التعاون الدولي في مجال مكافحة جريمة التجسس الإلكتروني

International cooperation in combating cyber espionage crime

بحث مقدم من قبل
الباحث المدرس المساعد حسين فلاح أبو الحب
الجامعة الإسلامية/ كلية الحقوق / ماجستير قانون دولي عام
أشراف الاستاذ الدكتور محمد فرحات
Assistant teacher. Hussein Falah Aboalhab
Islamic University / Faculty of Law
Master of Public International Law
husseinaboalhob@yahoo.com

الخلاصة
التجسس الإلكتروني أنموذج أجرامي ظهر حديثاً وقد تباينت التعاريف التي وضعت لهذه الجريمة فيما بينها لما تتميز به هذه الجريمة عن باقي الجرائم من سرعة في اتمامها وإمكانية محو الدليل واتلافه مما يصعب كشف مرتكبها وكونها لا تحتاج إلى قوة وعنف في تنفيذها علاوةً على ذلك تعد من الجرائم العابرة للحدود، لذلك عُد التجسس الإلكتروني من أخطر الجرائم المترابطة بتكنولوجيا المعلومات ومن أبرز التهديدات الأمنية التي تتعرض لها الحكومات والمواطنين من طرف استخبارات داخلية أو خارجية على حدٍ سواء، وعليه أضحت جريمة التجسس الإلكتروني محل جدل واسع في المحافل الدولية، نظراً للآثار الخطيرة المترتبة عليها سواء كانت على المستوى الشخصي أو السياسي أو الاقتصادي أو الأمني أو حتى الاجتماعي، مما دفع المجتمع الدولي والهيئات والمنظمات الدولية إلى ضرورة التعاون والتصدي لهذه الجريمة ومكافحتها من خلال اعتماد اتفاقيات دولية وبروتوكولات خاصة.
الكلمات المفتاحية: التجسس الإلكتروني، مكافحة الجريمة، التعاون الاتفاقي، التعاون القضائي.

Abstract:
Electronic espionage is a criminal model that has emerged recently, and the definitions that have been developed for this crime have varied among themselves because this crime is distinguished from the rest of the crimes in terms of speed in its completion and the possibility of erasing and destroying evidence, which is difficult to detect the perpetrator and the fact that it does not need force and violence in its implementation, moreover, it is considered a cross-border crime, so electronic espionage is one of the most serious crimes related to information technology and one of the most prominent security threats to governments and citizens by internal intelligence or Therefore, the crime of electronic espionage has become the subject of wide controversy in international forums, due to its serious effects, whether on the personal, political, economic, security or even social levels, which prompted the international community and international bodies and organizations to cooperate and address this crime and combat it through the adoption of international conventions and special protocols.
Keywords: cyber espionage, prevention crime, treaty cooperation, judicial cooperation.

المقدمة:

لم يعد يقتصر التجسس على المعلومات العسكرية أو السياسية[1]، بل تجاوزه إلى المجال الاقتصادي والثقافي والتجاري[2]، إذ تعتمد جريمة التجسس الإلكتروني على تقنيات عالية التقدم، لاسيما أن هذا النوع من الجرائم ظهر بصفة خاصة عقب أحداث الحادي عشر من سبتمبر التي شهدتها الولايات المتحدة الأمريكية، ويعد هذا النوع من أنواع الجرائم المعلوماتية أو الإلكترونية ومن الطرق المعتمدة على اقتراف هذه الجريمة وسيلة إخفاء المعلومات داخل المعلومات بحيث يتم إخفاء هذه المعلومات المهمة والمستهدفة داخل معلومات عادية في جهاز الحاسب الآلي، وبالتالي يتم تهريبها باستخدام أساليب حديثة ومتطورة لم يتم اكتشافها حتى ولو تم ضبط الشخص في حالة تلبس ومثال لذلك، شبكة دولية ضخمة للتجسس الإلكتروني التي تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات في كندا وبريطانيا لرصد المكالمات الهاتفية بقصد التعامل مع الأهداف غير العسكرية، ولا ينحصر الرصد في المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية، بل يضم الاتصالات التي تتم عبر أنظمة الاتصالات الأرضية[3]. أي أن التجسس الإلكتروني يتمثل بدخول الجاني إلى نظام المعلومات أو الشبكة المعلوماتية أو موقع إلكتروني بهدف الحصول على محتوى إلكتروني ليس متاحاً للجمهور ويمس الأمن الوطني أو بعلاقاتها الخارجية أو الاقتصاد الوطني أو سلامتها العامة[4].

ونظراً لخطورة تلك الجريمة وصعوبة الكشف عنها وغياب الدليل المادي الذي يدين فاعلها، فأصبحت تطغى على ساحة الإجرام بشكل ضخم وذلك لعدم وجود استراتيجية فعالة لمحاربتها والحد منها لاسيما على المستوى الدولي في ظل ضالة الاتفاقيات الدولية وصعوبة التعاون الدولي للتقليل منها، وذلك بالنظر إلى الطبيعة الخاصة لها.

أهمية موضوع البحث:

تكمن أهمية موضوع البحث في سعي المجتمع الدولي إلى التعاون في مكافحة جريمة التجسس الالكتروني نظراً للخطورة الملحقة بالأمن المعلوماتي سواء بالنسبة للأشخاص بصفة خاصة، أو على مستوى الدول بصفة عامة، كذلك مدى فاعلية القوانين المجرمة لها، خاصة وأنها تعد جريمة من الجرائم العابرة للحدود والتي تثير بدورها الخلاف حول مسألة التنازع القانوني والقضائي.

الهدف من البحث:

تبدو أهداف هذا البحث فيما تثيره جريمة التجسس الإلكتروني من زعزعة للأمن ونشر الخوف والرعب، وإخلال نظام الدول العام وتهديد وابتزاز الأشخاص والسلطات العامة والمنظمات الدولية، وعلى أساس ذلك معرفة إمكانية التعاون الدولي ومدى فاعلية المعاهدات والاتفاقيات والبروتوكولات المطبقة لمكافحة هذه الجريمة.

إشكالية البحث:

تبدو المشكلة الرئيسية لموضوع التجسس الإلكتروني في القانون الواجب التطبيق عليها، خاصة وأنها جريمة عبر وطنية وتنتقل عبر الحدود عبر شبكات إلكترونية حول العالم، وقد يكون من الصعوبة بمكان تحديد الجاني مرتكب الجريمة ومكان وقوع الجريمة وعليه، فهي تثير عدة إشكالات أخرى في الاختصاص.

خطة البحث:

تضمن البحث فضلاً عن المقدمة والخاتمة مبحثين تناولنا في المبحث الاول التعاون الاتفاقي الدولي في مجال مكافحة جريمة التجسس الإلكتروني أما في المبحث الثاني التعاون القضائي الدولي في مجال مكافحة جريمة التجسس الإلكتروني.

المبحث الأول/ التعاون الاتفاقي الدولي في مجال مكافحة جريمة التجسس الإلكتروني

تسعى العديد من الدول إلى بناء تعاون اتفاقي دولي رغبةً منها في تعزيز التعاون في مجال مكافحة الجريمة الإلكترونية لاسيما ذكرنا سابقاً أن الجريمة الإلكترونية بصفة عامة ومنها جريمة التجسس الإلكتروني التي تعد من أكثر الجرائم العابرة للحدود الوطنية والتي باتت تهدد أمنها ومصالحها وسلامة مجتمعاتها، فقد يقوم بعملية التجسس الإلكتروني شخص في دولة معنية إلا أن أثرها يحدث في دول مختلفة[5] ونتيجة الفوارق بين الأنظمة العقابية الداخلية للدول ما يدفع المجرم إلى البحث عن الأنظمة الأكثر تسامحاً، ولمواجهة هذه الجريمة قامت الدول بعقد اتفاقيات ومؤتمرات لمكافحتها وذلك على النحو التالي:-

المطلب الأول/ القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر[6].

يعد هذا القرار من الجهود التي بذلتها الأمم المتحدة، إذ عقد هذا المؤتمر في هافانا سنة 1990 وقد حث في قراره الخاص بالجرائم المتعلقة بالكمبيوتر[7] الدول الأعضاء أن تكثّف جهودها لمكافحة إساءة استعمال هذا الجهاز وبتجريم تلك الأفعال جنائياً. واتخاذ الإجراءات التالية متى دعت الضرورة لذلك:

الفرع الأول: ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق والأدلة في الإجراءات القضائية تنطبق على نحو ملائم، وإدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك.

الفرع الثاني: النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة إذ تدعو الضرورة للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم.

كما حث أيضاً الدول الأعضاء على مضاعفة الأعمال التي تقوم ببذلها على الصعيد الدولي للعمل على مكافحة الجرائم المتصلة بالكمبيوتر بما فيها دخولها كأطراف في المعاهدات المرتبطة بتسليم المجرمين وتبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بشكل تام على الأشكال الجديدة للإجرام مثل الجرائم الإلكترونية، وأن تتخذ خطوات محددة نحو تحقيق هذا الهدف. كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة المعلوماتية بصفة عامة بضرورة وضع أو تطوير:-

أ. معايير دولية لأمن المعالجة الآلية للبيانات.

ب. اتخاذ تدابير ملائمة لحل إشكالية الاختصاص القضائي التي تنشئها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية.

ج. إبرام اتفاقيات دولية تنطوي على نصوص تنظيم وإجراءات التفتيش والضبط المباشر الحاصل عبر الحدود على الأنظمة المعلوماتية المرتبطة فيما بينها والصور الأخرى للمساعدة المتبادلة مع ضمان الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم وسيادة الدول.

المطلب الثاني/ مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 1994 البرازيل بشأن جرائم الكمبيوتر.

انعقد هذا المؤتمر سنة 1994 بالبرازيل والذي نَصَّ على الأفعال المجرمة والمصنفة جرائم معلوماتية كالاحتيال والغش المرتبط بالكمبيوتر من خلال إتلاف ومحو المعطيات، وأيضاً ما يعرف بالتزوير المعلوماتي ويشمل إتلاف ومحو البرامج والبيانات وتعطيل وظائف الكمبيوتر ونظام الاتصالات (الشبكات)، أو الدخول غير المصرح به عن طريق انتهاك إجراءات الأمن.

أما من الجهة الإجرائية فإنّ القرار الصادر عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات تضمن جملة من القواعد الإجرائية في بيئة الجرائم المعلوماتية تكمن فيما يلي[8]:

الفرع الأول/ القيام بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وأيضاً تفتيش شبكات الحاسب الآلي.

الفرع الثاني/ التعاون الفعال بين المجني عليهم والشهود وكذلك مستخدمي المعلومات من أجل إتاحة استخدام المعلومات للأغراض القضائية.

الفرع الثالث/ اعتراض الاتصالات داخل نظام الحاسب الآلي ذاته وممارسة الرقابة عليها.

المطلب الثالث/ اتفاقية برن الدولية لحماية المصنفات الأدبية والفنية.

بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام اتفاقية برن الدولية في 9 أيلول/ سبتمبر 1886، والمكملة بباريس في آذار/ مارس 1896، والمعدلة في برلين في 13 أيلول/ سبتمبر 1908، والمكملة بـ برن في 20 آذار/ مارس 1914، والمعدلة بروما في حزيران/ يونيو 1928، وبروكسل سنة 1948، وستوكهولم في تموز/ يوليو 1967، وباريس في تموز/ يوليو 1971، إذ تشكل الدول الأطراف في هذه الاتفاقية اتحاداً لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية.

وبموجب اتفاقية برن الدولية تتمتع برامج الحاسب الآلي "الكمبيوتر" سواء أكانت بلغة المصدر أو بلغة الآلة بالحماية كونها أعمالاً أدبية وفقا لماً جاء فيها[9].

المطلب الرابع/ اتفاقية بودابست لمكافحة جرائم المعلوماتية 2001.

إدراكاً من الدول بمدى خطورة الجريمة المعلوماتية بوصفها جريمة عابرة للحدود فقد تم التوقيع عليها من طرف ثلاثين دولة في العاصمة المجرية "بودابست" نذكر منها: دول أعضاء من الاتحاد الأوروبي، فضلاً عن كندا، اليابان، جنوب إفريقيا، أمريكا، وجاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة الإلكترونية وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها والمساعدة على الاستدلال عليهم وضبطهم، كما تحدد أفضل الوسائل التي ينبغي اتباعها في التحقيق في جرائم الإنترنت التي تعيد الدول الموقعة بالتعاون الوثيق بقصد محاربتها، كذلك فصلت الاتفاقية النصوص الجنائية الموضوعية للجريمة وأنواعها كما تشمل جوانب عديدة من جرائم الإنترنت من بينها الإرهاب، عمليات تزور بطاقات الائتمان وغيرها.... وتعد هذه الاتفاقية في رأي الباحث أجد محاولة وأكثرها تنوعاً من أجل تنسيق قوانين جديدة في دول عديدة ضد إساءة استخدام الإنترنت. كما نشير إلى أنها تأتي بعد فترة طويلة من المشاورات بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر وقد صاغ نصها عدد من الخبراء القانونين في مجلس أوروبا بمساعدة دول أخرى.

المطلب الخامس/ قانون الأونستيرال النموذجي[10].

اقتناعاً من الدول بضرورة منع هذه الجرائم ومكافحتها خاصة وأن ذلك يتطلب استجابة ديناميكية في ضوء الطابع الدولي والأبعاد الدولي لإساءة استخدام الكمبيوتر والجرائم المتعلقة به تم صياغة قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية والآخر بشأن التجارة الإلكترونية.

الفرع الأول/ قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية.

اعتمد هذا النص في 5 تموز/ يوليو 2001 وينطبق هذا القانون حيثما تستخدم توقيعات إلكترونية[11] خاصة بعدما أصبح للتوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة، والحداثة التكنولوجية إذ إنّه أمام هذه التطورات تلاشت وظيفة التوقيع التقليدي ليحل محله التوقيع الإلكتروني وهو عبارة عن كود سري أو شفرة سرية يتم الحصول عليها بعد إتباع جملة من الإجراءات.

الفرع الثاني/ قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية.

تنطبق نصوص هذا القانون على أي صورة من المعلومات التي تكون على شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية، بحيث يتم استلامها أو تخزينها بطرق الكترونية، ويتم تبادل هذه البيانات من خلال نقلها الكترونياً من حاسوب إلى آخر باستخدام معيار متفق عليه، مع الأخذ في الحسبان تفسير هذا القانون لمصدره الدولي ولضرورة توحيد تطبيقه.

المطلب السادس/ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010

رغبةً من الدول العربية في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعها، واقتناعاً منها بضرورة الحاجة إلى تبنّي سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذاً بالمبادئ الدينية والأخلاقية السامية لاسيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الانسان ذات الصلة من حيث ضمانها واحترامها وحمايتها، ومن الاعمال التي جرمتها الاتفاقية العربية جريمة الاعتداء على سلامة البيانات حيث تطرّقت لها الاتفاقية في المادة الثامنة من الفصل الثاني أما في المادة

التاسعة فقد تطرّقت إلى جريمة إساءة استخدام وسائل تقنية المعلومات وفي المادة الثامنة عشر الاستخدام غير المشروع لأدوات الدفع الإلكتروني[12].

المبحث الثاني/ التعاون القضائي الدولي في مجال مكافحة جريمة التجسس الإلكتروني

لما كانت الجرائم المعلوماتية ذات طابع عالمي، وبالتالي يمكن أن تتعدى آثارها عدة دول فإن ملاحقة مرتكبي هذه الجرائم ومحاكمتهم وتوقيع الجزاء عليهم يتطلب القيام بأعمال إجرائية خارج حدود الدولة، إذ ارتكب الجريمة أو جزء منها، مثل معاينة موقع الإنترنت في الخارج، أو ضبط الأقراص الصلبة التي توجد عليها معلومات غير مشروعة أو صور إباحية، 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 تساعدهم في تحقيق هذه الجرائم، كل ذلك لا يمكن تحقيقه بدون تعاون قضائي بين الدول.

هذا وتتمثل صور التعاون القضائي الدولي في مجال مكافحة جريمة التجسس الإلكتروني في الآتي: -

المطلب الأول/ المساعدة القضائية الدولية:

الفرع الأول/ مفهومها: -

تعني المساعدة القضائية الدولية هي كل إجراء قضائي تباشره دولة ما من اجل تيسير مهمة المحاكمة في دولة أخرى بشأن إحدى الجرائم[13].

وترتبط المساعدة القضائية بالمعاونة في مكافحة الجرائم في المجال الجنائي وذلك عن طريق عقد الاتفاقيات، وذلك كنقل صحف الحالة الجنائية، والمساعدة في المواد الجنائية من خلال تجميع عناصر الأدلة، والقيام بالبحث، وتقديم المعلومات، والوثائق التي تطلبها سلطة قضائية أجنبية [14].

ولا تتم هذه المساعدة إلا من خلال خطوات ثلاث هي[15]:

أ. الطلب:

ويقدم بواسطة الدولة صاحبة الاختصاص الجنائي بالمحاكمة، هذا الطلب يخضع لقانون الدولة الطالبة وفي إطار الاتفاقية التي تبرمها مع الدولة التي ستقوم بتقديم المساعدة، ويتم تقديم الطلب بالوسائل الدبلوماسية وفقا للأصل، إلا أن بعض الاتفاقيات الدولية تجيز الاتصال المباشر بين جهات العدل في الدولتين لإنجاز للوقت.

ب. فحص الطلب:

وتباشره الدولة التي ستقدم المساعدة، ويحدث ذلك من خلال التأكد من اعتبار الواقعة المطلوب تحقيقها تمثل جريمة طبقاً لقانون الدولة الطالبة، وفي ضوء مدى اختصاص الدولة المطلوب منها بقبول هذا الطلب طبق النصوص الاتفاقية التي تعقدها مع الدولة الطالبة.

ج. تنفيذ المساعدة القضائية:

ويحدث حسب قواعد الدولة المطلوب منها، إذ يتم تنفيذ الإجراء طبقا لقانون الدولة التي تنفذه.

وتعد الاتفاقيات الدولية وحدها الوسيلة التي يجوز أن تنشأ عنها الالتزامات بين الدول، وبالتالي فإنه بغير الاتفاقيات الدولية، وخارج الشروط التي تنص عليها لا تستطيع الدولة أن تعتمد على مساعدة الدولة المطلوب منها، على أن ما ليس ملزماً يظل مع ذلك ممكناً طبقاً لما ينص عليه القانون الداخلي في كلا الدولتين.

الفرع الثاني/ أشكال المساعدة القضائية:

أ. تبادل المعلومات يعني به تقديم المعلومات والوثائق التي تحتاجها سلطة قضائية أجنبية بشأن جريمة من الجرائم عن الاتهامات التي تم توجيهها إلى رعاياها في الخارج والإجراءات التي اتخذت تجاههم، كما أن هناك شكلاً آخر لتبادل المعلومات يرتبط بالسوابق القضائية للجناة، بواسطتها تتحري الجهات القضائية بدقة على الماضي الجنائي للشخص المحال إليها، وهي تساهم في تقرير الأحكام الخاصة بالعود ووقف تنفيذ العقوبة، إلا أن تدويل الصحيفة الجنائية يظل في مراحله الأولى، وتقوم الدول بإعدادها فيما يخص رعايا الدول التي ترتبط بها باتفاقيات تبادل معلومات[16]. وقد أقرت بتبادل المعلومات الاتفاقية الأوروبية حول الجريمة الافتراضية في المادة (23) والتي نصت بشكل صريح على ضرورة توافر التعاون الدولي بين الدول الأطراف وترسيخه وتقليل العراقيل بما يضمن أكبر قدر من السهولة والسرعة لتبادل

المعلومات والأدلة بين الأطراف[17]. كما اشارت اتفاقية الرياض العربية للتعاون القضائي في مادتها الأولى على ضرورة التبادل بين وزارات العدل لدى الأطراف المتعاقدة بصورة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل المعلومات المختلفة بالتنظيم القضائي[18]. وفيما يخص الجرائم الإلكترونية فقد نَصَّت المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على "تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسالمة مجتمعاتها وأفرادها"[19].

ب. حضور الشهود والخبراء ويعد حضور الشهود والخبراء من دولة إلى دولة أخرى شكلاً مهماً من أشكال المساعدة القضائية الدولية في المجال الجنائي[20]، وينبغي أن يحضر الشاهد أو الخبير باختياره لهذا الهدف أمام الهيئات القضائية في الدولة التي تطلب حضوره، وله حصانة إزاء اتخاذ أية إجراءات جنائية ضده أو القبض عليه أو حبسه عن أفعال أو تنفيذ أحكام سابقة على دخوله إقليم الدولة طالبة حضوره.

وينبغي عند إعلان الشاهد أو الخبير أن يتم إخطاره بشكل كتابي بتلك الحصانة قبل حضوره لأول مرة.

المطلب الثاني/ نقل الإجراءات

يقصد بنقل الإجراءات قيام إحدى الدول باتخاذ الإجراءات الجنائية بشأن جريمة وقعت داخل إقليم دولة أخرى ولصالح تلك الدولة بناء على اتفاقية، وذلك إذا توافرت شروط معينة، أهمها:

الفرع الأول/ أن يعد السلوك المنسوب إلى الشخص يمثل جريمة في كلتا الدولتين الطالبة والمطلوب منها.

الفرع الثاني: أن تكون الإجراءات الواجب اتخاذها معمول بها في قانون الدولة المطلوب منها عن نفس الجريمة.

الفرع الثالث/ أن يكون الإجراء الواجب اتباعه ينشأ عنه التوصل إلى الحقيقة، كحالة وجود أدلة الجريمة بالدولة المطلوب منها.

ولقد أكّدت الكثير من الاتفاقيات الدولية والإقليمية على تلك الصورة كإحدى أشكال المساعدة القضائية الدولية، كمعاهدة الأمم المتحدة النموذجية بخصوص نقل الإجراءات في المسائل الجنائية[21]، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000 [22]، وكذلك معاهدة المؤتمر الإسلامي لمكافحة الإرهاب 1999، وكذلك النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن المجلس التعاوني الخليجي 2003، وكذلك الاتفاقية الفرنسية المصرية المبرمة في 1982/3/15، وكذلك الاتفاقية المصرية الإيطالية الموقعة بالقاهرة في 2001/2/15.

ويحقق نقل الإجراءات الجنائية تقليص النتائج السلبية التي تنشأ عن تنازع الاختصاص بين الدول وتفوت الفرصة على المجرمين الجاري التحقيق معهم في الإفلات من العقاب.

ولكن بالرغم من ذلك فإن هذه الاتفاقيات تمثل آليات تقليدية في مكافحة الجرائم وملاحقة مرتكبيها، وهو ما قد لا يكون مجدياً في إطار الجرائم الواقعة في بيئة الإنترنت لما تسببه هذه الفئة من الجرائم وفقاً لسماتها وطبيعتها العابرة للحدود الوطنية من صعوبات تتعلق بإقامة الدليل على ارتكابها، ومدى قبول التشريعات لدى مختلف الدول للأدلة المستمدة من الحاسوب، وكذلك ما يتعلق بمسائل الضبط والتفتيش في القضاء الرقمي وتتبع المسارات الإلكترونية، كل هذه العوامل تؤدي إلى صعوبة إثبات جرائم الإنترنت ونسبتها إلى مرتكبيها، لذا فقد دعت بعض التشريعات إلى التعاون الدولي في مجال تفتيش أجهزة الحاسوب[23].

ومن أمثلة نقل الإجراءات كنوع من التعاون القضائي الدولي حينما تلقت السلطات الأوكرانية عام 2006، طلباً بالوسائل الدبلوماسية من محكمة لبنانية بمقتضى المادة 18 من اتفاقية الجريمة المنظمة عبر الدولية والوطنية لاستصدار أوامر استدعاء لأربعة شهود، وقد استجابت أوكرانيا لذلك الطلب، وبالفعل صدر أمر استدعاء لأحد الشهود، أما أوامر الاستدعاء الأخرى فلم تصدر، لأن الشهود لم يكونوا متواجدين على الأرضي الأوكرانية[24].

المطلب الثالث/ الإنابة القضائية:

يقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لوجوب ذلك للفصل في أمر مطروح على السلطة القضائية في الدول الطالبة ويصعب عليها القيام به بذاتها[25]. فالإنابة القضائية تعبّر عن قيام دولة ما بمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لدولة أخرى نيابة عنها، بناء على طلب تلك الدولة المناب عنها، ووفقاً لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن[26]. وتهدف الإنابة القضائية إلى نقل الإجراءات في الأمور الجنائية لمحاربة ما تحدثه الظواهر الإجرامية من تطور وتيسير العقبات التي تعترض سير الإجراءات الجنائية الخاصة بقضايا تمتد خارج الحدود الوطنية. وتعبير الإنابة في الشريعة الإسلامية ليس تعبيراً حديثاً ابتكره فقهاء القانون، وإنما هو تعبير استخدمه أيضاً علماء المسلمين منذ زمن طويل، صحيح أن الكثير من فقهاء المسلمين تكلموا عن الإنابة القضائية ضمن كلامهم عن كتاب القاضي إلى القاضي، والآخرون كالمالكية تكلموا عنه في خطاب القضاة، لكنهم عبروا عنه أيضاً بالاستنابة [27].

ويراد بكتاب القاضي إلى القاضي - والذي تدور حوله مفهوم الإنابة القضائية - الكتابة من قاض إلى آخر، أي الإنهاء إليه بأداء الشهادة أو الثبوت أو الحكم، معنى ذلك أن لكتاب القاضي إلى القاضي ثلاثً صور:

الصورة الأولى: أن يكتب القاضي ما يسمعه من شهادة الشهود دون تعديل أو تزكية ويرسل بها إلى القاضي الآخر الذي ينظر في تعديل الشهود ويستكمل باقي الإجراءات في الدعوى ويفصل فيها.

الصورة الثانية: أن يكتب القاضي الشهادة التي سمعها من الشهود مع تعديلهم وتزكيتهم ويرسل بها إلى القاضي الآخر، فالإنهاء هنا تضمن نقل ثبوت الحق فقط، وبالتالي فالقاضي المكتوب إليه يحكم في الدعوى وينفذ الحكم دون البحث عن عدالة الشهود.

الصورة الثالثة: أن يكتب القاضي صورة الحكم الذي حكم به ويرسل بها إلى القاضي المكتوب إليه ليقوم بتنفيذه[28].

ومن خلال الرجوع إلى أحكام كتاب القاضي إلى القاضي في كتب المذاهب الإسلامية يتضح أن كتاب القاضي إلى القاضي لا يقتصر فقط على الصور السابقة ولكنه قد يتضمن أيضاً العديد من الصور الأخرى على حسب موضوعه. وقد أجاز الفقهاء كتاب القاضي إلى القاضي - الإنابة - لحاجة الناس إلى ذلك، فقد يكون الشاهد للمرء على حقه في بلد وخصمه في بلد آخر فيتعذر عليه الجمع بينهما، كما قد يتعذر عليه السفر بالشهود، كما أن صاحب الحق قد يتعذر عليه حمل خصمه والزامه بالحضور إلى موطنه أو موطن الشهود، كما يجوز أن يكون العين المدعى بها في بلد آخر غير التي يوجد بها القاضي وطرفي الخصومة، وعلى هذا فكتاب القاضي وسيلة لإحياء الحقوق وتحقيق العدالة والتيسير على الناس[29].

وتتميز الإنابة القضائية بين الدول في مجال مكافحة الجرائم ذات الطابع الدولي بوجه عام والجرائم المعلوماتية بوجه خاص بمميزات هامة تتمثل في الحفاظ على السيادة الوطنية، فتعمل الأجهزة الأمنية المختصة بهذه الإجراءات المطلوبة على أرض الدولة دون مشاركة حقيقية من الأجهزة الأمنية في الدولة الأخرى الطالبة. ويساعد تنفيذ ذلك التعاون في الوقت المناسب على عدم ضياع الأدلة والآثار المتعلقة بالجريمة وإنجاز التحقيقات الجارية في الدولة الطالبة، ويحفظ حقوق المتهمين في الإسراع بمحاكمتهم وعدم بقائهم في السجن دون محاكمة، انتظاراً لإتمام تلك الإجراءات القانونية في دولة أخرى.

وتتطلب الإنابة القضائية الدولية إرسال الملف المتعلق بالدعوى الجنائية ومرفقاته من مستندات ووثائق ومحاضر التحقيق التي تم إجراؤها بمعرفة السلطة القضائية في الدولة المطلوب فيها اتخاذ بعض إجراءات التحقيق، وتتشابه إلى حد كبير مع نظام الندب (الإنابة القضائية الداخلية). وتتضمن الاتفاقيات الدولية المبرمة في هذا الشأن[30] على شروط وأساليب تنفيذ هذه الإنابة، وغالباً ما تتضمن شرطاً باستبعاد وتنفيذ الأحكام في المجال السياسي والضريبي والعسكري، أو إذا قدّرت الدولة المطلوب منها أن التنفيذ المطلوب من شأنه المساس بسيادة الدولة أو النظام العام، أو المصالح الأساسية، الأمر الذي يترك للدولة سلطة تقديرية لتنفيذ أو عدم تنفيذ ما يطلب إليها وذلك خشية قيام مسئوليتها دولياً عن إهمالها. وبالمقابل فإنه في ظل عدم وجود اتفاقية فإن الإنابة القضائية لا يمكن تنفيذها إلا إذا وافقت الدولة المطلوب إليها على ذلك وفقاً للإجراءات والشروط المنصوص عليها في القانون الداخلي لها.

*** صعوبة التعاون الدولي لمكافحة الجريمة الإلكترونية[31].**

لقد قدّمت شبكة المعلومات الدولية مجموعة متعددة ومعقدة من الاستخدامات في شتى الأنشطة السياحية الثقافية الاقتصادية والأمنية وحتى الشؤون العسكرية الأمر الذي زاد من حالات الاعتداء على خصوصية سرية المعلومات بقصد السرقة، التجسس، القرصنة، والتخريب. إذ أصبح هاجساً لكل دول العالم خاصة بسبب الانتشار الواسع لتبادل المعلومات المشفرة ذات الصلة بالتجسس السياسي أو العسكري أو الصناعي، أو أية نشاطات إجرامية. فنادى البعض بوجوب انشاء وحدات معينة تختص بمكافحة الجريمة المعلوماتية أسوةً بهيئات البحث الجنائي الوطنية والدولية (الإنتربول)، وذلك لإثبات الجريمة حال حدوثها وتحديد الأدلة المتعلقة بها وفاعليها، مما يعنى إيجاد صيغة مناسبة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة وتبادل الخبرات والمعلومات إزاء هذا الشكل من الجرائم وفاعليها ووسائل مكافحتها. وبالرغم من محاولات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، غير أن هناك صعوبات تمنع تحقيق ذلك ، ويمكن إيجاز ذلك في الأسباب التالية[32]:

أولاً: عدم وجود أنموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي، بسبب أن الأنظمة القانونية في بلدان العالم لم تتفق على صور محددة يندرج ضمنها ما يسمى بإساءة استخدام نظم المعلومات الواجب إتباعها، كما أنه ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه وهذا راجع إلى قصور التشريع نفسه في جميع بلدان العالم وعدم مجاراته السرعة في التقدم المعلوماتي وبالتالي الجريمة المعلوماتية.

وما تجدر الإشارة إليه أن هناك دول عربية لم تصدر قانوناً يتعلق بالجريمة المعلوماتية سواء ارتكبت عن طريق الكمبيوتر أو من خلال أجهزة أخرى، ولا يزال الخلاف قائماً حول أفضلية تعديل التشريعات العقابية لكي تستوعب نماذج الجريمة المعلوماتية أم أنه تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه الأنشطة من السلوك ويتم تجريمها، أم من الأفضل صدور تشريعات جديدة خاصة بالجريمة المعلوماتية، حتى أن الأمر لا يتوقف هنا بل يتعداه، إذ إن عدم اتفاق الأنظمة القانونية المختلفة على صورة موحدة للفعل الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على تنظيم أنفسهم وارتكاب جرائمهم دون التقيد بالحدود الجغرافية الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة.

ثانياً: لا يوجد معاهدات جماعية أو ثنائية بين الدول بحيث يعمل على التعاون المثمر في مجال تلك الجرائم، وحتى إذا وجدت فإنّ تلك المعاهدات تظل مقتصرة عن تحقيق الحماية المطلوبة في ظل التقدم الهائل لنظم وبرامج الحاسب الآلي وشبكة الإنترنت، وبالتالي تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك المشرع وسلطات أمن الدول، ويبرز الأثر السلبي في التعاون الدولي وهو ما حاولت الأمم المتحدة الاعتناء به وأيضا بعض البلدان الأوروبية.

ثالثاً: عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة المتعلقة بالجريمة المعلوماتية بين الدول المختلفة لاسيما فيما يرتبط بالتحقيق والحصول على الأدلة لاسيما وأن الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط أو التفتيش في نظام معلوماتي معين أمر في غاية الصعوبة اضافة إلى صعوبة العثور على الدليل ذاته.

رابعاً: إشكالية الاختصاص في الجرائم الإلكترونية كونها تعد من المشكلات التي تعرقل الحصول على الدليل فيها خاصة وأنها من أبرز الجرائم التي تثير مسألة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات لأن الجريمة قد تقع في مكان معين وتنتج أثارها في مكان آخر.

وما يلاحظ أن جل التشريعات الجنائية المطبقة حالياً في معظم دول العالم ترتكز على الصفة الإقليمية فيما يخص سريان قواعد الإجراءات الجنائية عن طريق السلطات غير الوطنية لذلك لا مناص من الاتفاقيات الثنائية والجماعية بين الدول لتسهيل تحقيق جرائم المعلوماتية، بالرغم من إبرام بعض الاتفاقيات إلا أنها لم تفِ بالغرض في حل مشكلات الاختصاص وتبادل الأدلة الجنائية وتسليم المجرمين. لذلك تظل الحاجة جد ماسة إلى تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم التكنولوجي وعصر المعلوماتية[33].

لاسيما إن إجراءات التحقيق في بيئة تكنولوجيا المعلومات وفقاً لما جاء في توصية المجلس الأوروبي رقم (95/13) تقتضي التدخل السريع لمد الإجراءات إلى أنظمة كمبيوتر قد تكون موجودة خارج الدولة، وحتى لا يمثل هذا الأمر اعتداء على سيادة دولة معينة أو على أحكام القانون الدولي يجب وضع قاعدة قانونية صريحة تسمح بهذا الإجراء. لذلك فإنّ الحاجة ملحة لاتفاقيات دولية تنظم طريقة اتخاذ تلك الإجراءات، كما يجب توافر إجراءات سريعة وملائمة ونظم اتصال تبيح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة محددة وهو ما يوجب تطوير اتفاقيات التعاون الدولي.

الخاتمة

نتيجةً للتطور السريع في تكنولوجيا المعلومات وتوسع ميادين استعمالها على كافة الاصعدة الأمنية والسياسية والتجارية والاقتصادية وحتى الشخصية، الأمر الذي أدى إلى ظهور العديد من الجرائم المعقدة في هذا المجال وتضاعف وتيرة الأنشطة الإجرامية المرتكبة في سياقها والتي باتت من أهم المعضلات الأمنية في الوقت الراهن، إذ تشكل تحدياً واضحاً للمجتمع الدولي ككل، ما دفع الأخير إلى تضافر الجهود في وضع حد لمثل هكذا جرائم ومحاولة السيطرة عليها.

التوصيات

- أعداد القوانين والأنظمة اللازمة المتعلقة بالمجال الإلكتروني وتطويرها بصورة مستمرة بما يتوافق مع طبيعة الجريمة الإلكترونية ولمواكبة التطور التكنولوجي المستمر.
- أنشاء وتفعيل أجهزة أمنية مختصة ومدرّبة على كيفية التعامل مع أجهزة الحاسوب والانترنت تتولى البحث والتحقيق في الجرائم الإلكترونية.
- حجب المواقع الإلكترونية المشبوهة التي تسعى إلى نشر الفكر المتطرف والإرهاب الإلكتروني، والعمل على تفعيل الدور الوقائي عن طريق نشر ثقافة توعوية تُعّرف المستخدمين مدى خطورة هذه الجرائم من خلال المواقع الالكترونية أو من خلال المؤسسات التعليمية.
- عقد اجتماعات دورية وتنظيم ورشات عمل للجهات المختصة في الدول تتبنّى التنسيق والتعاون وتوحيد الجهود فيما بينها للسيطرة ووضع حد لهذه الجرائم.
- إبرام الاتفاقيات الدولية لتوحيد وجهات النظر في مسألة تنازع الاختصاص القضائي بالنسبة لهذه الجرائم.

الهوامش.

(1) حسنين المحمدي، الجاسوسية لغة الخيانة، دار الفكر الجامعي، الإسكندرية 2007، ص 7.
(2) براهام يوست، تكنولوجيا التجسس (نظرة شاملة إلى وسائل التجسس الحديثة ما هي؟ وكيف تعمل ومن يستعملها؟ من المسدس اليدوي إلى القمر الصناعي التجسسي (KH – 1)، ترجمة على جواد حسين، الدار العربية للموسوعات، الطبعة الأولى، بيروت 1999، ص 4.
(3) عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007، ص 29.
(4) عبد الإله محمد النوايسة، وممدوح حسن العدوان، جرائم التجسس الإلكتروني في التشريع الأردني (دراسة تحليلية)، دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد (46)، العدد (1)، ملحق (1)، 2019، ص 468.
(5) سعيد بن سالم البادي، زايد بن حمد الجنيبي، يوسف الشيخ يوسف حمزة، محمود أحمد العطاء، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى - سلطنة عمان 2016، ص 58، فتوح عبد الله الشاذلي، المواجهة التشريعية للجرائم المستحدثة (غسيل الأموال، الإرهاب) بحث مقدم لمؤتمر الأمن والسلامة الذي عقدته وزارة الداخلية بدولة الإمارات العربية المتحدة، أبو ظبي في الفترة من 5-8 تشرين الأول/أكتوبر 2003، ص 1.
(6) راجع في هذا الصدد: عبد الفتاح مراد، قانون مكافحة غسل الأموال ولائحته التنفيذية والقوانين المكملة له، منشأة المعارف، الإسكندرية 2008 ص 42، 43.

(7) انظر: محمد الشناوي، استراتيجية مكافحة جرائم النصب المستحدثة (الإنترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة)، الطبعة الأولى، دار البيان للطباعة والنشر، القاهرة 2006، ص 81، 84، 61.
(8) عبد الفتاح مراد، قانون مكافحة غسل الأموال ولائحته التنفيذية والقوانين المكملة له، مرجع سابق، ص 242.
(9) للاطلاع على هذه الاتفاقية أنظر: محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية "جرائم الكمبيوتر والإنترنت"، المكتب العربي الحديث، الإسكندرية بدون سنة نشر، ص12 وما بعدها، وكذلك عبد الفتاح مراد، قانون مكافحة غسل الأموال ولائحته التنفيذية والقوانين المكملة له، المرجع السابق، ص 280 وما يليها.
()10 الأونيسترال: وهي هيئة قانونية ذات عضوية عالمية متخصصة في إصلاح القانون التجاري على النطاق العالمي منذ ما يزيد على 50 سنة، وتتمثل مهمة الأونيسترال في عصرنة ومواءمة القواعد المتعلقة بالأعمال التجارية الدولية (لجنة الأمم المتحدة للقانون التجاري الدولي).
(11) عبد الفتاح مراد، قانون مكافحة غسل الأموال ولائحته التنفيذية والقوانين المكملة له، مرجع سابق ص 244.
وكذلك: محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 14.
- منير محمد الجنبيهي وممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، مرجع سابق، ص 111- 115.
- كذلك شريف محمد غنام، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، دار الجامعة الجديدة 2007، ص 194.
()12 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.
(13) سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دارسة مقارنة، الدار الجماهيرية للنشر والتوزيع والاعلان، ليبيا 2000، ص 425، ينظر أيضاً: ماجد إبراهيم علي، قانون العلاقات الدولية، دراسة في إطار النظام القانوني الدولي والتعاون الدولي الأمني، مكتبة مركز بحوث الشرطة، القاهرة 2010، ص 374.
(14) أحمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، بحث منشور بمجلة الفكر الشرطي، المجلد (17)، العدد (3)، 2008، ص 153.
(15) حسنين إبراهيم صالح عبيد، القضاء الجنائي الدولي، الطبعة الأولى، دار النهضة العربية، القاهرة 1977، ص 140.
ينظر أيضاً: حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دارسة مقارنة، رسالة دكتوراه، حقوق عين شمس، 2007، ص 501.
(16) عبد الرحمن فتحي سمحان، تسليم المجرمين في ظل قواعد القانوني الدولي، دار النهضة العربية، 2012، ص 527.
(17) المادة (23) من القسم الأول من الفصل الثالث من الاتفاقية الاوربية حول مكافحة الجرائم المعلوماتية لسنة 2001 " على الأطراف أن تتعاون مع بعضها البعض، وفقاً لأحكام هذا الفصل، ومن خلال تطبيق الأدوات الدولية ذات العلاقة حول التعاون الدولي في الشؤون الجنائية، والإجراءات المتفق عليها على أساس التشريع الموحد أو المتبادل، والقوانين المحلية إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة وبيانات الحاسوب أو لجمع الأدلة بشكلها الإلكتروني في جريمة جنائية". ومن صور التعاون الدولي في مجال مكافحة الجرائم الالكترونية قيام الشرطة الدولية (الانتربول) في المانيا بإبلاغ النيابة العامة اللبنانية في قضية يحقّق فيها القضاء اللبناني بتهمة شخص قام بأرسال صور إباحية إلى قاصرة دون العشر سنوات من موقعه الإلكتروني وهذه ما يوكد وجود تعاون إلى حدٍ ما بين الدول لمكافحة مثل هكذا جرائم وتبادل البيانات والمعلومات حول المجرم والجريمة. ينظر في ذلك: حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة 2009، ص328.
(18) المادة الأولى من الباب الأول من اتفاقية الرياض العربية للتعاون القضائي لسنة 1983 والتي نصت على "تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل المعلومات المتعلقة بالتنظيم القضائي، وتعمل على اتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية والتنسيق بين الأنظمة القضائية لدى الأطراف المتعاقدة حسبما تقتضيه الظروف الخاصة بكل منها".
(19) المادة الأولى من الفصل الأول من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.
(20) سامع أحمد موسى، الجوانب الاجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة الاسكندرية 2010، ص 502.
(21) والتي اعتمدت بواسطة الجمعية العامة للأمم المتحدة بالقرار رقم 118/45 الصادر في 14 كانون الأول/ ديسمبر 1990.
(22) والتي تم التوقيع عليها في مدينة باليرمو عام 2000، وذلك بموجب قرار الجمعية العامة رقم 25/55، وقد وقعت عليها وعلى البروتوكول المكمل لها 88 دولة و 117 هيئة.
(23) سامع أحمد موسى، الجوانب الاجرائية للحماية الجنائية لشبكة الانترنت، مرجع سابق، ص 508 وما بعدها.
(24) ينظر الرابط التالي: CB2015_AR.pdf (stl-tsl.org)

(25) عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية 2000، ص 102. وينظر: حازم الحاروني، الإنابة القضائية الدولية، المجلة الجنائية القومية، القاهرة، مجلد 31، عدد 2، يوليو 1988، ص 20، عبد الرحيم صدقي، التعاون العقابي الدولي في الفكر المعاصر، مجلة القانون والاقتصاد، السنة 53، 1983، ص 1 وما بعدها، أمين عبد الرحمن محمد عباس، الإنابة القضائية، رسالة دكتوراه، حقوق الإسكندرية، 2011، ص 237 وما بعدها، إدوار عيد، الإنابات والإعلانات القضائية وفقاً لقواعد القانون الدولي الخاص واتفاقية الدول العربية في عام 1953، معهد البحوث والدراسات العربية، جامعة الدول العربية، 1969م، ص9.

(26) ذات المعنى طارق سرور، الاختصاص الجنائي العالمي، دار النهضة العربية، القاهرة ،الطبعة الأولى، 2006، ص5.

(27) المعيار المعرب والجامع المغرب من فتاوى أهل إفريقية والأندلس والمغرب، لأبي العباس أحمد بن يحيى الونشريسي، ج 10، ص 12 وما بعدها، طبعة وزارة الأوقاف، المغرب 1981.

(28) ينظر: شرح الزرقاني على مختصر سيدي خليل، الجزء السابع، طبعة دار الفكر بيروت، 2002، ص 151، مغني المحتاج، شمس الدين الشربيني، الجزء الرابع، طبعة دار إحياء التراث العربي، 1933، ص 409، كشاف القناع على متن الإقناع، الجزء السادس، طبعة دار الفكر 1982، ص 362. مشار إليه لدى عادل عبدالعال إبراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015، ص211.

(29) منصور محمد الجندي، أحكام الإنابة القضائية في الفقه الإسلامي والقانون الدولي الخاص، دراسة مقارنة، رسالة دكتوراه، كلية الشريعة والقانون بالقاهرة، جامعة الأزهر، 1999، ص 26.

(30) ومن الاتفاقيات التي أبرمت في مجال الإنابة القضائية تلك التي عقدتها فرنسا مع الجزائر في 1962/8/28، ومع ألمانيا في أكتوبر 1974، ومع مصر في 1982/3/15، والاتفاقية الأوربية للتعاون القضائي في المواد الجنائية عام 1962، والاتفاقية المبرمة بين دول الجامعة العربية في 9 حزيران/يونيو 1953، ووافقت عليها مصر بالقانون رقم 30 لسنة 1954.

للمزيد ينظر: عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية مرجع سابق، ص 85، حازم مختار الحاروني، نطاق تطبيق القاضي الجنائي للقانون الجنائي، رسالة دكتوراه، حقوق القاهرة، 1987، ص 519.

(31) سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص 103.

(32) عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 188.

(33) عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 192.

المصادر والمراجع:

1. حسنين المحمدي، الجاسوسية لغة الخيانة، دار الفكر الجامعي، الإسكندرية 2007.

2. براهام يوست، تكنولوجيا التجسس (نظرة شاملة إلى وسائل التجسس الحديثة ما هي؟ وكيف تعمل ومن يستعملها؟ من المسدس اليدوي إلى القمر الصناعي التجسسي (KH – 1)، ترجمة على جواد حسين، الدار العربية للموسوعات، الطبعة الأولى، بيروت 1999.

3. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007.

4. عبد الإله محمد النوايسة، وممدوح حسن العدوان، جرائم التجسس الإلكتروني في التشريع الأردني (دراسة تحليلية)، دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد (46)، العدد (1)، ملحق (1)، 2019.

5. سعيد بن سالم البادي، زايد بن حمد الجنيبي، يوسف الشيخ يوسف حمزة، محمود أحمد العطاء، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى - سلطنة عمان 2016.

6. فتوح عبد الله الشاذلي، المواجهة التشريعية للجرائم المستحدثة (غسيل الأموال، الإرهاب) بحث مقدم لمؤتمر الأمن والسلامة الذي عقدته وزارة الداخلية بدولة الإمارات العربية المتحدة، أبو ظبي في الفترة من 5-8 تشرين الأول/أكتوبر 2003.

7. عبد الفتاح مراد، قانون مكافحة غسل الأموال ولائحته التنفيذية والقوانين المكملة له، منشأة المعارف، الإسكندرية 2008.

8. محمد الشناوي، استراتيجية مكافحة جرائم النصب المستحدثة (الإنترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة)، الطبعة الأولى، دار البيان للطباعة والنشر، القاهرة 2006.

9. محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية "جرائم الكمبيوتر والإنترنت"، المكتب العربي الحديث، الإسكندرية بدون سنة نشر.

10. شريف محمد غنام، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، دار الجامعة الجديدة 2007.

11. سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دارسة مقارنة، الدار الجماهيرية للنشر والتوزيع والاعلان، ليبيا 2000.
12. ماجد إبراهيم علي، قانون العلاقات الدولية، دراسة في إطار النظام القانوني الدولي والتعاون الدولي الأمني، مكتبة مركز بحوث الشرطة، القاهرة 2010.
13. أحمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، بحث منشور بمجلة الفكر الشرطي، المجلد (17)، العدد (3)، 2008.
14. حسنين إبراهيم صالح عبيد، القضاء الجنائي الدولي، الطبعة الأولى، دار النهضة العربية، القاهرة 1977.
15. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دارسة مقارنة، رسالة دكتوراه، حقوق عين شمس، 2007.
16. عبد الرحمن فتحي سمحان، تسليم المجرمين في ظل قواعد القانوني الدولي، دار النهضة العربية، 2012.
17. الاتفاقية الاوربية حول مكافحة الجرائم المعلوماتية لسنة 2001.
18. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة 2009.
19. اتفاقية الرياض العربية للتعاون القضائي لسنة 1983.
20. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.
21. سامع أحمد موسى، الجوانب الاجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة الاسكندرية 2010.
22. قرار الجمعية العامة للأمم المتحدة رقم 118/45 الصادر في 14 كانون الأول/ ديسمبر 1990.
23. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية 2000.
24. حازم الحاروني، الإنابة القضائية الدولية، المجلة الجنائية القومية، القاهرة، مجلد 31، عدد 2، يوليو 1988.
25. عبد الرحيم صدقي، التعاون العقابي الدولي في الفكر المعاصر، مجلة القانون والاقتصاد، السنة 53، 1983.
26. أمين عبد الرحمن محمد عباس، الإنابة القضائية، رسالة دكتوراه، حقوق الإسكندرية، 2011.
27. طارق سرور، الاختصاص الجنائي العالمي، دار النهضة العربية، القاهرة، الطبعة الأولى، 2006.
28. المعيار المعرب والجامع المغرب من فتاوى أهل إفريقية والأندلس والمغرب، لأبي العباس أحمد بن يحيى الونشريسي، ج 10، طبعة وزارة الأوقاف، المغرب 1981.
29. شرح الزرقاني على مختصر سيدي خليل، الجزء السابع، طبعة دار الفكر بيروت، 2002.
30. مغني المحتاج، شمس الدين الشربيني، الجزء الرابع، طبعة دار إحياء التراث العربي، 1933.
31. عادل عبدالعال إبراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015.
32. منصور محمد الجندي، أحكام الإنابة القضائية في الفقه الإسلامي والقانون الدولي الخاص، دراسة مقارنة، رسالة دكتوراه، كلية الشريعة والقانون بالقاهرة، جامعة الأزهر، 1999.
33. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007.