوم إذا ثبت علمه الفعلي بالمضمون المعلوماتي غير المشروع، ومع ذلك لم تتخذ الاجراءات اللازمة لشطبه، أو منع وصوله للجمهور، أو في حالة إذا طلب منه شطب هذا المضمون أو منع وصول الجمهور إليه.

وكذلك الشأن بالنسبة لموقف المشرع الألماني، إذ جاء مضمون نص المادة الخامسة من قانون الاتصالات والمعلوماتية الصادر عام ١٩٩٧ على أنه تنتفي مسؤولية مقدم الخدمة الاستضافة، وفقاً من هذا القانون إذا علم بوجود المحتوى غير المشروع ولكن ألا يكون لديه بعد علمه به القدرة الفنية ليعيق الوصول إلى المحتوى غير المشروع.

٣. مقدم خدمة الإتصال بالإنترنت:

أ. تعريف مقدم خدمة الاتصال بالإنترنت:

مزود خدمة الاتصال بالإنترنت هو أي شخص طبيعي أو معنوي، يقوم بدور فني لتوصيل المستخدم إلى شبكة الإنترنت، بمقتضى عقد الشراك تضمن توصيل العميل للمواقع التي يريدها، وليس له علاقة بالمحتوى المعلوماتي.

ويستفاد من هذا التعريف إن مزود خدمة الاتصال بالإنترنت هو كل شخص طبيعي، أو معنوي، يستغل شبكات الاتصال عن بعد في سبيل إيصال عملائه بشبكة الإنترنت، وذلك بموجب عقد الدخول إلى شبكة الإنترنت، وغالباً يكون بمقابل مادي، ويحظر عليه الاطلاع على المحتوى الإلكتروني للرسائل الإلكترونية وفقاً لسرية الاتصالات عن بعد، ولكن يستثنى من ذلك الحالات التي ينص عليها القانون، ولا يجوز له أيضاً أن يباشر أية رقابة على الرسائل الإلكترونية المرسلة أو التي يتم تلقيها من قوائم البث وإلا تعرض للعقوبات المنصوص عليها في القانون.

ونظراً لارتباطه الدائم بشبكة الإنترنت ولطبيعة الخدمة التي يقدمها، يعد مزود خدمة الاتصال بالإنترنت واحداً من أهم مقدمي الخدمات في العالم الافتراضي، فنشاطه الرئيسي يتمحور في تزويد مشتركيه بالوسائل الفنية اللازمة لربطهم بشبكة الإنترنت، ولإبحارهم فيها بحري ولوصولهم إلى المواقع الإلكترونية التي يريدون الاطلاع على مضمونها.

تعددت الآراء الفقهية بشأن المسؤولية الجنائية لمقدم خدمة الاتصال بالإنترنت، ويمكن إرجاعها إلى ثلاثة آراء فقهية، فالرأي الأول يرى عدم مسؤولية مقدم خدمة الاتصال، بينما يذهب اتجاه آخر إلى قيام مسؤوليته، بينما ذهب الاتجاه الثالث إلى إن مسؤوليته تتحدد حسب طبيعة الدور الذي يقوم به.

ومن الإطلاع على السوابق القضائية للقضاء الأمريكي يتضح أنه قد ميز بين مسؤولية الموزع الذي لم يقوم إلا بتوفير خدمة الاتصال بالإنترنت للعملاء وقرر عدم مسؤوليته، وبين الناشر الذي له سيطرة أكبر على محتوى المعلومات ويقع على عاتقه مهمة مراقبة ما يقوم بتوفيره للعملاء لهذا تتقرر مسؤوليته.

المحور الثاني

الشريعة الإسلامية والتعاون الدولي في مواجهة الجرائم السيبرانية

تمهيد وتقسيم:

نعلم أن الشريعة الإسلامية لا تحارب العلم، بل تدعو إليه وتحبذه. لكننا رأينا أن هذه التقنيات العلمية التي لا ترفضها الشريعة ترتب علي استخدامها جرائم تلحق الأذى بالآخرين وتضربهم وذلك مثل: السرقة عن طريق جهاز الحاسب الآلي باستخدام بطاقات الدفع الآلي، والقذف عن طريق صفحات الإنترنت، والمهاترات الجنسية عن طريق الإنترنت. لذا كان لا بد من وقفة مع هذه الوسائل العلمية الحديثة لنرى ماذا قالت الشريعة الإسلامية في ذلك.

أما بالنسبة للتعاون الدولي فالمقصود بالتعاون لغة هو العون المتبادل، أي تبادل المساعدة لتحقيق هدف معين. وهذا هو المعنى العام لكلمة تعاون، ويفهم منه التضافر المشترك بين شخصين أو أكثر لتحقيق نفع مشترك أو خدمة مشتركة على وجه العموم.

ويمتد هذا التعاون ليشمل كافة صنوف العلاقات السياسية والعسكرية والإقتصادية والاجتماعية والأمنية وغيرها، ليعكس في النهاية بروز مصالح عالمية أو دولية مشتركة، تقوم جنباً إلى جنب مع المصالح الوطنية الذاتية لكل من الدول أطراف هذا التعاون.

والتعاون الدولي، بصفة عامة، هو مصطلح يطلق على الجهود المبذولة بين دول العالم من أجل تحقيق مصلحة الدول المتعاونة وفي سبيل تحقيق الأمن والسلم الدوليين ومواجهة التحديات السياسية والاجتماعية والاقتصادية والأمنية، كما يمكن للتعاون الدولي أن يتم على مستوى الأفراد بين الدول والمجتمعات والاعراق المختلفة إضافة إلى المنظمات الحكومية والغير حكومية بشكل عام التعاون الدولي يتم بصفة رسمية عبر الاتفاقيات والمعاهدات البيئية أو الدولية، كما يمكن أن يتجدد في المساعدات الإنسانية والتحرركات المشتركة يعد هذا المبدأ من القواعد الأساسية التي تقوم عليها منظمة الأمم المتحدة وتدعو إلى تحقيقها.

ولكل ما سبق سوف نشرح هذا المحور من المحاضرة من خلال العناصر التالية:

أولاً : موقف الشريعة الإسلامية في مواجهة الجرائم السيبرانية:

ثانياً : أهمية التعاون الدولي لمكافحة الجرائم السيبرانية:

ثالثاً: أنواع التعاون الدولي:

١. التعاون الدولي غير الرسمي:

٢. التعاون الدولي الرسمي:

رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:

١. وثائق الجمعية العامة للأمم المتحدة بشأن الجرائم السيبرانية:

٢. قرارات المجلس الاقتصادي والاجتماعي:

٣. مؤتمر الأمم المتحدة الثامن لمنع الجريمة معاملة السجناء ... هافانا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر:

٤. إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية :

خامساً : الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية:

١. معاهدة بودابست لمكافحة جرائم الإنترنت :

٢. توصيات المجلس الأوروبي :

سادساً : جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية:

١. الاتحاد الدولي للاتصالات :

٢. المنظمة العالمية للملكية الفكرية :

٣. منظمة حلف شمال الأطلسي:

أولاً : موقف الشريعة الإسلامية في مواجهة الجرائم السيبرانية:

وإذا كانت شبكة الإنترنت وأمثالها من النظم المستحدثة فإن ذلك لا يعني أن الشريعة ترفضها وتبعدها علي العكس ما دام هناك فوائد تعود علي البشرية من خلال هذه التقنية فإن الشريعة الإسلامية تدعوا إليها ذلك أن تعظيم الشريعة للعلم النافع أمر تحبذه الشريعة والنصوص في ذلك كثيرة ومشهورة سواء كانت نصوصاً قرآنية أو أحاديث نبوية وتقنية الإنترنت لها فوائد جمة وعظيمة وما دام للتقنية فائدة فإنها لا ترفض.

ولا يقال هنا إن "دفع المفساد مقدم علي جلب المصالح" هي قاعدة أصولية، فنقول نعم أن دفع المفساد مقدم علي جلب المصالح، لكن هذه التقنية فوائدها جليلة وعظيمة والمفسدة تأتي من خلال استغلال التقنية الاستغلال السيء إلا أنها نفع في ذاتها، ذلك أن لو قلنا بذلك دفع المفساد "لما أخذنا بأي تقنية علمية، لأنه ما من اكتشاف موجود إلا وله إضرار مثلما له فوائد والإضرار تأتي من خلال استعمال الفرد للتقنية استعمالاً سيئاً، لذا لزم إذا كان فعل الفرد يشكل جريمة من الجرائم فإن فعله هذا يجب أن يعاقب عليه، وأعتقد أن نظرية العقاب في الشريعة غاية في المرونة ذلك أن نظام التعزيز يصلح لكل زمان ومكان، ما لم يكن الفعل يشكل جريمة حد أو قصاص.

ثانياً : أهمية التعاون الدولي لمكافحة الجرائم السيبرانية:

تبدو أهمية التعاون الدولي في شأن مكافحة الجرائم السيبرانية من عدة نواحي نتناولها على نحو ما يلي:

١. يعتبر التعاون الدولي من التدابير المانعة للجريمة بصفة عامة، والجريمة السيبرانية بصفة خاصة، لأن المجرم سوف يجد نفسه محاطاً بسياج مانع من الإفلات من المسؤولية عن الجريمة التي ارتكبتها، أو من العقوبة التي حكم عليه بها ، فإذا ارتكب جريمته في دولة ما وتمكن من الهرب إلى دولة أخرى، فإنه سيكون عرضه للقبض عليه أو تسليمه إلى البلد الآخر، ومن شأن كل ذلك أن يجعل المجرم يعزف عن سلوك سبيل الجريمة.

٢. أثبت الواقع العملي أن الدولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة، فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم السيبرانية، التي باتت تشكل خطراً لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة.

٣. ومع تميزها بالعالمية ويكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها.

فمثلا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة، فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها.

لذا فإن التحقيقات في الجرائم المتصلة بالكمبيوتر والإنترنت وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة بين الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى آخر أنه متى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزاً.

٤. يعتمد التعاون الدولي على قدرة الدول على معالجة طلبات الأدلة الرقمية بطريقة تضمن مقبولة الأدلة في المحكمة، ولتحقيق ذلك هناك حاجة إلى متخصصين مؤهلين في الجرائم المعلوماتية لضمان الحصول على الأدلة وفقاً لقواعد الإثبات الوطنية والإجراءات الجنائية، سيما وأن أجهزة العدالة الجنائية ليست بنفس المستوى والجاهزية في جميع الدول وإنما هناك تفاوت فيما بينها فبعض الدول متقدمة تقنيا وتكنولوجيا ولها صيت كبير في مواجهة الجرائم المعلوماتية، والبعض الآخر تفتقد ذلك، من هنا كان لابد من التعاون بين الدول.

ثالثاً: أنواع التعاون الدولي:

الجريمة السيبرانية تعتبر شكلاً جديداً من أشكال الجرائم العابرة للحدود الدولية بين كافة دول العالم، ولذلك قد تكون هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة.

وتوصي دراسة الأمم المتحدة بضرورة إيجاد آليات رسمية وغير رسمية للتعاون القضائي بين الدول، إما بموجب اتفاقيات دولية أو ثنائية، أو بموجب القانون الوطني، أو وفق مبدأ المعاملة بالمثل، وذلك تفادياً للتعرض لسيادة الدول، إذ قد يكون من الضروري تمكين الدول من القيام بأعمال تحقيق في أراضي

دول أخرى، باعتبار أن العديد من الدول المستفتاه أفادت بأن أكثر من نسبة ٢١ في المائة من الجرائم المعلوماتية تتضمن عنصر دولياً.

وهناك نوعان أساسيان للتعاون المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة:

(أ) التعاون الدولي غير الرسمي :

مثل تبادل المعلومات بين أجهزة الشرطة وجهات التحقيق، فهي أسرع إنجازاً، وهي الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية - أي أوامر تفتيش أو طلب تسليم المجرم - وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الاتصالات التي جرت مع الوقت في مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

ويختلف نوع المعلومات التي يتم تبادلها بين أجهزة الشرطة وجهات التحقيق باستخدام القنوات غير الرسمية حسب الدولة، فقد تكون السلطات في أحد الدول قادرة على تقديم أنواع معينة من المساعدة مثل إفادات الشهود الطوعية، وإجراء مقابلات طوعية للشهود، وأخذ شهادة الشهود الطوعية عبر تكنولوجيا الفيديو كونفرانس، واستضافة الشرطة الأجنبية التي تجري تحقيقات في أحد الجرائم السيبرانية، بينما في دولة ثانية قد يتخذ شكل المساعدة غير الرسمية تبادل المعلومات الاستخبارية، وإجراء المراقبة المادية، والحصول على السجلات الجنائية، وفي دولة ثالثة قد تستخدم قنوات التعاون غير الرسمي في المقام الأول للحصول على المشورة والمساعدة القانونية والتقنية.

وتسهل المنظمات الدولية والإقليمية التعاون الدولي غير الرسمي، على سبيل المثال، يمكن تقديم طلبات المساعدة إلى مكتب الأمم المتحدة المعني بالمخدرات والجريمة، أو من خلال الإنتربول Interpol الذي يعتبر أكبر منظمة دولية للشرطة في العالم، ولا شك أن آليات التعاون غير الرسمي تسهل النقل السريع للمعلومات بين جهات التحقيق.

(ب) التعاون الدولي الرسمي :

يعتمد التعاون الدولي على القوانين الوطنية الموضوعية المنسقة للجرائم السيبرانية، التي تبين الجوانب الموضوعية لهذه الجرائم، وقوانين الجرائم السيبرانية الإجرائية الوطنية التي تحدد قواعد الأدلة والإجراءات الجنائية.

كما يمكن تيسير التعاون الدولي الرسمي عن طريق إبرام المعاهدات الثنائية والإقليمية والمتعددة الأطراف بشأن الجرائم السيبرانية، مثل معاهدات المساعدة القانونية المتبادلة ومعاهدات تسليم المجرمين، ويلزم الانضمام إلى المعاهدات الإقليمية والمتعددة الأطراف المتعلقة بالجرائم السيبرانية أو التصديق عليها لجعل هذه المعاهدات ملزمة قانوناً.

ويلاحظ أنه ما زالت العديد من دول العالم تعتمد بشدة على الوسائل القضائية الرسمية التقليدية، وخصوصاً المعاهدات الثنائية المعنية بالمساعدة القانونية المتبادلة، لغرض الحصول على الأدلة الإثباتية التي تتجاوز الحدود الإقليمية، حيث يستخدم أكثر من ٧٠ في المائة من البلدان طلبات المساعدة القانونية المتبادلة الرسمية.

رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:

تلعب العديد من المنظّمات وعلى رأسها منظمة الأمم المتحدة دوراً هاماً في تعزيز العمل المشترك بين الدول؛ للحد من انتشار الجرائم السيبرانية ومواجهتها، وعقدت في سبيل ذلك العديد من المؤتمرات بداية من المؤتمر السابع الذي عقد في ميلانو ١٩٨٥ حتى المؤتمر الثاني عشر في ٢٠١٠ بالإضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات والذي عُقد تحت إشراف الأمم المتحدة في عام ١٩٩٤، ونتج عنه عدة توصيات ذات صلة بجرائم السيبرانية، بعضها تناول الأفعال التي تقع تحت طائلة الإجمام المعلوماتي، والبعض الآخر يتمثل في الإجراءات الواجب اتباعها لتطبيق القواعد الموضوعية.

وهكذا أصدرت منظمة الأمم المتحدة عدة قرارات وتوصيات بشأن العمليات السيبرانية، كما أنشأت فرقاً من الخبراء الحكوميين المعنيين بهذه العمليات، وناقشت هيئاتها أمن الفضاء السيبراني، وفيما يلي بيان ذلك:

١. وثائق الجمعية العامة للأمم المتحدة بشأن الجرائم السيبرانية:

أصدرت الجمعية العامة للأمم المتحدة عدة قرارات بشأن الجرائم السيبرانية، منها القرار رقم ٥٥/٦٣ في ٤ ديسمبر ٢٠٠٠م، والقرار رقم ٥٦/١٢١ في ١٩ ديسمبر ٢٠٠١، بشأن مكافحة سوء استخدام تكنولوجيا المعلومات، وقد أوصى القرار الأول بأن: تضمن الدول في قوانينها وممارساتها عدم توفير ملاذات آمنة لكل من يُسيء استخدام تكنولوجيا المعلومات، وضمان حماية سرية المعلومات وسلامة أنظمة الحاسوب، ضد أي اعتداء غير مشروع، مع تقرير عقوبة على ذلك الفعل.

ودعا القرار ٥٦/١٢١، الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

وفي عام ٢٠٠٢ أصدرت الأمم المتحدة القرار رقم ٥٧/٢٣٩، بشأن إرساء ثقافة عالمية للأمن السيبراني، حيث اعتمدت فيه قرارًا بشأن الأمن السيبراني والذي سلمت فيه بضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون في هذا المجال على الصعيد الوطني والإقليمي والدولي؛ كي يتسنى التصدي الفعال لما تتسبب به هذه التهديدات السيبرانية بصفة متزايدة، من طابع عابر للحدود الوطنية.

ويشهد هذا القرار على التزام العالم بإنشاء ثقافة عالمية للأمن السيبراني، وأهم ما في القرار أنه يُؤكّد أنّ الأمن السيبراني للهياكل الأساسية الحيوية للمعلومات مسئولية ملقاة على عاتق الحكومات، ومجال يجب عليها أن تحمل فيه لواء الصدارة وطنياً، بالتنسيق مع أصحاب المصلحة ذوي الشأن.

وفي عام ٢٠٠٥ أصدرت الأمم المتحدة القرار ١٧٧/٦٠، بشأن تشجيع التعاون الدولي لمكافحة الجرائم الإلكترونية، وتقديم المساعدة للدول الأعضاء في هذا المجال، كما أصدرت في عام ٢٠١٠، القرار رقم ٢١١/٦٤ الذي يدعو الدول إلى تحديث قوانينها في مجال الجرائم السيبرانية، والخصوصية، والبيانات الشخصية، والتجارة والتوقيع الإلكترونية، وكذلك اعتماد اتفاقيات إقليمية بهذا الشأن.

٢. قرارات المجلس الاقتصادي والاجتماعي:

قرارات المجلس الاقتصادي والاجتماعي ٢٠٠٦/٤٦ ، ٢٠٠٧/٨ ، ٢٠٠٨/٣ ، ٢٠٠٩/٧، هي التي أحاطت فيها اللجنة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية علماً بنتائج تنفيذ مؤتمر القمة العالمي لمجتمع المعلومات، استناداً إلى ما ورد من مساهمات من كيانات الأمم المتحدة ذات الصلة وغيرها من الكيانات، حسب الاقتضاء.

فضلاً عن ذلك افتتح المجلس الاقتصادي والاجتماعي دورته لعام ٢٠١٠ بجلسة إعلامية عن التحديات التي يطرحها الأمن السيبراني، فضلاً عن التهديدات والفرص التي يتيحها استخدام الإنترنت الآخذ في الاتساع، وقد شدّد المجلس من بين عدة أمور على الحاجة إلى اتخاذ مبادرات دولية تكفل تبادل المعلومات وأفضل الممارسات والتدريب والبحث، وإضافة إلى ذلك، أعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن «توحد أداؤها» بشأن هذه القضية، مما سيؤدي حتماً إلى زيادة التعاون بين البلدان بل وبين الدول والقطاع الخاص أيضاً؛ لضمان الأمن السيبراني وحذروا من النطاق الدولي لحرب سيبرانية فعلية وعواقبها وخيمة سوف تحدث بشكل خطير إن لم يتم تدارك الأمر، ومن ثمّ لا بُدّ أن تكون هناك استجابة منسقة بين الدول؛ ولا تكفي الآن إستراتيجيات اعتماد حلول على أساس مخصّص وتقوية الدفاع.

ودعا القرار أيضاً إلى اتّباع نهج قائم على إدراك المخاطر، بحيث يُحاط جميع أصحاب المصلحة علماً بالمخاطر ذات الصلة والتدابير الوقائية والردود الفعالة على نحو مناسب، كلّ في إطار الدور المنوط به.

وأشار القرار إلى أنَّ الجهود الوطنية إلزامية إلى حماية الهياكل الأساسية الحيوية للمعلومات التي تستفيد من التقييم الدوري للتقدم الذي تُحرزه هذه الجهود. وطالب القرار بمزيد من العناية الموضوع الأمن الإلكتروني، حيث دعا الدول الأعضاء إلى تقديم موجزات لمبادراتها الرئيسية بشأن الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات؛ كي يتسنى إبراز « ما يتم تحقيقه من الإنجازات وأفضل الممارسات والدروس المكتسبة والإجماليات التي تتطلب مزيدًا من التدابير على الصعيد الوطني»، وقدم استقصاء طوعيًا في شكل تقييم ذاتي للأمن الإلكتروني الوطني باعتباره أداة يمكن أن تساعد البلدان على استعراض الجهود الوطنية المبذولة في مجال الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات.

وفي سبتمبر عام ٢٠١١ عقد المجلس الاقتصادي والاجتماعي للأمم المتحدة، اجتماعًا لمناقشة أمن الفضاء الإلكتروني والتنمية والقضايا والتحديات ذات الصلة، واشترك في المناقشات إدارة الشؤون الاقتصادية والاجتماعية، والاتحاد الدولي للاتصالات، ورئيس لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية، ومنظومة الأمم المتحدة، والقطاعين العام والخاص، بالإضافة إلى منظمات المجتمع المدني المهتمة بمجالات الفضاء السيبراني والجرائم السيبرانية وحددت أهداف الاجتماع بأنّها تتمثل في بناء وعي على مستوى السياسات الدولية، عبر تزويد أعضاء المجلس الاقتصادي والاجتماعي، بصورة عن الوضع الحالي والتحديات المتعلقة بأمن الفضاء الإلكتروني، وارتباطه بالتنمية؛ وتحديد أفضل السياسات المتعلقة بهذا المجال، والمبادرات المطبقة في مختلف أنحاء العالم؛ لبناء ثقافة أمن الفضاء السيبراني، وكذا استكشاف خيارات للاستجابة العالمية بشأن تزايد معدلات الجريمة السيبرانية.

٣. مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء ... هافانا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر:

يُعتبر مؤتمر هافانا ١٩٩٠ من أبرز جهود الأمم المتحدة المتعلقة بالجرائم ذات الصلة بالكمبيوتر، فقد أكّد المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح الشعوب، وبالتالي لمنع الجريمة على نحو فعال.

كما أكّد على أنَّ التكنولوجيا بما أنها قد تولّد أشكالًا جديدة من الجريمة فإنّه ينبغي اتخاذ تدابير مُلائمة ضد حالات إساءة الاستعمال المخلة لهذه التكنولوجيا، وأشاروا إلى مسألة الخصوصية التي يمكن أن تخترق عن طريق الاطلاع على البيانات الشخصية المخزنة داخل نُظم الحسابات الآلية والتي تُشكّل انتهاكًا لحقوق الإنسان واعتداء على حرمة الحياة الخاصة، كما أكّد المؤتمر على وجوب اعتماد ضمانات مُلائمة لحفظ السرية.

٤. إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية :

في عام ٢٠٠٤، أنشأت الجمعية العامة للأمم المتحدة مجموعة للخبراء الحكوميين؛ لدراسة تأثير تطورات تكنولوجيا المعلومات والاتصالات على الأمن القومي والشئون العسكرية للدول، وقد تابع الفريق اجتماعاته سنوياً، وخلال عام ٢٠١٠ قدّم الفريق تقريراً، سلّط من خلاله الضوء على التهديدات التي تُثيرها العمليات السيبرانية للسلم والاستقرار الدوليين، وأن الافتقار إلى توجيه دولي بشأنها قد يتسبب في أضرار جسيمة، وقد أورد التقرير التوصيات التالية:

١. مواصلة الحوار بين الدول لمناقشة المعايير المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات للحد من مخاطرها، وحماية البنى التحتية الإلكترونية للدول.

٢. السعي لتحقيق تدابير بناء الثقة في مجال الحد من مخاطر استخدام الدول لتكنولوجيا المعلومات والاتصالات، بما في ذلك تبادل الآراء الوطنية بشأن استخدامها.

٣. تبادل المعلومات بشأن التشريعات الوطنية والمعلومات الوطنية وإستراتيجيات وتقنيات وسياسات أمن الاتصال وأفضل الممارسات.

٤. تحديد تدابير لدعم بناء القدرات في أقل البلدان نمواً.

خامساً : الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية:

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة، وفي مجال مكافحة الجرائم الناتجة عن الهجوم السيبراني بصفة خاصة، ومن بين المعاهدات والاتفاقيات التي تعمل على مكافحة الجرائم السيبرانية معاهدة بودابست لمكافحة جرائم الإنترنت، وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، وتبينها فيم يلي:

١. معاهدة بودابست لمكافحة جرائم الإنترنت :

تُعد معاهدة بودابست لمكافحة جرائم الإنترنت أولى المعاهدات المتعلقة بتلك الجرائم، والتي تمت في العاصمة المجرية بودابست في ٢٣/١١/٢٠٠١، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم السيبرانية، ويُعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت والاستخدام السيء لها.

وقد وقعت على تلك المعاهدة ٢٦ دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا والولايات المتحدة الأمريكية، وتُوفّر المعاهدة أسس الأمن العام.

وعلى الرغم من أنّ هذه الاتفاقية أوروبية المنشأ، إلا أنها مفتوحة للدول الأخرى لطلب الانضمام إليها لتعم الفائدة. وتتضمن الاتفاقية التعاون والعمل المشترك ما بين الدول الأعضاء وأعضاء القطاعات وأصحاب المصلحة ذوي الصلة، وهما ضروريان لبناء ثقافة للأمن السيبراني وفي الحفاظ عليها، وسبل مكافحة الجرائم السيبرانية.

هذا وقد تناولت المعاهدة الجرائم التي تُعتبر من أكثر الجرائم شيوعًا على مستوى العالم مثل الإرهاب السيبراني وعمليات تزوير بطاقات الائتمان ودعارة الأطفال. كما حددت المعاهدة الطرق الواجب اتباعها في التحقيق في جرائم الإنترنت، وتعهّدت الدول الموقعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، وما عبرت عنه المنظمات المدافعة عن حقوق الإنسان ومزودي خدمات الإنترنت من قلق، حيث تخشى منظمات حقوق الإنسان من أن تحدّ المعاهدة من حرية الأفراد، وأن تُؤدّي الرقابة إلى انتهاك حقوق مستخدمي الإنترنت.

٢. توصيات المجلس الأوروبي :

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية في هذا المجال إلى إصدار المجلس الأوروبي التوصية رقم ١٣/٩٥ في ١١/٩/١٩٩٥ في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، وحثّ الدول الأعضاء بمراجعة قوانين الإجراءات الجنائية الوطنية؛ لكي تتلاءم مع التطور في هذا المجال.

٣. إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لعام ٢٠٢٥:

هي أول معاهدة دولية شاملة، اعتمدها الجمعية العامة للأمم المتحدة ، تهدف لتوحيد جهود الدول لمكافحة الجرائم السيبرانية عبر تجريم الأفعال السيبرانية المجرمة، وتعزيز التعاون الدولي، وتمكين تبادل الأدلة الإلكترونية، وحماية الضحايا، وتدعم بناء القدرات للدول النامية لمواجهة التهديدات الرقمية المتزايدة مثل الإرهاب والاتجار بالبشر، ودخلت مرحلة التوقيع في أكتوبر ٢٠٢٥ .

أ. أبرز ملامح الاتفاقية :

بعد عقود من الاتفاقيات الإقليمية، مثل اتفاقية بودابست لعام ٢٠٠١ والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، هناك الآن اتفاقية دولية تجمع دولاً من جميع أنحاء العالم لغرض

وحيد هو مكافحة هذه الظاهرة الإجرامية. تتناول الاتفاقية (مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية) القضاء على الجريمة السيبرانية ومنعها في ستة فصول رئيسية، بما في ذلك صياغة التعريفات ذات الصلة في المادة ٢ استخدام المصطلحات ومن أبرز ملامحها:

- التجريم: تجريم أفعال مثل الوصول غير المصرح به، اعتراض البيانات، الاحتيال، استغلال الأطفال جنسياً عبر الإنترنت، ونشر الصور الحميمة دون موافقة.
- التعاون الدولي: إنشاء آليات للتعاون القضائي وتبادل الأدلة الرقمية بسرعة بين الدول، وشبكة اتصال على مدار الساعة.
- بناء القدرات: توفير الدعم والمساعدة التقنية للدول النامية لمواجهة الجرائم السيبرانية.
- حماية الضحايا: نصوص خاصة لحماية الضحايا، وخاصة النساء والأطفال.
- المساءلة: تضع إطاراً قانونياً لمكافحة استغلال تكنولوجيا المعلومات والاتصالات في ارتكاب جرائم خطيرة (إرهاب، اتجار بالبشر، جرائم مالية) .

ب. الوضع الحالي (ديسمبر ٢٠٢٥):

- الاعتماد: اعتمدت في ٢٤ ديسمبر ٢٠٢٤.
- التوقيع: فتح باب التوقيع في أكتوبر ٢٠٢٥ في هانوي، ووقعت عليها ٧٢ دولة في المراسم الأولية.
- التنفيذ: تدخل حيز التنفيذ بعد ٩٠ يوماً من إيداع التصديق الأربعين من الدول الأطراف .

ج. الأهمية:

- تُعد أول معاهدة عالمية شاملة، تسد فجوة في القانون الدولي وتكمل الاتفاقيات الإقليمية مثل اتفاقية بودابست.
- تؤكد قدرة المجتمع الدولي على إيجاد حلول مشتركة لمواجهة التحديات العالمية المتزايدة في الفضاء السيبراني .

سادسا : جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية:

كان للمنظمات العلمية المتخصصة دور مهم بشأن التعامل مع العمليات السيبرانية بأنواعها المختلفة، وتحقيق قدر من الأمن في مجال المعاملات الإلكترونية ومن أبرز هذه المنظمات الاتحاد الدولي للاتصالات والمنظمة العالمية للملكية الفكرية، ومنظمة حلف شمال الأطلسي، وتعرض لجهود كل منظمة منها من خلال الفروع التالية:

١. الاتحاد الدولي للاتصالات :

نشأ الاتحاد الدولي للاتصالات بمقتضى اتفاقية باريس عام ١٨٦٥ تحت اسم (اتحاد التلغراف الدولي)، ثم عُدّل الاسم ليصبح (الاتحاد الدولي للاتصالات السلكية واللاسلكية، وفي عام ١٩٤٧ انضمَّ الاتحاد إلى هيئة الأمم المتحدة، وصار إحدى الوكالات المتخصصة في عمل الاتصالات المنطوية تحت مظلة الأمم

المتحدة فأصبح بمثابة ملتقى دولي رئيسي لهذه الأنشطة . ويتكون هذا الاتحاد من ١٩٢ دولة و ٧٠٠ شركة من القطاع الخاص والمؤسسات الأكاديمية، ويُعتبر منبرًا «إستراتيجيًا» للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة، حيث يعمل الاتحاد على مساعدة الحكومات في الإتفاق على مبادئ مشتركة تُفيد الحكومات أو الصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات.

ويقترح الأمين العام للاتحاد الدولي للاتصالات خمسة مبادئ توجيهية لإحلال السلام وحفظه في العالم السيبراني الناشئ إدراكا منه للخطر المتنامي للهجوم السيبراني، وقد أُعدَّت لوائح الاتصالات الدولية كإطار تنظيمي لمعالجة القضايا الناشئة والتحديات التي تُصاحب عالم الاتصالات الجديد الذي تجسد في أواخر ثمانينات القرن الماضي، وقد صيغت هذه اللوائح لتعزيز الكفاءة والتنمية الدوليين، فضلا عن أنها تُبرز تركيز الاتحاد على حماية الحق في الاتصال وفي الوقت نفسه عدم إلحاق الضرر بالمرافق .

٢. المنظمة العالمية للملكية الفكرية :

إبان عام ١٩٦٧ تم التوقيع في ستوكهولم بالسويد على اتفاقية المنظمة العالمية للملكية الفكرية، وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارًا من السابع عشر من ديسمبر عام ١٩٧٤، والتي من أهدافها حماية الملكية الفكرية في شتى أنحاء العالم عن طريق التعاون بين الدول الأعضاء والمنظمات الدولية الأخرى، وتعمل المنظمة على متابعة تنفيذ الاتفاقيات المتعلقة بالتصميمات الصناعية وتصنيف السلع التجارية وحماية الأعمال الإدارية والفنية وحقوق الإنتاج.

كما تشجع المنظمة كذلك على توقيع معاهدات دولية جديدة، وتقوم بالتنسيق بين التشريعات الوطنية، وتقديم المساعدات القانونية والفنية للدول النامية؛ بهدف حماية الملكية الفكرية وتنميتها وتغطية بعض أوجه القصور في مجال التوثيق العلمي ونقل التقنية الحديثة .

وبالرجوع إلى اتفاقية إنشاء هذه المنظمة تتضح غايات هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم بجميع صورها (المصنفات الأدبية والفنية والعلمية والاختراعات)، ومع تزايد الحاجة العالمية لحماية البرامج شكلت هذه المنظمة مجموعة عمل تضم عددًا من الخبراء؛ بهدف حماية برامج الحاسب الآلي، وبعد سلسلة من الاجتماعات والدراسات حول الأساليب المثلى لحماية برامج الحاسوب، ساد الاتجاه لدى أغلب الدول إلى الميل إلى خضوع برامج الحاسوب لقوانين حماية حق المؤلف .

٣. منظمة حلف شمال الأطلسي:

دفع عجز حلف الناتو في مواجهة الهجمات السيبرانية على إستونيا عام ٢٠٠٧ وجورجيا عام ٢٠٠٨ إلى تكوين وحدة للدفاع السيبراني، مقرها تالين عاصمة إستونيا، وعمل على تطوير المفهوم الإستراتيجي

للحلف؛ بحيث أصبح الفضاء السيبراني منطقة لعمليات الحلف، وأنَّ عليه أن يُطور قدراته الدفاعية السيبرانية بما يش مل مساندة ودعم حلفائه الذين يتعرضون لهجمات سيبرانية، وأنه وفقًا لذلك فإنَّ أي هجوم يتم على أوروبا أو أمريكا الشمالية يُعتبر هجومًا ضد الجميع .

ولذا نفّذت الناتو السياسة الخاصة بها في مجال الدفاع السيبراني في ٢٠٠٨؛ من أجل حماية مواردها التكنولوجية وتلك الخاصة بالدول الأعضاء وكجزء من هذه السياسة، أنشأ الحلف هيئة معيّنة بإدارة الدفاع السيبراني، وفريقًا للاستجابة للحوادث الحاسوبية، يكفل إرسال فرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزًا للتميز من أجل الدفاع السيبراني التعاوني، ويضم هذا المركز الذي يُوجد مقره في إستونيا خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني.

المراجع

• الكتب:

د. أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة تحليلية تأصلية مقارنة، الطبعة الأولى، سنة ٢٠١٧ .

• الرسائل:

١. د. أحمد طلعت عبد الحكيم عبد الحكيم عبد الرحمن، السياسة الجنائية في مواجهة جرائم تقنية المعلومات في ضوء القانون المصري رقم ١٧٥ لسنة ٢٠١٨، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، ٢٠٢٢.

٢. د. محمد خالد إبراهيم، الجوانب الموضوعية لجرائم تقنية المعلومات، دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، سنة ٢٠٢٣.

• المواقع الإلكترونية:

٣. د. هاني محمد إبراهيم خليل، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، بحث منشور علي موقع:

<https://espes1.journals.ekb.eg.pdf>

تم بحمد الله

الإنهاء من شرح المحاضرة العاشرة
مع تمنياتي بالتوفيق د. أسماء رويحي