التعاون القضائى الدولى
فى مجال الجرائم الإلكترونية

هند نجيب(*)

يعتبر اختراع جهاز الحاسب الآلى واتصاله بشبكة المعلومات الدولية (الإنترنت) من أهم إنجازات العلم فى العصر الحديث والتى أسهمت بدور كبير فى بلورة فكرة العولمة وتقارب الثقافات وفتح الحدود أمام الأفراد والجماعات والدول بلا قيود أو حواجز حدودية أو جغرافية، بيد أن بعض محترفى هذه التقنية الحديثة وجدوا فيها وسيلة بارعة لارتكاب أنماط جديدة من الجرائم يصعب اكتشافها أو ضبطها أو الحصول منها على أدلة قاطعة بنسبة هذه الأفعال إلى مرتكبيها.

مقدمة

فى عصر التقنية، وثورة الاتصالات الحديثة تعقدت الجريمة، وتنوعت أساليبها مستفيدة من التطور التقنى فى كل مناحى الحياة، حيث وظف المجرمون هذه المستحدثات التقنية الحديثة فى تطوير أساليبهم، بل حتى التقنية ذاتها لم تسلم من الجريمة فمنذ بداياتها ظهر معها ما يعرف بجرائم التقنية، أو الجرائم الإلكترونية.

وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم، التى لم تعد تتمركز فى دولة معينة، ولا توجه لمجتمع

---

* مدرس القانون الجنائى المساعد، المركز القومى للبحوث الاجتماعية والجنائية.

بعينه بل أصبحت تعبر الحدود وهو ما أظهر ضرورة وجود تعاون قضائى على المستوى الدولى فى مجال هذه الجرائم.

ويهدف البحث إلى إلقاء الضوء على جهود التعاون الدولى فى مواجهة الجرائم الإلكترونية وصور هذا التعاون، وكذلك الوقوف على صعوبات التعاون الدولى فى مواجهة الجرائم الإلكترونية وسبل مواجهتها.

وسوف نتناول هذا الموضوع كما يلى:

أولًا: جهود التعاون الدولى فى مواجهة الجرائم الإلكترونية وصوره

الجرائم الإلكترونية تتميز بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها. ليس هذا فحسب بل اتصفت بالعالمية وبأنها عابرة للحدود، وهذا أمر طبيعى خاصة إذا ما علمنا أن شبكة المعلومات الدولية ذاتها لا تعرف الحدود أى أنها ذات طبيعة عالمية، ويدرك الباحث فى اتجاهات التشريع المقارن، فيما يتعلق بالجرائم الإلكترونية، أنها جاءت متوازية مع اتجاهات عمل المنظمات والهيئات الإقليمية والدولية، ولهذا بدأ تزايد الجهود الدولية لتحقيق تعاون فيما بينها لمواجهة هذه الجرائم، والذى اتخذ العديد من الصور.

وسوف نتناول فيما يلى جهود التعاون الدولى فى مواجهة الجرائم الإلكترونية ثم صور التعاون الدولى لمواجهة هذه النوعية من الجرائم.

١-جهود التعاون الدولى فى مواجهة الجرائم الإلكترونية

ستظل تشريعات الجرائم الإلكترونية فى أية دولة غير ذات أثر فى ظل إغفال الحاجة الملحة للتحرك الدولى الشامل لمكافحة خطر هذه الجرائم وحل مشكلات

الاختصاص وتنازع القوانين ومشكلات صلاحيات جهات التحقيق الوطنية خارج الحدود وتنظيم أنشطة الملاحقة ضمن تعاون دولى متوازن وفاعل.

ومن أجل ذلك اجتمع فى موسكو وزراء العدل والداخلية للدول الثمانى الكبار فى شهر أكتوبر ١٩٩٩، وطلبوا من ممثليهم وضع خيارات وحلول عملية تسمح بكشف ومتابعة الاتصالات الإلكترونية الدولية فى إطار التحقيقات الجنائية، وقد صدر عنهم التصريح التالى: "بغية التأكد من أننا جميعًا نستطيع أن نحدد مكان وهوية المجرمين الذين يستخدمون الاتصالات الإلكترونية لأهداف غير مشروعة، يجب علينا أن نزيد قدراتنا على اقتفاء أثر وكشف هذه الاتصالات أثناء وبعد إجرائها، حتى وإن كانت تلك الاتصالات تمر عبر عدة دول".

ولما كانت الإجراءات الحالية تتسم بالبطء وتتم فى إطار تعاون ثنائى فقط بدلًا من أن تهدف إلى مواجهة الجرائم بصفة مطلقة، لذلك يجب أن يتعاون الجميع مباشرة من أجل مكافحتها وإيجاد حلول سريعة وحديثة".

وفى مايو عام ٢٠٠٠ وضع الخبراء أيديهم على بداية الحلول والمقترحات، وفى يوليو عام ٢٠٠٠ وافق رؤساء الدول الثمان الكبار خلال اجتماعهم فى أوكيناوا باليابان على بدء الأعمال المقترحة، وفى فبراير ٢٠٠١ طالب وزراء العدل والداخلية للدول الثمانى الكبار من الخبراء فى الاجتماع الذى تم فى ميلان، وضع توصيات عن اقتفاء أثر المجرمين على شبكات المعلومات، مع الأخذ فى الاعتبار احترام الحقوق الأساسية مثل حماية المعلومات الشخصية والحريات الفردية، وفى موسكو طلب الوزراء مرة أخرى

من الخبراء أن يستشيروا ممثلى الصناعات المتطورة فى هذا المجال حول الملاحقة وبعض المسائل الأخرى المتصلة بالجريمة ذات التقنية العالية. ثم تتابعت المؤتمرات وورش العمل فى باريس وبرلين وطوكيو والتى شارك بها أكثر من مائة ممثل عن شركات التقنية العالية فى العالم أجمع.

ثم جاءت أحداث ١١ سبتمبر ٢٠٠١ فجعلت هذا العمل أكثر إلحاحًا وسرعة، إذ أن الإرهابيين يمكنهم استخدام مواقع الإنترنت والرسائل الإلكترونية والتليفونات المحمولة وبعض الوسائل التقنية الأخرى فى الاتصالات المتطورة، وذلك لعمل مخططاتهم ونشر ونقل المعلومات إلى مختلف القارات، بحيث يصبح كشفها أمرًا صعبًا إن لم يكن مستحيلًا، وفى ٢٠٠١/١١/٢٣ تم توقيع الاتفاقية الأوروبية لمكافحة جرائم الإنترنت.

وسوف نتناول الجهود الدولية للتعاون الدولى فى مجال الجرائم الإلكترونية على النحو التالى:

أ - جهود هيئة الأمم المتحدة.

ب - الجهـــود الإقليميـــــة.

أ - جهود هيئة الأمم المتحدة

بذلت الأمم المتحدة ولا تزال تبذل جهودها فى مجال مكافحة الجرائم الإلكترونية، وذلك لما تمثله هذه الجرائم من أضرار بالغة وخسائر فادحة، وإيمانا منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية فى ضوء الطابع والأبعاد الدولية للجرائم الإلكترونية والجرائم المتعلقة بها، ويفترض

التعاون الدولى وجود فهم مشترك لهذه الظاهرة والحلول المقترحة لها، إلا أن هناك مشكلات عديدة تعترض التعاون الدولى فى مجال مكافحة الجرائم الإلكترونية[١].

ولقد حظيت الجرائم الإلكترونية باهتمام مؤتمرات الأمم المتحدة لمنع الجريمة ومعاملة المجرمين حيث صدر قرار بالجرائم المتعلقة بالحاسب، وأشار القرار إلى أن الإجراء الدولى لمواجهة جرائم الحاسب يتطلب من الدول الأعضاء اتخاذ عدة إجراءات تتلخص فى[٢]:

١ - تحديث القوانين وأغراضها الجنائية بما فى ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية (التحقيق وقبول الأدلة) على نحو ملائم وإدخال التعديلات إذا اقتضت الضرورة.

٢ - مصادرة العائد والأصول من الأنشطة غير المشروعة.

٣ - اتخاذ أى تدابير لازمة للأمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.

٤ - رفع الوعى لدى الجماهير والقضاة والعاملين على مكافحة هذا النوع من الجرائم بأهمية مكافحة هذه الجرائم ومحاكمة مرتكبيها.

٥ - التعاون مع المنظمات المهتمة بهذا الموضوع ووضع وتدريس الآداب المتبعة فى استخدام الحاسب ضمن المناهج الدراسية.

٦ - حماية مصالح وحقوق ضحايا الجرائم الإلكترونية[٣].

ومع استمرار الجرائم الإلكترونية، وما تثيره من مشكلات عقد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات فى البرازيل عام ١٩٩٤حيث

أوصى بأن تتضمن قائمة الحد الأدنى للأفعال المتعين تجريمها باعتبارها من الجرائم الإلكترونية، والتى تضمنت ست جرائم رئيسية: الاحتيال أو الغش المرتبط بالحاسب، تزوير الكمبيوتر أو التزوير المعلوماتى، الإضرار بالبيانات والإضرار بالبرامج، تخريب الحاسب، الدخول غير المصرح به، وفصل القرار مشتملات كل جريمة من هذه الجرائم.

وبتزايد الجرائم الإلكترونية وما تثيره من مشكلات، دفع ذلك منظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية سنة ٢٠٠٠، حيث أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول فى مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة إلى الدور الذى يمكن أن تقوم به كل من منظمة الأمم المتحدة والمنظمات الإقليمية(٤).

وعقدت كذلك منظمة الأمم المتحدة المؤتمر الثانى عشر لمنع الجريمة والعدالة الجنائية بالبرازيل أبريل ٢٠١٠، حيث ناقشت فيه الدول التطورات الأخيرة فى استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة فى مكافحة الجريمة بما فى ذلك الجرائم الإلكترونية، حيث احتل هذا النوع من الجرائم موقعًا بارزًا فى جدول أعمال المؤتمر وذلك تأكيدًا على خطورتها والتحديات التى تطرحها، وقد دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومى دولى مفتوح العضوية من أجل دراسة شاملة لمشكلة الجريمة الإلكترونية وتدابير التصدى لها، ولقد ركز فريق الخبراء دراسته لهذا الموضوع على ظاهرة الجريمة الإلكترونية بالتطرق للعديد من

الموضوعات ومنها: تحليل ظاهرة الجريمة الإلكترونية، جمع المعلومات والإحصائيات المتعلقة بالجريمة الإلكترونية، تحديات الجريمة الإلكترونية، مدى مواءمة التشريعات للظاهرة الإجرامية الإلكترونية، النص على الجرائم الإلكترونية، إجراءات التحقيق، التعاون الدولى، الأدلة الإلكترونية، وغيرها.

وقد دأبت منظمة الأمم المتحدة استمرارًا لتلك الجهود المبذولة لمكافحة الجرائم الإلكترونية على عقد عدة مؤتمرات، فلم تكن المؤتمرات السالفة الذكر هى الوحيدة، حيث عمدت اللجنة الاقتصادية والاجتماعية لغربى آسيا التابعة للمجلس الاقتصادى والاجتماعى وذلك تحت غطاء منظمة الأمم المتحدة على عقد ورشة عمل حول التشريعات الإلكترونية وتطبيقها فى منطقة الإسكوا عام ٢٠٠٨[٥]، بالإضافة إلى تلك المؤتمرات التى عقدتها أطراف فى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المنعقد بفيينا، أكتوبر ٢٠١٠، حيث بين المؤتمر فهرس الأمثلة المتعلقة بتسليم المجرمين وتبادل المساعدة القانونية وأشكال أخرى من التعاون الدولى فى المسائل القانونية، استنادا إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[٦].

نجد فى المؤتمر نفسه مشاورات الخبراء بشأن استخدام الاتفاقية من أجل التصدى للأشكال المستجدة من الجريمة[٧].

كما لا يمكننا إغفال مجهودات لجنة حقوق الطفل التابعة لمنظمة الأمم المتحدة التى عقدت اتفاقية خاصة بحقوق الطفل وذلك من أجل النظر فى الجرائم التى ترتكب فى حق الطفولة منها استغلالهم فى المواد الإباحية عبر الإنترنت[٨].

واستمرارًا للجهود المبذولة لمكافحة هذا النوع من الجرائم أصدرت الأمم المتحدة دليلًا عامًا إرشاديًا حول الجرائم الإلكترونية ويتم تعديله وتنقيحه كل فترة، تضمن تحديدًا للمشكلة وتعريفًا بالجرائم الإلكترونية، كما وضع تحديدًا للحد الأدنى من هذه الجرائم إضافة إلى العديد من المحتويات التى تتعلق بهذا النوع من الجرائم.

إضافة إلى جهود الأمم المتحدة فى مكافحة الجرائم الإلكترونية اهتمت منظمة التعاون الاقتصادى والتنمية بالعمل على مكافحة هذا النوع من الجرائم وأصدرت المنظمة العديد من التوصيات تتعلق بالتدابير والإجراءات التى ينبغى اتخاذها لحماية نظم المعلومات[٩]، وتهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادى وتناغم التطور الاقتصادى مع التنمية الاجتماعية.

بدأت هذه المنظمة الاهتمام بالجرائم المرتكبة عبر الإنترنت منذ عام ١٩٧٨، حيث وضعت مجموعة أدلة وقواعد إرشادية تتصل بتقنية المعلومات ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التى تم تبنيها من قبل مجلس المنظمة فى عام ١٩٨٠ مع التوصية للأعضاء بالالتزام بها.

أصدرت هذه المنظمة تقريرًا عام ١٩٨٣، بعنوان الجرائم المرتبطة بالحاسب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة فى عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى لأفعال سوء استخدام الحاسب التى يجب على الدول أن تجرمها وتفرض لها عقوبات فى قوانينها، ومن أمثلة هذه الأفعال الاستخدام أو

الدخول غير المصرح به لنظام الحاسب الآلى، إتلاف أو تخريب ما يحويه الحاسب من بيانات.

وقد أوصت اللجنة المكلفة المصدرة للتقرير إلى وجوب أن تمتد الحماية إلى صورة أخرى لإساءة استخدام الحاسب، منها الاتجار فى الأسرار والاختراق غير المصرح به، وفى عام ١٩٩٢ وضعت المنظمة توصيات إرشادية خاصة بأمن أنظمة المعلومات، وقد تمخضت جهود المنظمة من أجل معالجة الجرائم الإلكترونية بالتوصية بضرورة أن تعطى التشريعات الجنائية للدول الأعضاء الأفعال الآتية:

١- التلاعب فى البيانات المعالجة آليًا بما فى ذلك محوها.

٢- التجسس المعلوماتى ويندرج تحته الحصول، أو الاقتناء أو الاستعمال غير المشروع للمعطيات.

٣- التخريب المعلوماتى ويندرج تحته الاستخدام غير المشروع، أو سرقة وقت الحاسب.

٤- قرصنة البرامج.

٥- الدخول غير المشروع على البيانات أو نقلها.

٦- اعتراض استخدام المعطيات أو نقلها[١٠].

ب- الجهود الإقليمية

إضافة إلى الجهود الدولية التى تبذلها الأمم المتحدة هنالك جهود إقليمية تتمثل فى الجهود التى يبذلها المجلس الأوروبى والاتحاد الأوروبى[١١] والتى تُوجت

بصدور اتفاقية بودابست لمكافحة الجرائم الإلكترونية ٢٠٠١، وتتلخص أهم أهدافها فى السعى لتحقيق وحدة التدابير التشريعية بين الدول الأوربية والدول المنضمة إلى الاتفاقية من غير الدول الأوروبية، والتأكيد على أهمية التعاون الإقليمى والدولى فى ميدان مكافحة الجرائم الإلكترونية، وتحقيق التوازن بين حقوق الإنسان والإجراءات المتخذة لمواجهة الجرائم الإلكترونية، حيث تقدم هذه الاتفاقية دليلًا إرشاديًا لتطوير مثل هذا التشريع[١٢].

كما تم إنشاء مركز الشكاوى الخاص بجرائم الإنترنت فى العالم الذى يعتبر من أهم المؤسسات لمكافحة الجرائم الإلكترونية والإنترنت، والذى يتولى التحقيق فى جرائم الإنترنت على مستوى العالم، ومركز الشكاوى الخاصة بجرائم الإنترنت (IC3) هو كناية عن نظام تبليغ وإحالة لشكاوى الناس فى الولايات المتحدة والعالم أجمع ضد جرائم الإنترنت[١٣]، والمركز يقدم الخدمة بواسطة استمارة للشكاوى مرسلة على الإنترنت، وبواسطة فريق من الموظفين والمحللين، وقد نشأ مركز الشكاوى الخاصة بجرائم الإنترنت كمفهوم سنة ١٩٩٨، حيث تم الإدراك بأن الجريمة بدأت تدخل عالم الإنترنت، وذلك عقب بدء إجراء الأعمال التجارية والمالية عبر الإنترنت، ولأن مكتب التحقيقات الفيدرالى أراد أن يكون قادرًا على تعقب مثل هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بهذه الجرائم.

وقد تم تأسيس أول مكتب للمركز سنة ١٩٩٩ فى مورغانتاون بولاية وست فرجينيا، وسمّى مركز شكاوى الاحتيال على الإنترنت؛ وكان المكتب عبارة عن شراكة بين مكتب التحقيقات الفيدرالى والمركز القومى لجرائم موظفى

المكاتب، وهذا الأخير مؤسسة لا تبغى الربح متعاقدة مع وزارة العدل الأميركية مهمتها الأساسية تحسين قدرات موظفى أجهزة تطبيق القانون، على صعيد الولاية والصعيد المحلى، واكتشاف جرائم الإنترنت أو الجرائم الاقتصادية ومعالجة أمرها.

وفى العام ٢٠٠٢، وبغية توضيح نطاق جرائم الإنترنت التى يجرى تحليلها، بدءًا من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية التى أخذت تظهر على الإنترنت، أعيدت تسمية المركز وأطلق عليه اسم مركز الشكاوى الخاصة بجرائم الإنترنت، ودعا مكتب التحقيقات الفيدرالى وكالات فيدرالية أخرى، مثل مكتب التفتيش البريدى وهيئة التجارة الفيدرالية والشرطة السرية وغيرها، للمساعدة فى تزويد المركز بالموظفين وللمساهمة فى العمل ضد جرائم الإنترنت.

وبإمكان الناس من جميع أنحاء العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بجرائم على الإنترنت (http://www.ic3.gov). ويطلب الموقع اسم الشخص وعنوانه البريدى ورقم هاتفه؛ إضافة إلى اسم وعنوان ورقم هاتف والعنوان الإلكترونى، إذا كانت متوفرة للشخص أو المنظمة المشتبه بقيامه بنشاط إجرامى؛ علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب اعتقاد مقدم الشكوى ووقت وقوعها وسبب اعتقاده بوقوعها؛ بالإضافة إلى أى معلومات أخرى تدعم الشكوى، ويساعد مركز الشكاوى الخاصة بجرائم الإنترنت أحيانًا وكالات تطبيق القانون من خلال إجراء الأبحاث وإعداد ملف القضية الأولى. وقد وجد محققو المركز، خلال السنتين والنصف الأُوَل من عمر

المشروع، وعلى الرغم من جهود إعداد القضايا وإحالتها بسرعة إلى وكالات تطبيق القوانين، فإن فرق العمل الخاصة بمكافحة جرائم الإنترنت لم تكن جميعًا مجهزة لمتابعة هذه الجرائم أو التحقيق فيها بسرعة. وقد لا تملك بعض فرق العمل هذه القدرة على القيام بعمليات سرية، أو قد لا تملك التجهيزات اللازمة لاقتفاء الآثار الرقمية للأدلة الجرمية التى يحولها إليها مركز الشكاوى. لذلك، أصبح من المهم جدًا بالنسبة لمركز الشكاوى أن يطور ويتعقب آثار الجرائم ثم يتوصل إلى إعداد ملف القضية الأولى.

فقد يتعرف مركز الشكاوى الخاصة بجرائم الإنترنت على هوية ١٠٠ ضحية، ويقرر أنه يبدو أن النشاط الإجرامى صادر عن جهاز مقدم خدمات كمبيوتر فى كندا، مثلًا، لكن ذلك الجهاز قد يكون مجرد كمبيوتر تم التسلل إليه. وقد يكون ما حدث هو أن المجرمين يستخدمون هذه الآلة "كنقطة انطلاق وهمية" لإخفاء مكان تواجدهم الحقيقى. لذا فإنه من المفيد بالنسبة لمحللى مركز الشكاوى أن يعرفوا المزيد عن "نقطة الانطلاق الوهمية"؛ فقد تكون هناك مجموعة فى تكساس، أو إفريقيا الغربية، أو رومانيا، تستخدم جهاز مقدم خدمات الإنترنت فى كندا لجمع المعلومات عن الضحايا المحتملين.

تحظى وحدة مبادرات جرائم الإنترنت (CIRFU) بالدعم من بعض أكبر الشركات التى يستهدفها مجرمو الفضاء السيبرانى، أى المنظمات والتجار الذين يعملون فى مجال الإنترنت مثل مايكروسوفت، وأميركا أونلاين، وجمعيات هذه الصناعة التجارية مثل اتحاد برامج كمبيوتر الأعمال، وجمعية التسويق المباشر، ومجلس مخاطر التجار، وصناعة الخدمات المالية، وغيرها. وقد

انضم محققون ومحللون من هذه المنظمات، يعمل الكثير منهم على قضايا جرائم الإنترنت، إلى وحدة المبادرات المذكورة لتحديد اتجاهات وتكنولوجيات جرائم الإنترنت، ولجمع المعلومات لإعداد ملفات قضايا قانونية ذات شأن، ولمساعدة وكالات تطبيق القانون فى جميع أنحاء العالم على اكتشاف جرائم الإنترنت ومحاربتها.

يعمل مركز الشكاوى الخاصة بجرائم الإنترنت أيضًا مع منظمات دولية مثل هيئة الجرائم الاقتصادية والمالية (EFCC) فى نيجيريا، حيث توجد مستويات عالية من الجرائم الاقتصادية والمالية كتبييض الأموال والاحتيال بقبض أموال مسبقة لمشاريع وهمية، أو ما يسمى احتيال ٤١٩، مما كانت له عواقب سلبية شديدة على ذلك البلد.

ويعمل مركز الشكاوى عن كثب أيضًا مع المنظمة الكندية المسماة "الإبلاغ عن الجرائم الاقتصادية على خط الإنترنت (RECOL)" ويدير هذه المنظمة المركز القومى للجرائم المكتبية فى كندا، وتدعمها شرطة الخيالة الملكية الكندية، ووكالات أخرى. وتنطوى منظمة الإبلاغ عن جرائم الإنترنت على شراكة متكاملة بين وكالات تطبيق القوانين الدولية والفيدرالية والإقليمية من جهة، وبين المسئولين عن وضع وتطبيق أنظمة العمل والمنظمات التجارية الخاصة التى لها مصلحة تحقيقية مشروعة فى تلقى شكاوى الجرائم الاقتصادية، من جهة أخرى.

ويعمل مركز الشكاوى الخاصة بجرائم الإنترنت مع المسئولين عن تطبيق القانون فى بلدان عديدة، بينها أستراليا والمملكة المتحدة. كما يحضر

ممثلو مركز الشكاوى أيضًا اجتماعات دورية للمجموعة الفرعية حول جرائم التكنولوجيا المتقدمة التابعة لمجموعة الثمانى (كندا، فرنسا، ألمانيا، إيطاليا، اليابان، روسيا والمملكة المتحدة والولايات المتحدة). ويعمل قسم من هذه المجموعة الفرعية على محاربة جرائم الإنترنت وتعزيز التحقيقات بشأنها[١٤].

وكذلك هناك التحالف الدولى لحماية الأمن الإلكترونى (ICSPA)، هذا التحالف عبارة عن منظمة عالمية غير ربحية أنشئت لتوجيه التمويل والخبرات والمساعدة المباشرة فى تنفيذ القانون لمكافحة الجريمة الإلكترونية فى الأسواق المحلية والدولية على حد سواء، وتتمثل مهمة التحالف الدولى لحماية الأمن الإلكترونى فى تعزيز السلامة وأمن الإنترنت والمجتمعات التجارية والمساعدة على توفير الموارد والخبرة من القطاع الخاص لدعم جميع أجهزة السلطات التنفيذية المحلية والدولية وحكوماتها، فى مهمتهم لتقليل الضرر من الجريمة الإلكترونية، ويشمل ذلك زيادة تمويل القطاع العام من الحكومات والمؤسسات التى ترغب فى المساعدة على زيادة قدرة وإمكانية وحدات مكافحة الجريمة الإلكترونية[١٥].

كذلك مجموعة دول الثمانية حيث اعتمد وزراء العدل لدول مجموعة الثمانى خلال اجتماع عقد بواشنطن ٩-١٠ ديسمبر ١٩٩٧ المبادئ التى تشكل الأساس لشبكة نقاط اتصال وطنية وبجانب هذه المبادئ تم وضع خطة عمل لإنشاء شبكة متابعة لتقديم تقارير بشأن مدى التزام الدول الأعضاء فى الشبكة، وقد أنشئت على غرار نموذج الإنتربول فى الفترة بين ١٩٩٨ -٢٠٠٠ وتتواصل الجهود من أجل زيادة الدول المشاركة، وتناولت مجموعة الثمانى فى

المؤتمر الذى عقدته فى باريس عام ٢٠٠٠، موضوع الجريمة الإلكترونية، وحثت على ضرورة التصدى لها وربطت المجموعة منذ ذلك الوقت محاولاتها الرامية إلى إيجاد حلول دولية باتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية وفى عام ٢٠٠١ ناقشت مجموعة الثمانى الأدوات الإجرائية لمكافحة الجريمة الإلكترونية فى ورشة عمل عقدت بطوكيو، ركزت على ما إذا كان ينبغى تنفيذ الالتزامات باحتجاز البيانات أو ما إذا كان حفظ البيانات يعد حلا بديلًا[١٦].

وفى نطاق العالم العربى اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمى بقانون الإمارات العربى الإرشادى لمكافحة جرائم تقنية المعلومات وما فى حكمها، والذى اعتمده مجلس وزراء العدل العرب، وقد أصدرت عدة دول عربية قوانين لمكافحة الجرائم الإلكترونية، ويعتبر القانون الاتحادى لمكافحة الجرائم المعلوماتية هو القانون الأول فى العالم العربى، كما قامت بعض الدول بإجراء بعض التعديلات على قوانينها الجنائية، وكذلك تم إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والموقعة فى القاهرة فى ٢١ ديسمبر ٢٠١٠، وقد صدر قرار جمهورى بالموافقة على انضمام جمهورية مصر العربية إليها بشرط التحفظ، وقد صدر قرار الموافقة عليه فى ١٩ أغسطس ٢٠١٤.

وأوضحت الاتفاقية أن الهدف منها هو تعزيز التعاون وتدعيمه بين الدول العربية فى مجال مكافحة جرائم تقنية المعلومات لدرء الخطر عنها وحفظ أمنها وسلامتها.

وتضم الاتفاقية دول: "المملكة الأردنية الهاشمية، الإمارات العربية المتحدة، مملكة البحرين، الجمهورية التونسية، جمهورية الجزائر، جمهورية جيبوتى، المملكة العربية السعودية، جمهورية السودان، الجمهورية العربية السورية، جمهورية الصومال، جمهورية العراق، سلطنة عمان، ودولة فلسطين، ودولة قطر، جمهورية القمر، جمهورية القمر المتحدة، دولة الكويت، الجمهورية اللبنانية، الجماهيرية العربية الليبية، والمملكة المغربية، الجمهورية الإسلامية الموريتانية، الجمهورية اليمنية"، وأصدر وزير الخارجية قرارًا بتاريخ ٢٥ سبتمبر ٢٠١٤ بنشر نص الاتفاقية لبدء العمل بها اعتبارا من ٨ أكتوبر ٢٠١٤[١٧].

وفى مجال الملكية الفكرية أبرمت الاتفاقية العربية لحماية حقوق المؤلف حيث نصت فى مجال المعلوماتية، على توفير الحماية القانونية للبرامج المعلوماتية (برامج الحاسب الآلى)، بالإضافة إلى حث وتشجيع الدول الأعضاء على ضرورة تطوير التشريعات الجزائية لمواجهة الجرائم المرتكبة عبر الإنترنت[١٨].

وإضافة إلى الجهود التى تبذلها الهيئات الدولية والإقليمية، هنالك جهود مقدرة فى مجال مكافحة الجرائم الإلكترونية تبذل من قبل هيئات وجمعيات أكاديمية مصرية منها الجمعية المصرية للقانون الجنائى، والتى أصدرت فى مؤتمرها السادس عام ١٩٩٣ توصيات حددت فيها صور السلوك التى يتعين تجريمها حماية للمصالح التى يقع عليها الاعتداء فى الجرائم الإلكترونية، ولا تختلف كثيرًا عن الصور المجرمة التى اشتملت عليها التوصيات الدولية فى هذا الشأن، ومنها أيضًا عقد المؤتمر العلمى الأول حول "العالم الرقمى وجرائم

الشبكات الإلكترونية" بالقاهرة عام ٢٠٠٩، والذى تناول لأول مرة بالدراسة مسألة الإثبات الجنائى باستخدام الوسائل الإلكترونية الحديثة، ومدى قبول الدليل الإلكترونى فى الإثبات الجنائى[١٩]، ومن ضمن تلك الجهود تأسيس جمعيات أهلية تعمل على مكافحة الجرائم الإلكترونية منها الجمعية المصرية لمكافحة الجرائم الإلكترونية والإنترنت والتى تهدف كهيئات مجتمع مدنى وعمل تطوعى للمساهمة فى التصدى للجرائم الإلكترونية.

وفى الأردن أيضًا تم قيام الجمعية الأردنية للحد من الجرائم الإلكترونية ولا تختلف أهدافها عن أهداف الجمعية المصرية لمكافحة الجرائم الإلكترونية حيث أكدت التزامها بكل القيم التى أرساها المؤتمر التأسيسى لجمعيات قانون الإنترنت الذى عقد بالقاهرة إضافة إلى التزامها بمقررات المؤتمرات التى عقدت فى القاهرة[٢٠].

٢ - صور التعاون الدولى فى مواجهة الجرائم الإلكترونية

يمكن ارتكاب الجرائم الإلكترونية من أقصى بقاع الأرض بنفس سهولة ارتكابها من أقرب مكان، كما أن رسالة واحدة تعزز ارتكاب الجريمة يمكن تمريرها من خلال الكثيرين من مقدمى الخدمات فى بلدان مختلفة لها نظم قانونية مختلفة. كما أن الآثار الرقمية التى يمكن تتبعها تكون ضعيفة أو سريعة الزوال، ولذا تستلزم اتخاذ إجراء سريع. وهذا هو الحال تحديدًا حين يسعى المرء إلى منع ارتكاب جريمة فى مرحلة التنفيذ، مثل شن هجوم إلكترونى على بنية أساسية حرجة. وتصبح المهمة بالغة الصعوبة حين تعبر الهجمة اختصاصات قضائية

متعددة ذات نظم مختلفة فى حفظ الأدلة. وهكذا لم تعد تكفى الوسائل التقليدية لإنفاذ القانون، كما أن بطء الإجراءات الرسمية قد يؤدى إلى فقدان الأدلة، فقد تكون بلدان متعددة متورطة فى الأمر. ولذا تشكل متابعة وحفظ سلسلة الأدلة تحديًا كبيرًا. بل حتى الجرائم "المحلية" قد يكون لها بعد دولى، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التى مرت الهجمة من خلالها.

وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السلطات فى البلد الذى كان منشأ الجريمة، أو من السلطات فى البلد أو البلدان التى عبر من خلالها النشاط المجرَّم وهو فى طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة. وهناك عنصران أساسيان للتعاون: المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة.

وقد تكون المساعدة غير الرسمية أسرع إنجازًا، وهى الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أى أوامر تفتيش أو طلب تسليم المجرم)، وهى تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الاتصالات التى جرت مع الوقت فى مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هى عملية أكثر إرهاقًا يتم اللجوء إليها عادة عملًا بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية، وهى تشترط فى الغالب الأعم أن تكون الجريمة المعنية

على درجة معينة من القسوة وأن تشكل جريمة فى كل من البلدان الطالبة والموجه إليها الطلب، ويشار إلى هذا الأمر الأخير باعتباره "تجريمًا مزدوجًا"، وسوف نتناول فيما يلى التعاون القضائى ثم التعاون فى مجال التدريب:

أ - التعاون القضائى

فعالية التحقيق والملاحقة القضائية فى الجرائم المتعلقة بالحاسب الآلى غالبًا ما تقتضى تتبع أثر النشاط الإجرامى من خلال مجموعة متنوعة من مقدمى خدمات الشبكة الدولية للمعلومات أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلى بالشبكة الدولية للمعلومات، وحتى ينجح المحققون فى ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلى المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمى خدمات وسطاء فى بلدان مختلفة. ولتحديد مصدر الجريمة غالبًا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التى تبين متى أجريت تلك التوصيلات ومن أين ومن الذى أجراها. وفى أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه. وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبًا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها فى ولايات قضائية أخرى. بمعنى الحاجة إلى ما يسمى التعاون القضائى ومن أهم صورة التعاون الأمنى والمساعدة القضائية الدولية، وسوف نقتصر على دراسة المساعدة القضائية الدولية.

- المساعدة القضائية الدولية

وتعّرف المساعدة القضائية الدولية بأنها" كل إجراء قضائى تقوم به دولة من شأنه تسهيل مهمة المحاكمة فى دولة أخرى بصدد جريمة من الجرائم"[٢١].

وتتخذ المساعدة القضائية فى المجال الجنائى صور عدة، منها:

*** تبادل المعلومات**

وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التى تطلبها سلطة قضائية أجنبية وهى بصدد النظر فى جريمة ما، عن الاتهامات التى وجهت إلى رعاياها فى الخارج والإجراءات التى اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة[٢٢].

ومن الدول العربية التى أصدرت قانون لمكافحة الجرائم الإلكترونية دولة قطر، القانون رقم (١٤) لسنة ٢٠١٤ بشأن مكافحة الجرائم الإلكترونية، وقد أكدت المادة (٣٠) منه على المساعدة القانونية والقضائية الدولية فى مجال الجرائم الإلكترونية، كما أكدت المادة (٣١) عدم جواز رفض طلب المساعدة المتبادلة إلا فى حالات معينة[٢٣].

ولهذه الصورة من صور المساعدة القضائية الدولية صدى كبير فى كثير من الاتفاقيات كالبند "و" والبند "ز" من الفقرة الثانية من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة فى المسائل الجنائية[٢٤]، وهناك البند أولًا من المادة الرابعة من معاهدة منظمة المؤتمر الإسلامى لمكافحة الإرهاب الدولى[٢٥].

والصورة ذاتها نجدها فى المادة الأولى من اتفاقية الرياض العربية للتعاون القضائى[٢٦]، والمادة الأولى والثانية من النموذج الاسترشادى لاتفاقية التعاون القانونى والقضائى الصادر عن مجلس التعاون الخليجى[٢٧]. ويوجد لها تطبيق كذلك فى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ٢٠٠٠ فى البنود الثالث والرابع والخامس من المادة الثامنة منها.

*** نقل الإجراءات**

يُقصد بنقل الإجراءات أن تقوم دولة بإجراءات تجريها فوق أراضيها بمعرفة سلطاتها القضائية بناءً على طلب دولة أخرى بشأن جريمة وقعت فوق أراضى الدولة الأخيرة. وتسمى الدولة القائمة بالإجراءات "الدولة المطلوب إليها" بينما تسمى الدولة التى تطلب اتخاذ الإجراءات "بالدولة الطالبة" ويتم ذلك وفقا شروط معينة[٢٨]، من أهمها التجريم المزدوج ويُقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة فى الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة فى قانون الدولة المطلوب إليها عن ذات الجريمة. وأيضًا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدى دورًا مهمًا فى الوصول إلى الحقيقة.

ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات فى المسائل الجنائية[٢٩]، واتفاقية الأمم المتحدة لمكافحة

الجريمة المنظمة عبر الوطنية ٢٠٠٠م فى المادة (٢١) منها، والشيء ذاته نجده فى معاهدة منظمة المؤتمر الإسلامى لمكافحة الإرهاب الدولى ١٩٩٩م فى المادة (٩) منها، وأيضًا المادة (١٦) من النموذج الاسترشادى لاتفاقية التعاون القانونى والقضائى الصادر عن مجلس التعاون الخليجى ٢٠٠٣م، وقد أوردت المعاهدة النموذجية الخاصة بنقل الإجراءات التى اعتمدتها الجمعية العامة للأمم المتحدة أسبابًا خاصة لرفض الدولة المطلوب إليها نقل الإجراءات حاصلها كما يلى:

- إذا لم يكن المتهم من رعايا الدولة المطلوب إليها أو من المقيمين فيها عادة.
- إذا كان للجريمة علاقة بالضرائب أو الرسوم أو الجمارك أو النقد الأجنبى.
- إذا تخلف شرط ازدواج التجريم، بمعنى أن يكون الفعل محل طلب نقل الإجراءات مؤثمًا فى تشريع الدولتين الطالبة والمطلوب إليها وإن اختلف تكييف الفعل فيها.

يضاف إلى ما تقدم أسباب عامة للرفض ومثالها إذا اعتبرت الدولة المطلوب إليها أن الجرم ذو طابع سياسى أو يشكل جريمة عسكرية محضة.

ومن الاتفاقيات الدولية التى تتناول موضوع المساعدة القضائية الاتفاقية الفرنسية المصرية المبرمة فى ١٥ مارس ١٩٨٢ وهى تتضمن جملة نصوص تتعلق بالمساعدة القضائية بين الدولتين أو الأمن العام[٣٠].

*** الإنابة القضائية الدولية**

ويُقصد بها طلب اتخاذ إجراء قضائى من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك للفصل فى مسألة معروضة على السلطة القضائية فى الدولة الطالبة ويتعذر عليها القيام به بنفسها[٣١]. وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التى تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وحضور الشهود، والخبراء، والأشخاص التابعين لهم[٣٢].

وعادة وكما هو معهود يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية[٣٣]، ويكون موضوعها مباشرة إجراءات التحقيق الابتدائى ومنها سماع أقوال المتهم والشهود والخبراء[٣٤]، وإجراء المعاينات وأخذ توقيع أطراف الدعوى، وكذلك القيام بالتفتيش وضبط الأشياء وتسليم المستندات والأشياء المتعلقة بالمساءلة الجنائية.

فمثلًا طلب الحصول على دليل إثبات وهو عادًة من شأن النيابة العامة تقوم بتوثيقه المحكمة الوطنية المختصة فى الدولة الطالبة ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة فى الدولة متلقية الطلب. وما أن تتم تلبية الطلب ينعكس الاتجاه الوارد فى سلسلة العمليات. إلا أنه وسعيًا وراء الحد من الروتين والتعقيد والبطء التى تتميز بها الإجراءات

الدبلوماسية يحدث وبدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية – عادة ما تكون وزارة العدل – ترسل إليها الطلبات مباشرة بدلًا من الولوج إلى القنوات الدبلوماسية والذى من شأنه تسريع الإجراءات التى قد تأخذ وقتا طويلًا فيما لو تم عبر تلك القنوات(٣٥).

وقد خلت نصوص التشريع المصرى من أى تنظيم لمسألة الإنابة القضائية، وإن كان مشروع قانون الإجراءات الجنائية لسنة ١٩٩٧ بدأ فى معالجتها. وتكتفى مصر حاليًا بالاشتراك فى اتفاقيات دولية لتنظيم موضوع الإنابة القضائية.

والسؤال هنا هل الاتفاقيات والمعاهدات القائمة بوضعها الحالى صالحة لأن تسهم فى الحد من الجرائم الإلكترونية؟ لا سيما وأن الحاجة إليها ملحة على نحو ما أسلفنا.

نظرًا لأن عامل السرعة يعتبر من العوامل الرئيسية والمهمة فى مكافحة الجرائم المتعلقة بشبكة الإنترنت، ولكون غالبية هذه الاتفاقيات صدرت فى وقت لم تكن شبكة المعلومات الدولية قد ظهرت، أو كانت موجودة ولكنها محدودة، فإن تعديل هذه الاتفاقيات التقليدية للتعاون القضائى الدولى أصبح ضرورة ملحة خاصة مع التطور الكبير فى تكنولوجيا المعلومات والاتصالات.

ولأجل ذلك أبرمت العديد من الاتفاقيات الجديدة التى أسهمت فى تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، مثال ذلك الاتفاقية الأمريكية الكندية التى تنص على إمكانية

تبادل المعلومات شفويًا فى حالة الاستعجال[٣٦]، والشىء نفسه نجده فى البند الثانى من المادة (٣٠) من معاهدة منظمة المؤتمر الإسلامى لمكافحة الإرهاب الدولى ١٩٩٩م والمادة (١٥) من اتفاقية الرياض العربية للتعاون القضائى ١٩٨٣م، والمادة (٥٣) من اتفاقية شينغين ١٩٩٠، والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية فى الدول الأطراف، والفقرة ١٣ من المادة (٤٦) من اتفاقية الأمم المتحدة لمكافحة الفساد[٣٧].

ومنذ عام ١٩٩٣م أدرك المجلس الأوروبى المشكلات التى يمكن أن تثيرها التكنولوجيا الحديثة فى مجال الإجراءات الجنائية، حيث إن الاقتراح رقم ١٧ للتوصية رقم (R٩٥-١٣) قد أكدت بوضوح على وجود قصور على مستوى التعاون الدولى بالنسبة لإجراء التفتيش عبر الحدود، ونصت هذه التوصية على أنه "تمتد سلطة التفتيش إلى الأجهزة المعلوماتية المتواجدة بدائرة اختصاص جهة أجنبية بشرط وجود حالة الضرورة ولكى يتم تجنب انتهاك سيادة الدول أو القانون الدولى فإنه يجب إيجاد سند قانونى لإجراء هذا التفتيش الممتد خارج إقليم الدول[٣٨]. وفى عام ١٩٩٧م أنشأ المجلس الأوروبى لجنة خاصة، كانت مهمتها إعداد اتفاقية خاصة لمواجهة الجرائم التى ترتكب فى فضاء شبكة المعلومات الدولية[٣٩].

وقد أرسلت الاتفاقية الأوروبية حول الإجرام المعلوماتى لسنة ٢٠٠١م قواعد المساعدة القضائية والتعاون القضائى حينما قررت بأنه إذا تم ارتكاب جريمة بواسطة الحاسب أو بدونه كجرائم القتل التى ترتكب بوسائل إلكترونية فإنه يجب تطبيق نصوص المواد (٢٤) الخاصة بالتسليم و(٣٣) والمتعلقة

بالمساعدة القضائية التى تأخذ فى الاعتبار تجميع حركة البيانات فى الزمن الفعلى، والمادة (٣٤) المتعلقة بالمساعدة القضائية فى مجال مراقبة محتوى البيانات وهو ما يجعل لجميع الأطراف فى هذه الاتفاقية وجود نطاق مختلف تطبق فيه تلك الإجراءات[٤٠].

ب - التعاون الدولى فى مجال التدريب على مواجهة الجرائم الإلكترونية

التقدم المتواصل فى التكنولوجيا والإلكترونيات وبشبكة المعلومات الدولية يفرض على جهات إنفاذ القانون أن تسير فى خطوات متناسقة مع التطورات السريعة التى تشهدها هذه التقنيات، والإلمام بها حتى يمكن التصدى للأفعال الإجرامية التى صاحبت هذه التكنولوجيا ومواجهتها هذا من ناحية، ومن ناحية أخرى فإن إعمال القانون فى مواجهة الجرائم المتعلقة بالحاسب الآلى يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة فى المدونة العقابية التقليدية، لما تتسم به هذه الجرائم من حداثة فى الأسلوب وسرعة فى التنفيذ وسهولة فى إخفائها والقدرة على محو آثارها، حيث أثبتت الوقائع العملية أن هناك جرائم متعلقة بالحاسب الآلى وشبكة المعلومات الدولية قد ارتكبت على مرأى ومسمع من رجال التحقيق، بل قام بعض رجال التحقيق بتقديم يد المساعدة لمرتكبى هذه الجرائم دون قصد وعن جهل، أو على سبيل واجبات المهنة التى يلزمهم بها هذا القانون، مثلما حدث عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلى لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب

الجريمة، ونتيجة لذلك أتلف ما كان قد سلم من الملفات والبرامج[٤١]. وإتلاف الأدلة قد يقع كذلك عن خطأ مشترك بين الخبراء وبين الجهة المجنى عليها، فمثلا فى تحقيق إحدى جرائم الحاسب الآلى والتى تدور وقائعها حول طلب أحد الأشخاص من إحدى الشركات زعم أنه وضع قنبلة منطقية بنظام حاسبها الآلى، تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرًا للتحقق من صحة ذلك وإبطال مفعول القنبلة إن وجدت، وبالفعل نجح الخبير فى اكتشاف القنبلة وإزالتها من البرنامج الموضوعة فيه، وعندما تولت الشرطة التحقيق اتضح أنه بإزالة القنبلة أتلفت كل الأدلة على وجودها.

وبالتالى فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح وهذا ما أثبته الواقع العملى يشكل عبئًا ثقيلًا على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائى أو رجال التحقيق أو المحاكم على مختلف درجاتها سيما وأن متطلبات العدالة وكما أسلفنا تقتضى أن تتحمل الأجهزة الأمنية الحكومية كامل المسئولية تجاه اكتشاف جميع الجرائم المعلوماتية وضبط الجناة فيها وتحقيق العدالة فى حقهم.

لأجل ذلك كان لا بد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة ودقة متناهيتين. وهذا لن يتحقق إلا بالتدريب[٤٢]، فكفاءة رجال العدالة لمواجهة هذه الظواهر المستحدثة وقدرتهم فى التصدى لها لا بد وأن ترتكز على كيفية تطوير العملية التدريبية[٤٣] والارتقاء بها والنهوض بأساليب تحقيقها لأهدافها، من هذا المنطلق كانت الدعوة إلى

وجوب تأهيل القائمين على هذه الأجهزة[٤٤]" وحيث إنه ما من دولة يمكنها النجاح فى مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول كانت الدعوة إلى ضرورة وجود تعاون دولى فى مجال تدريب رجال العدالة الجنائية.

- التدريب وأهميته فى مجال مكافحة الجرائم الإلكترونية

التدريب يُعد جزءًا من عملية التنمية الإدارية وهو يهتم بالدرجة الأولى بالكفاءة والفعالية فى إنجاز العمل. إضافة إلى تهيئتهم لتحمل المزيد من المسئوليات من خلال زيادة قدراتهم التى حرصت الكثير من المنظمات العامة والخاصة على العناية بها، باعتبارها إحدى الأدوات الأساسية لرفع مستوى الأداء وزيادة الكفاية الإنتاجية وإعداد العاملين على اختلاف مستوياتهم للقيام بواجبات أعمالهم ومواجهة المهام المعقدة فى الحاضر والمستقبل.

ولهذا أصبح ينظر إلى التدريب على أنه وسيلة للاستثمار الذى تلجأ إليه المنظمات الإدارية لتحقيق أهدافها باعتباره عنصرًا حيويًا لا بد منه لبناء الخبرات والمهارات المتجددة[٤٥].

والواقع أن التدريب أصبح يلعب دورًا هامًا فى حياة الإنسان فى عصرنا الحاضر، حتى يمكننا القول بأننا نعيش اليوم عصر التدريب، فقد زاد الاهتمام بالتدريب.

بمختلف جوانبه الفنية والتكتيكية فقد أضحى ضرورة للفرد المتدرب وللمنظمة التى ينتسب إليها فى آن واحد، سواء أكانت منظمة مدنية أو عسكرية، حكومية أو خاصة، تعمل فى قطاع العدالة أم فى غيره، فهو أحد

العناصر الأساسية لزيادة كفاءة العنصر البشرى ويرفع إنتاجيته ويحقق التنمية بمفهومها الشامل، والهدف من عملية التدريب إدخال وإحداث تعديلات جوهرية على سلوك المتدربين، تبدو آثارها واضحة فى سلوكهم لأداء الأعمال التى يكفلون بها كل فى مجال تخصصه، بشكل أفضل بعد عملية التدريب لا قبلها.

وتبدو أهمية التدريب وضرورته فى أنه من ناحية يُعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التى تكفل الاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء مؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة، كما أنه يُعد من ناحية أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق الفعلى والتعرف على الأخطاء والسلبيات التى يمكن أن يكشف التطبيق العملى للقوانين والأنظمة واللوائح عنها، ووضع الحلول الكفيلة بتجنبها. وتزداد أهمية التدريب فى الوقت الحاضر نظرًا للتطور التكنولوجى الكبير الذى يشهده العالم اليوم(٤٦).

والتدريب المقصود هنا ليس التدريب التقليدى فحسب فلا يكفى أن تتوافر لدى رجال العدالة الجنائية الخلفية القانونية أو أركان العمل الشرطى وإنما لا بد من إكسابهم خبرة فنية فى مجال جريمة الحاسب الآلى. وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصى يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقى التدريب، ويلاحظ هنا أنه من الأسهل تدريب متخصص فى تكنولوجيا المعلومات وشبكات الاتصال بدلًا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلى الادعاء العام، ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى

المتدرب خبرة لا تقل عن خمس سنوات فى المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلى[٤٧]، وبالنسبة للمنهج التدريبى فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلى مع ذكر لمفاهيم معالجة البيانات وتحديد نوعية وأنماط جرائم الحاسب الآلى، وبيان لأهم الصفات التى يتميز بها مجرم الحاسب الآلى، والدوافع وراء ارتكاب الجرائم الإلكترونية.

وفيما يتعلق بمنهج التحقيق فإنه لابد وأن يشتمل على:

- إجراءات التحقيق.
- التخطيط للتحقيق.
- تجميع المعلومات وتحليلها.
- أساليب المواجهة والاستجواب.
- مراجعة النظم الفنية للبيانات.
- أساليب المعمل الجنائى.

بالإضافة إلى ذلك لا بد وأن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلى كأداة للمراجعة والحصول على أدلة الاتهام وما يخص الملاحقة الدولية والتعاون المشترك.

وفيما يخص التدريب فإنه لا بد وأن يراعى فى البرنامج التدريبى نوعه وصفته وما إذا كان رسميًا من خلال حلقات دراسية أو حلقات نقاش – ورش

العمل-حول هذا النوع المستحدث من الجرائم، وحلقات النقاش التى يمكن أن تثمر أفضل تدريب رسمى هى تلك التى تكفل تفاعل المشاركين، وتتضمن تحليلًا لحالات دراسية وإكساب خبرة عملية فى كيفية التعامل مع الحاسب الآلى وكيفية استخدام تقنيات الاتصال بين شبكات الحاسب الآلى، وما يرتبط بها من قواعد بيانات ومعلومات. وقد يكون البرنامج التدريبى غير رسمى من خلال تكليف المتدرب بالعمل مع شخص لدية خبرة فى تحقيق جرائم الحاسب الآلى، أو التدريب باستخدام أسلوب الفريق والذى تقوم فلسفته على تدريب الفريق أو مجموعة متخصصة فى جرائم الحاسب الآلى مرة واحدة بحيث يكون لكل فريق من الفرق مهمة محددة فضلًا عن إلمامه بمهام زملائه الآخرين، فطبقا لهذا الأسلوب يتم التركيز على تدريب مجموعة من المتخصصين فى مجالات معينة بحيث يلم كل منهم بتخصص الآخرين، ويزداد فى نفس الوقت فهما لتخصصه الأصلى[٤٨]. ويتعين هنا على الفريق أن يخوض تجارب عملية بحيث تعرض عليه عينة من جرائم الحاسب الآلى التى تم التحقيق فيها، على أن يراعى فى هذه العينة التنويع لكى تؤدى دورها فى إكساب المشاركين فى البرنامج التدريبى الخبرة المطلوبة. وهذا الأمر يتطلب أن يعهد بالتدريب إلى جهات متخصصة تعنى باختيار المدربين ممن تتوافر لديهم الصلاحية العلمية والفنية والصفات الشخصية ليتولوا التدريب فى هذا المجال، والذى من شأنه تحقيق نتائج طيبة فى عملية التدريب[٤٩]. والعلمية التدريبية لا بد وأن تكون مستمرة ولا تتوقف عند حد معين، سيما وأن الجرائم الإلكترونية ومنها الجرائم المتعلقة بشبكة المعلومات الدولية فى تطور مستمر وبشكل سريع جدًا.

ليس هذا فحسب بل لا بد وأن تسعى الأجهزة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات فى المجال المعلوماتى وضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم، ومن أجل ذلك ينبغى على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات من الجامعين من خريجى كليات الحاسبات الآلية لتخرجهم ضباطًا مؤهلين قانونيًا وتقنيًا، كذلك يتعين على الكليات المعنية بتدريس القانون أن تسعى جاهدة إلى تدريس الحاسبات الآلية وكل ما يتعلق به إلى الطلبة، وأن تكون مادة الحاسب الآلى وتقنية المعلومات إحدى المواد الأساسية، لأن من شأن ذلك أن تتكون لدى خريجى هذه الكليات ثقافة قانونية وثقافة حاسوبية.

خلاصة القول إن غرس وتطوير الثقافة الحاسوبية وسط رجال القانون والشرطة، وربطها بالثقافة القانونية والشرطية التقليدية يكفل للأجهزة الأمنية ولسلطات التحقيق النجاح الباهر فى مواجهة جرائم الحاسب الآلى.

- مظاهر التعاون الدولى فى مجال تدريب رجال العدالة الجنائية

أجهزة العدالة فى الكثير من الدول سيما الدول النامية ليست لديها تلك الجاهزية لمواجهة الجرائم المتعلقة بشبكة الإنترنت ومثيلاتها من الجرائم المستحدثة ذات التطور المستمر لعدة أسباب منها الافتقار إلى الموارد الكافية مادية كانت أو بشرية، أو لأن سلطات التحقيق لديها محدودة أو لأنه لديها قوانين ونظم سبقها الزمن أو قد تفتقر لأى قوانين لتتصدى بها لهذه النوعية من الجرائم.

من هنا ولأننا نعلم أنه ما من دولة يمكنها النجاح فى مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول كانت الدعوة إلى ضرورة وجود تعاون دولى ليس فقط فى مجال المساعدات القضائية المتبادلة أو فى مجال تسليم المجرمين فحسب، وإنما أيضًا فى مجال تدريب رجال العدالة[٥٠]، فتدريب الكوادر البشرية القائمة على إنفاذ القانون ليس بذات المستوى فى جميع الدول وإنما يختلف من دولة لأخرى بحسب تقدم الدولة ورقيها. ولو أمعنا النظر فى بعض الصكوك الدولية والإقليمية لوجدنا أنها دعت وبصريح النص إلى ضرورة وجود تعاون بين الدول فى مجال التدريب ونقل الخبرات فيما بينها. كما هو الحال فى المادة ٢٩ من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ٢٠٠٠م، والمادة (٩) من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

والتعاون الدولى فى مجال تدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكة المعلومات الدولية قد يكون بين الدول وأجهزة العدالة الجنائية لديها، فعلى الصعيد العربى نجد مثلا أنه هناك اجتماعات تم عقدها فى إطار التنسيق بين المعاهد القضائية العربية لتوفير التدريب والتأهيل المناسبين لأعضاء الهيئات القضائية العربية. وقد تمخضت الاجتماعات عن الاتفاق على إعداد مشروع اتفاقية للتعاون بين المعاهد القضائية العربية تسمى اتفاقية عمّان للتعاون العلمى بين المعاهد القضائية العربية والتى وقعت فى ٩ أبريل ١٩٩٧م[٥١]. وفى جمهورية مصر العربية نجد أن النيابة العامة تعقد الكثير من الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقدت داخل مصر أو

خارجها، بالإضافة أنه يتم إرسال أعضاء النيابة من مختلف الدرجات فى برامج خارجية وذلك بالتعاون مع أجهزة النيابة العامة فى الدول الأخرى والهيئات الدولية بهدف الإطلاع على أحدث النظم المقارنة، والشىء ذاته نجده فى سلطنة عمان. وقد يتم من خلال عقد ندوات ومؤتمرات أو ورش العمل الجماعى[٥٢] متخصصة فى مواجهة تلك الجرائم تعقد على المستوى الدولي أو على المستوى الإقليمى، حيث تلقى هذه الفعاليات العلمية من أبحاثها ودراستها وموضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل ومناقشة أبعادها بعقلية ناجحة مما يمكن المعنيين بالوقاية ومكافحة هذه الجرائم من التعرف على أساليب ارتكابها وأخطارها ووسائل الوقاية والمكافحة بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها. وعلى هامش هذه المؤتمرات أو الندوات أو ورش العمل الجماعى تعقد اللقاءات وتبادل الآراء والخبرات.

وقد يتحقق من عقد اللقاءات وحلقات المناقشة المصغرة بين مسئولى الاتصال بالسفارات أو المكاتب الجغرافية الإقليمية للمنظمات والأجهزة المعنية مع جهات أو أطراف يقعون فى دائرة عملهم أو بالقرب منها بناءً على رغبة الجهة التى يمثلونها، يتم خلالها تبادل الآراء والخبرات بين المشاركين. وتمثل كل هذه اللقاءات وحلقات المناقشة وسيلة طيبة للحوار والمناقشة والتشاور للتعارف وتبادل الرأى والخبرة وطرح الأفكار والتصورات وتدارس سبل تنمية وتشجيع التعاون فيما بين الأطراف.

وقد يتحقق عن طريق تنظيم الدورات التدريبية للعاملين فى أجهزة العدالة الجنائية والمعنيين بمكافحة الجريمة على المستوى الدولى، وتعد هذه الصورة أكثر تطورًا للتعاون الدولى الذى يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين فى مكافحة الجريمة فى الدول المختلفة من خلال تبادل الخبرة، وطرح موضوعات ومشكلات للتدارس المشترك، والتعرف على أحدث التطورات فى مجال الجريمة سيما المعلوماتية وأساليب مكافحتها، وغالبًا ما يجرى تنظيم مثل هذا التدريب من خلال المنظمات أو الدول أو الأجهزة الكبرى ذات مستوى أكثر تقدمًا يمكن أن يشجع الأطراف الأخرى على المشاركة فى هذه البرامج التدريبية، كما يمكنها تحمل نفقات وأعباء مثل هذه الدورات(٥٣).

وتحقق مثل هذه الدورات والبرامج العديد من الفوائد للجهات المنظمة وللمشاركين فيها، فالجهة المنظمة يمكنها من خلال عقد مثل هذه البرامج أن تطرح ما تريد من موضوعات حيوية، كما أنها تعلن عن دورها الرائد لتزيد من ثقة الأطراف الأخرى فى أدائها، بما يشجع على إجراء المزيد من التعاون معها، وبما يضعها فى مكانة خاصة لدى المتدربين والجهات التى يتبعونها. وعلى الجانب الآخر فإن هذه البرامج يمكن أن تُفيد متلقى التدريب عن طريق زيادة مهاراته وخبراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى، الأمر الذى ينعكس على الجهة التى ينتمى إليها بالفائدة.

- تجربة الولايات المتحدة الأمريكية فى هذا المجال(٥٤)

تعد الولايات المتحدة الأمريكية من الدول المتقدمة تكنولوجيا والمتطورة تقنيًا فى مجال مكافحة الجرائم الإلكترونية وجرائم الشبكات، وعلى الرغم من ذلك فهى

تعى وتعلم أنه ما من دولة وإن كانت متقدمة يمكنها التصدى لأخطار هذه الأنماط المستحدثة من الجرائم.

من هذا المنطلق نجدها تحرص على توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجنائية لدى الحكومات الأخرى، ومساعدة ما لديها من أجهزة شرطة، ومسئولى الادعاء العام، والقضاة ليصبحوا أكثر فعالية فى مكافحة الجريمة. فمثل هذه المساعدة لا تؤدى إلى تيسير بناء إطار للتعاون الدولى فى مجال تطبيق القانون وحسب، ولكنها تعزز أيضًا قدرة الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة المعلوماتية لديها قبل أن يمتد ليتجاوز حدود بلدانها.

فمكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام فى الخارج، التابع لوزارة العدل الأمريكية، مكلّف تحديدًا بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجنائية فى دول أخرى، وتعزيز إدارة القضاء فى الخارج.

كما أن البرنامج الدولى للمساعدة والتدريب على التحقيق الجزائى (ICITAP)، الذى كثيرًا ما يعمل بالترادف مع وحدته الشقيقة - مكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام فى الخارج، العامل داخل وزارة العدل نفسها - على توفير مساعدات لأجهزة الشرطة فى البلدان النامية فى مختلف أنحاء العالم. وتهدف المساعدة التى يقدمها هذا البرنامج الأخير إلى تعزيز القدرات التحقيقية لدى أجهزة الشرطة فى البلدان الناشئة.

وفى الوقت الحاضر، تقدّم وزارة العدل الأميركية مساعدات لتطوير القطاع القضائى فى عدد من البلدان فى إفريقيا، وآسيا، وأوروبا الشرقية والوسطى وأمريكا اللاتينية ومنطقة حوض الكاريبى، والدول المستقلة حديثًا، بما فى ذلك روسيا والشرق الأوسط. مستعينة فى ذلك بخبرة الوحدات المتخصصة التابعة لها. منها على سبيل المثال وحدة مكافحة استغلال الأطفال وأعمال الفحش التابعة للقسم الجزائى بها، قامت بدور أساسى فى صياغة قانون نموذجى يهدف إلى مكافحة استغلال الناس عن طريق الاتجار بالبشر والبغاء.

هذا من جهة ومن جهة أخرى نجد أن أجهزة تطبيق القانون الأمريكية توفر أيضًا تدريبًا لنظيراتها من الأجهزة فى البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهد خاصة بتدريب العاملين فى أجهزة تطبيق القانون كما هو الحال فى كل من المجر، وبوتسوانا، وكوستاريكا، وتايلاند. وفى هذه المعاهد، يقوم خبراء أميركيون فى عمل أجهزة تطبيق القانون بإطلاع المتدربين على أساليب وسبل مبتكرة للتحقيق، ويشجعون على تبادل الآراء مع نظرائهم فى مختلف أنحاء العالم.

خلاصة القول وصفوته أنه ما من دولة يمكنها بنجاح مجابهة هذا التحدى فى مواجهة هذه الأنماط المستحدثة من الجرائم ومنها الجرائم الإلكترونية بمفردها. ولا مفر من مواصلة أجهزة تطبيق القانون فى أنحاء العالم تطوير القدرة على التعاون الدولى فى المجال التدريبى، ولا مفر للدول المتقدمة من مساعدة الدول النامية لتعزيز مؤسساتها المتخصصة بالتحرى والتحقيق والمحاكمة، من خلال توفير التدريب وسائر أنواع المعونة التقنية.

ثانياً: صعوبات التعاون الدولى فى مواجهة الجرائم الإلكترونية وسبل مواجهتها

التعاون الدولى بكل صوره فى مجال مكافحة الجرائم الإلكترونية يعد مطلبًا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، إلا أنه ثمة معوقات تقف دون تحقيقه وسوف نتناول فيما يلى: (صعوبات التعاون الدولى فى مواجهة الجرائم الإلكترونية، ثم سبل مواجهة صعوبات التعاون الدولى وتحديث آليات التعاون فى مواجهة الجرائم الإلكترونية).

١ - صعوبات التعاون الدولى فى مواجهة الجرائم الإلكترونية

تتمثل صعوبات التعاون الدولى فى مكافحة الجرائم الإلكترونية فى عدم وجود نموذج إجرامى موحد للأنشطة الإجرامية، وتنوع واختلاف نظم الإجراءات الجنائية بين الدول، وعدم وجود قنوات اتصال بين الدول، ثم مشكلة الاختصاص فى الجرائم الإلكترونية، والتجريم المزدوج، والصعوبات الخاصة بالإنابة القضائية، والصعوبات الخاصة بالتعاون الدولى فى مجال التدريب، والنقص الكبير بالنسبة لرجال الشرطة، وجهات التحقيق بالنسبة للطبيعة المعقدة لهذه الجريمة. وسنقوم بدراسة هذه الصعوبات كما يلى:

أ – عدم وجود نموذج موحد للنشاط الإجرامى وتنوع واختلاف النظم القانونية الإجرائية

– عدم وجود نموذج موحد للنشاط الإجرامى

بنظرة متأنية للأنظمة القانونية القائمة فى الكثير من الدول لمواجهة الجرائم الإلكترونية ومنها الجرائم المتعلقة بشبكة الإنترنت، يتضح لنا عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا فى أحد الأنظمة قد يكون مجرّمًا وغير مباح فى نظام آخر مما يؤدى لاختلاف عناصر الجريمة الإلكترونية من دولة لأخرى[٥٥]، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالى اختلاف السياسة الجنائية من مجتمع لآخر[٥٦].

– تنوع واختلاف النظم القانونية الإجرائية

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحرى والتحقيق والمحاكمة التى تثبت فائدتها وفاعليتها فى دولة ما قد تكون عديمة الفائدة فى دولة أخرى أو قد لا يسمح بإجرائها. كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الأدلة أو التحقيق قانونية فى دولة معينة، فإنه قد تكون الطريقة ذاتها غير مشروعة فى دولة أخرى، وبالتالى فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات تطبيق القانون فى الدولة

الأخرى على استخدام ما تعتبره هى أداة فعّالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أى دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه فى اختصاص قضائى وبشكل مشروع[٥٧]، وفى هذا السياق تبدو أهمية الاتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية التى أقرها المجلس الأوروبى فى ٣٠ نوفمبر سنة ٢٠٠٠[٥٨]. إذ تأتى هذه الاتفاقية فى إطار منظومة التعاون القانونى والقضائى بين دول الاتحاد الأوروبى، حيث سبقتها العديد من الاتفاقيات والبرتوكولات فى هذا المجال؛ كالاتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية لسنة ١٩٥٩، واتفاقية Benelux لسنة ١٩٦٢، وبرتوكول التعاون القضائى فى المسائل الجنائية لسنة ١٩٧٨، واتفاقية Schengen لسنة ١٩٩٠ التى دخلت إلى حيز التطبيق فى ٢٦ مارس سنة ١٩٩٥، واتفاقية تسليم المجرمين لسنة ١٩٩٦.

وقد عكست نصوص الاتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية، رغبة دول الاتحاد الأوروبى فى توسيع نطاق حالات التعاون القضائى فيما بينها، وإرساء آليات تكنولوجية حديثة تكفل سرعة ومرونة وفعالية هذا التعاون، لضمان مواجهة قانونية وقضائية فعالة للجرائم المنظمة عابرة الحدود، التى استفاد مرتكبوها، إلى أقصى حد ممكن، من المعطيات التكنولوجية الحديثة، لا سيما بعدما تهاوت- إلى حد كبير- الحدود الجغرافية بين هذه الدول، وما صاحب ذلك من سهولة انتقال الأشخاص والأموال فيما بينها[٥٩].

ويمثل اللجوء إلى تقنية الاتصال المرئى المسموع Vidéo conférence، كوسيلة للتحقيق الجنائى عن بعد، أهم مظاهر اعتداد الاتفاقية الأوروبية الجديدة للمساعدة القضائية فى المسائل الجنائية بالمعطيات التكنولوجية الحديثة فى مجال تطوير آليات التعاون القضائى بين دول الاتحاد الأوروبى. إذ أجازت المادة العاشرة من هذه الاتفاقية استخدام هذه التقنية لمباشرة بعض إجراءات التحقيق الجنائى عن بعد بواسطة السلطات القضائية لإحدى الدول المتعاقدة، فى مواجهة بعض الأشخاص الذين يتواجدون فى إقليم دولة متعاقدة أخرى وجاءت أحكامها التفصيلية متضمنة حلولا للعديد من المشكلات القانونية والعملية التى يثيرها تطبيق هذه التقنية فى مجال التحقيق أو المحاكمة الجنائية عن بعد، بحيث شكلت - إلى حد ما - محاولة جادة لتحقيق التوازن بين اعتبارات فعالية آليات المساعدة القضائية بين الدول المتعاقدة من جهة، ومقتضيات حماية الحريات والحقوق الفردية وكفالة حقوق الدفاع من جهة أخرى، ولكن على الرغم من إقرار الاتفاقية الأوروبية الجديدة للمساعدة القضائية فى المسائل الجنائية استخدام تقنية الاتصال المرئى المسموع Vidéo conférence كوسيلة للتحقيق الجنائى عن بعد، فإن الاتفاقية حصرت استخدام هذه التقنية فى نطاق محدود، وأسبغت عليه طابعًا احتياطيًا، بحيث لا يجوز اللجوء إليه إلا عند الضرورة، وقصرت نطاق استخدام تقنية الاتصال المرئى المسموع Vidéo conférence كوسيلة للتحقيق الجنائى عن بعد، وفقا لنص المادة العاشرة من الاتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية، على مباشرة بعض إجراءات التحقيق الجنائى التى تتفق وطبيعية هذه

التقنيـة، ولا تثيـر الكثيـر مـن المشـكلات القانونيـة، دون غيرهـا مـن إجـراءات التحقيق الجنائى الأخرى وعلى ذلك فقد حصرت الفقرة الأولى من المادة العاشرة من الاتفاقية، استخدام هذه التقنية- بصفة أساسية- فى مجال سماع شهادة الشهود، وإفادات الخبراء[٦٠]، حيث أجازت للسلطات القضائية لإحدى الدول المتعاقدة طلب سماع شخص يتواجد على إقليم دولة متعاقدة أخرى، بصفته شاهدًا أو خبيرًا، عبر تقنية الاتصال المرئى المسموع Vidéo conférence، متى ثبت استحالة أو عدم ملاءمة مثول هذا الشخص بشخصه أمام هذه السلطات، وقد استبعد واضعوا الاتفاقية - فى مرحلة المناقشات وصياغة النصوص- فى بداية الأمر، استخدام هذه التقنية فى مجال سماع أقوال المتهم واستجوابه، غير أنهم اضطروا تحت الضغوط التى مارسها أعضاء الوفد الإيطالى - لا سيما بعد أن أقرت إيطاليا بالفعل استخدام هذه التقنية كوسيلة للتحقيق والمحاكمة الجنائية عن بعد بموجب القانون رقم ١١ الصادر فى السابع من نوفمبر سنة ١٩٩٨- إلى الإقرار بإمكانية استخدام هذه التقنية، بصفة استثنائية وفى نطاق محدود، لسماع أقوال المتهم أو استجوابه عن بعد بواسطة السلطات القضائية لإحدى الدول المتعاقدة، متى تواجد فى إقليم دولة متعاقدة أخرى[٦١].

وتطبيقا لذلك أوردت المادة العاشرة، فى فقرتها التاسعة، حكما توفيقيا؛ يلبى رغبة بعض الدول فى استخدام تقنية الاتصال المرئى المسموع Vidéo conférence لسؤال المتهم أو استجوابه عن بعد، ويتجاوب، فى الوقت ذاته، مع معارضة غالبية الدول المتعاقدة لاستخدام هذه التقنية فى هذا الصدد.

إذ اشترطت لاستخدام هذه التقنية فى مجال سؤال المتهم أو استجوابه عن بعد، موافقة هذا الأخير على ذلك صراحة. كما اشترطت كذلك موافقة كل من الدولتين الطالبة والمنفذة على استخدام هذه التقنية، على أن يتم ذلك بموجب اتفاق خاص بين الدولتين تراعى فيه أحكام قانونيهما الوطنى، وكذلك الاتفاقيات الدولية ذات الصلة بما فيه الاتفاقية الأوروبية لحقوق الإنسان لسنة ١٩٥٠. وأشارت إلى ضرورة إرساء المجلس الأوروبى أداة قانونية ملزمة تكفل حماية حقوق المتهم فى هذه الحالة. بل وأجازت للدول المتعاقدة - لا سيما تلك التى تعارض استخدام هذه التقنية فى مجال سؤال المتهم أو استجوابه - التحفظ عند التصديق على الاتفاقية على تطبيق هذه التقنية فى مجال مساع أقوال المتهم أو استجوابه، بحيث يقتصر نطاق استخدامها بالنسبة لها على سماع شهادة الشهود وإفادات الخبراء، وإن أجازت لها، فى الوقت ذاته، سحب هذا التحفظ لاحقا فى أى وقت(٦٢).

ولم يكتف واضعوا الاتفاقية الأوروبية الجديدة للمساعدة القضائية فى المسائل الجنائية، بحصر استخدام تقنية الاتصال المرئى المسموع Vidéo conférence كوسيلة للتحقيق الجنائى عن بعد فى نطاق محدود، بل أسبغوا على استخدام هذه التقنية طابعا احتياطيا، بحيث لا يجوز اللجوء إليه إلا عند الضرورة.

وتطبيقا لذلك، حظرت الفقرة الأولى من المادة العاشرة من الاتفاقية، اللجوء إلى استخدام هذه التقنية لسماع الشاهد أو إفادة الخبير عن بعد، إلا فى

الحالات التى يثبت فيها عدم ملاءمة انتقال الشاهد أو الخبير إلى الدولة الطالبة للمثول أمام سلطاتها القضائية، أو استحالة هذا الانتقال.

ويجد هذا الحظر أساسه- علاوة على رغبة واضعى الاتفاقية فى حصر استخدام المعطيات التكنولوجية الحديثة فى مجال الدعوى الجنائية فى أضيق نطاق ممكن- فيما تنص عليه المادة العاشرة من الاتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية لسنة ١٩٥٩، من جواز انتقال الشاهد أو الخبير إلى الدولة الطالبة للمثول أمام سلطاتها القضائية متى كانت هناك ثمة ضرورة لذلك، وفقا للضمانات التى نصت عليها المادة الثانية عشرة من هذه الاتفاقية وأهمها؛ عدم توجيه الاتهام إليه أو حبسه أو تقييد حريته بأى وجه من الأوجه فى الدولة الطالبة[٦٣]. لا سيما وأن نصوص الاتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية، وفقا لما تنص عليه مادتها الأولى، لم تلغ، بصورة مطلقة، أحكام ما سبقتها من اتفاقيات أوروبية فى مجال المساعدة القضائية فى المسائل الجنائية، وإنما جاءت مكملة لها.

ويثير اشتراط ثبوت عدم ملاءمة انتقال الشاهد أو الخبير إلى إقليم الدولة الطالبة، أو تحقق استحالة هذا الانتقال، اللجوء إلى استخدام تقنية الاتصال المرئى المسموع Vidéo conférence لسماع شهادة الشاهد أو إفادة الخبير عن بعد، والتساؤل حول المقصود بعدم الملاءمة أو الاستحالة فى هذا الصدد من جهة، وتحديد الجهة التى تختص بتقدير مدى ملاءمة استخدام هذه التقنية، هل هى الدولة الطالبة التى تريد سلطاتها مباشرة الإجراء؟ أم الدولة المنفذة التى يتواجد على إقليمها الشاهد أو الخبير.

فيما يتعلق بالتساؤل الأول، أشارت المذكرة التفسيرية للاتفاقية الأوروبية الجديدة للمساعدة القضائية فى المسائل الجنائية - على سبيل المثال - إلى بعض الحالات التى يكون فيها انتقال الشاهد أو الخبير إلى الدولة الطالبة غير ملائم أو مستحيل. فالانتقال يكون غير ملائم فيما لو كان الشاهد صغير السن، أو كان على العكس طاعنا بالسن بحيث يصعب عليه الانتقال إلى الدولة الطالبة، أو كان أيا من الشاهد أو الخبير فى حالة صحية سيئة نظرا لإصابته بمرض خطير. ويكون مستحيلا فى الحالات التى ينطوى فيها انتقال الشاهد أو الخبير إلى الدولة الطالبة على تعريض حياته للخطر.

وفيما يتعلق بالتساؤل الثانى، لم تتضمن المادة العاشرة من الاتفاقية إجابة صريحة على هذا التساؤل. ولهذا فإننا نؤيد ما يذهب إليه البعض من أن الدولة المنفذة، التى يتواجد على إقليمها الشاهد أو الخبير، هى الأقدر على تقدير مدى ملاءمة انتقال الشاهد أو الخبير إلى الدولة الطالبة، ومن ثم مدى ملاءمة استخدام تقنية الاتصال المرئى المسموع Vidéo conférence لسماع شهادة الشاهد أو إفادة الخبير عن بعد بواسطة السلطات القضائية للدولة الطالبة. لا سيما وأن لهذه الدولة، وكما سنرى فيما بعد، رفض إجابة طلب الدولة الطالبة استخدام هذه التقنية لسماع الشاهد أو الخبير، متى انطوى هذا الاستخدام على تعارض مع المبادئ الأساسية التى يقوم عليها نظامها القانونى.

وكذلك حددت الفقرة الثانية من المادة العاشرة من الاتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية[٦٤]، شروط استخدام تقنية الاتصال

المرئى المسموع Vidéo conférence كوسيلة للتحقيق الجنائى عن بعد، حيث أوجبت عدم تعارض استخدامها مع المبادئ الأساسية فى قانون الدولة المنفذة من جهة، واستلزمت توافر الإمكانيات الفنية التى تمكن هذه الأخيرة من استخدام هذه التقنية من جهة أخرى.

ب - عدم وجود قنوات اتصال ومشكلة الاختصاص فى الجرائم الإلكترونية والتجريم المزدوج

- عدم وجود قنوات اتصال

أهم الأهداف المرجوة من التعاون الدولى فى مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزامًا أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعنى عدم القدرة على جمع الأدلة والمعلومات العملية التى غالبا ما تكون مفيدة فى التصدى لجرائم معينة ولمجرمين معينين. وبالتالى تنعدم الفائدة من هذا التعاون[٦٥].

- مشكلة الاختصاص فى الجرائم الإلكترونية

الجرائم الإلكترونية من أكبر الجرائم التى تثير مسألة الاختصاص على المستوى الدولى، ولا توجد أى مشكلة بالنسبة للاختصاص على المستوى الوطنى أو المحلى حيث يتم الرجوع إلى المعايير المحددة قانونًا لذلك.

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولى حيث اختلاف التشريعات والنظم القانونية والتى قد ينجم عنها تنازع فى الاختصاص بين الدول بالنسبة للجرائم الإلكترونية التى تتميز بكونها عابرة للحدود. فقد يحدث أن ترتكب الجريمة فى إقليم دولة معينة من قبل أجنبى، فهنا تكون الجريمة خاضعة للاختصاص الجنائى للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصى، وقد تكون هذه الجريمة من الجرائم التى تهدد أمن وسلامة دولة أخرى فتدخل عندئذ فى اختصاصها استنادًا إلى مبدأ العينية. كما تثار فكرة تنازع الاختصاص القضائى فى حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجانى ببث الصور الخليعة ذات الطابع الإباحى من إقليم دولة معينة وتم الإطلاع عليها فى دولة أخرى، ففى هذه الحالة يثبت الاختصاص وفقًا لمبدأ الإقليمية لكل دولة من الدول التى مستها الجريمة.

- التجريم المزدوج

التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه فى أغلب التشريعات الوطنية والاتفاقات الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته تلك، نجده عقبة أمام التعاون الدولى فى مجال تسليم المجرمين بالنسبة للجرائم الإلكترونية، سيما وأن معظم الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم

المتعلقة بالجريمة محل البحث أو لا. الأمر الذى يعوق تطبيق الاتفاقيات الدولية فى مجال تسليم المجرمين، ويحول بالتالى دون جمع الأدلة ومحاكمة مرتكبى الجرائم المتعلقة بالإنترنت[٦٦].

جـ - صعوبات الإنابة القضائية الدولية وصعوبات التعاون الدولى فى مجال التدريب ونقص الخبرات

- الصعوبات الخاصة بالإنابة القضائية الدولية

الأصل بالنسبة لطلبات الإنابة القضائية الدولية والتى تعد من أهم صور المساعدات القضائية الدولية فى المجال الجنائى أن تسلم بالطرق الدبلوماسية، فمثلًا طلب الحصول على دليل إثبات وهو عادة من شأن النيابة العامة تقوم بتوثيقه المحكمة الوطنية المختصة فى الدولة الطالبة ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب لتقوم بإرساله إلى السلطات القضائية المختصة فى الدولة متلقية الطلب وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذى قد يتعارض مع طبيعة الأعمال الإلكترونية وما تتميز به من سرعة، وهو الأمر الذى انعكس على الجرائم الإلكترونية، كذلك من الصعوبات الكبيرة فى مجال المساعدات القضائية الدولية المتبادلة التباطؤ فى الرد، حيث إن الدولة متلقية الطلب غالبًا ما تكون متباطئة فى الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق فى الإجراءات التى تعقد الاستجابة وغيرها من الأسباب، وقد أبرمت العديد من الاتفاقيات التى ساهمت فى تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، مثال ذلك الاتفاقية الأمريكية الكندية التى تنص

على إمكانية تبادل المعلومات شفويًا فى حالة الاستعجال، والشئ نفسه نجده فى البند الثانى من المادة ٣٠ من معاهدة منظمة المؤتمر الإسلامى لمكافحة الإرهاب الدولى ١٩٩٩م، والمادة ١٥ من اتفاقية الرياض العربية للتعاون القضائى ١٩٨٣م، والمادة ٥٣ من اتفاقية شينغن ١٩٩٠، والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية فى الدول الأطراف، والفقرة ١٣ من المادة ٤٦ من اتفاقية الأمم المتحدة لمكافحة الفساد ويعتبر عامل السرعة من العوامل الرئيسية والمهمة فى مكافحة الجرائم المتعلقة بالإنترنت، ولكون غالبية هذه الاتفاقيات صدرت فى وقت لم تكن شبكة الإنترنت قد ظهرت، أو كانت موجودة ولكنها محدودة، فإن تعديل هذه الاتفاقيات التقليدية للتعاون القضائى الدولى أصبح ضرورة ملحة خاصة مع التطور الكبير فى تكنولوجيا المعلومات والاتصالات.

- الصعوبات الخاصة بالتعاون الدولى فى مجال التدريب

يتمثل ذلك فى عدم رغبة بعض القيادات الإدارية فى بعض الدول فى التدريب لاعتقادهم بدوره السلبى فى تطوير العمل من خلال تطبيق ما تعلمه المتدربون فى الدورات التدريبية وما اكتسبوه من خبرات. ومن الصعوبات أيضًا والتى قد تهدد التعاون فى مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين. سيما فى مجال تكنولوجيا المعلومات وشبكات الاتصال حيث إنه يوجد بعض الأشخاص ممن لا يعى فى هذا المجال شيئا، وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة فى هذا المجال.

بالإضافة إلى أن نظرة المتدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبء لا طائل منه تهدد العملية التدريبية برمتها وبالطبع نسف التعاون الدولى فى هذا المجال.

أيضًا من الصعوبات التى قد تؤثر على العملية التدريبية وعلى التعاون الدولى فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملى لبيئة العمل الطبيعية تمثيلًا تامًا ومتقنًا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التى سيؤديها المتدربون فى بيئة العمل الطبيعية.

د - النقص الكبير فى خبرات رجال الشرطة، وجهات التحقيق بالنسبة للطبيعة المعقدة لهذه الجريمة

حيث يتطلب كشف الجرائم محل البحث والاهتداء إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات تحقيق وتدريبًا ومهارات خاصة تسمح بفهم ومواجهة تقنيات الحاسب الآلى المتطورة وأساليب التلاعب المعقدة التى تستخدم عادة فى ارتكاب هذه الجرائم لذلك وجدت سلطات البحث الجنائى والتحقيق نفسها غير قادرة على التعامل بالوسائل التقليدية مع هذه النوعية من الجرائم ولنقص الخبرة والتدريب كثيرًا ما تخفق أجهزة الشرطة فى تقدير أهمية الجريمة محل البحث فلا تبذل لكشف غموضها وضبط مرتكبيها جهودًا تتناسب مع هذه الأهمية ولهذا كثيرًا ما تفشل هى وجهات التحقيق فى جمع أدلة جرائم نظم المعلومات مثل مخرجات الحاسب وقوائم التشغيل بل إن المحقق نتيجة نقص خبرته فى الحاسب الآلى قد يدمر الدليل بمحوه الأسطوانة الصلبة عن خطأ أو إهمال أو

التعامل بخشونة مع الأقراص المرنة. هذه هى صعوبات التعاون الدولى فى مواجهة الجرائم الإلكترونية والتى يمكن أن يضاف إليها ندرة الاتفاقات الدولية التى تشجع وتنظم التعاون الدولى فى هذا المجال.

٢ - سبل مواجهة صعوبات التعاون الدولى وتحديث آليات التعاون فى مواجهة الجرائم الإلكترونية

- سبل مواجهة صعوبات التعاون الدولى

فيما يتعلق بالعقبة الأولى المتمثلة فى عدم وجود نموذج موحد للنشاط الإجرامى، فإن الأمر يقتضى توحيد هذه النظم القانونية. ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولى يتفق مع طبيعة هذا النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلية، وتتمثل هذه الوسيلة فى تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم.

وفيما يتعلق بتنوع واختلاف النظم القانونية الإجرائية نجد أن المواثيق الدولية الصادرة عن الأمم المتحدة غالبًا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشىء الذى يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولى فعّال. فمثلا المادة (٢٠) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة ٢٠٠٠ تشير فى هذا الصدد إلى التسليم المراقب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة، والتى تعد من أهم التقنيات

المستخدمة فى التصدى للجماعات الإجرامية المنظمة بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد فى الملاحقات القضائية المحلية منها أو الدولية فى دول أطراف فى سياق نظم المساعدة القانونية المتبادلة[٦٧].

وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتى حيث نصت المادة (٢٩) على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكانى لذلك الطرف الآخر والتى ينوى الطرف طالب المساعدة أن يقدم طلبًا للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأى طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها.

كما أشارت المادة (٣١) من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأى طرف أن يطلب من أى طرف آخر أن يقوم بالتفتيش أو أن يدخل بأى طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكانى لذلك الطرف والتى يدخل فيها أيضًا البيانات المحفوظة وفقًا للمادة (٢٩)، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن فى حالة ما إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر الفقد أو التعديل.

فـى حـين نجـد أن المـادة (٣٢) مـن ذات الاتفاقيـة سـمحت بالـدخول للبيانات المخزنة خارج نطاق الحدود بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور.

وهناك أيضا المادة (٣٤) من الاتفاقية ذاتها والتى نصت على التعاون فى مجال التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التى تتم عن طريق إحدى شبكات المعلومات.

ونلاحظ مما سبق أن الاتفاقية الأوربية للإجرام المعلوماتى أوجدت بعض الحلول التى من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولى لمواجهة الجرائم المتعلقة بشبكة الإنترنت.

وللحد من ظاهرة عدم وجود قنوات اتصال بين جهات تطبيق القانون نلاحظ أنه غالبا ما تشجع الاتفاقيات الدولية الدول على التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير فى الحصول على هذه المعلومات وتبادلها، ومن الأمثلة على هذه الاتفاقيات اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية فى المادة (٢٧) منها، والمادة (٤٨) من إتفاقية الأمم المتحدة لمكافحة الفساد. والبند الثانى من المادة (٢٧) من الاتفاقية الأوربية بشأن الإجرام المعلوماتى، والمادة (٣٥) من ذات الاتفاقية الأوربية والتى أوجبت على الدول الأطرف فيها ضرورة تحديد نقطة اتصال تعمل لمدة ٢٤ ساعة يوميًا طوال أيام الأسبوع لكى تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم

البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكترونى، وهذه المساعدة تشمل:

- حفظ البيانات وفقًا للمادتين (٢٩)، (٣٠)، جمع الأدلة وإعطاء المعلومات ذات الطابع القضائى وتحديد أماكن المشتبه فيهم. كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر. وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربون القادرون على تسهيل عمل الشبكة.
- أما بالنسبة لمشكلة الاختصاص فى الجرائم الإلكترونية فثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائى خاصة بالنسبة للجرائم المتعلقة بالإنترنت[٦٨]، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير الذى تشهده تكنولوجيا المعلومات والاتصالات.

ولأجل القضاء على مشكلة التجريم المزدوج والذى يعد من أهم الشروط الخاصة بنظام تسليم المجرمين، ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة فى المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال والتى تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضى قوانين

الدولتين معًا، أو بمجرد السماح بالتسليم لأى سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة فى كل دولة.

وفيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ فى الرد فإننا نجد أن الحاجة ملحة إلى إيجاد وسيلة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعيين سلطة مركزية مثلًا أو السماح بالاتصال المباشر بين الجهات المختصة فى نظر مثل هذه الطلبات لنقضى على مشكلة البطء والتعقيد فى تسليم طلبات الإنابة. وهذا بالفعل ما أوصى به مؤتمر الأمم المتحدة الحادى عشر لمنع الجريمة والعدالة الجنائية والذى انعقد فى بانكوك فى الفترة من ١٨-٢٥/٤/٢٠٠٥م حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية فى أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات فى الوقت المناسب[٦٩]، والشىء نفسه نجده فى البند الثانى من المادة (٢٨) من الاتفاقية الأوربية بشأن الإجرام المعلوماتى. والمادة (٣٥) من ذا الاتفاقية الأوربية ذاتها والتى أوجبت على الدول الأطرف فيها ضرورة تحديد نقطة اتصال تعمل لمدة ٢٤ ساعة يوميًا طوال أيام الأسبوع لكى تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو لاستقبال الأدلة فى الشكل الإلكترونى عن الجرائم. كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر. وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربون القادرون على تسهيل عمل الشبكة.

أما بالنسبة للرد على طلبات التماس المساعدة فإنه من الضرورة بمكان الاستجابة الفورية والسريعة على هذه الطلبات، لأجل ذلك تنص غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة. وهذا ما أكدت عليه الفقرة الثالثة من المادة (٢٥) من الاتفاقية الأوربية للإجرام المعلوماتى حيث نصت على أنه: يمكن لكل طرف، فى الحالات الطارئة أن يوجه طلبًا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكترونى على أن تستوفى هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها (ويدخل ضمن ذلك الكتابة السرية إذا لزم الأمر) مع تأكيد رسمى لاحق إذا اقتضت الدولة المطلوب منها المساعدة فى ذلك. وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريعة.

أما فيما يتعلق بالصعوبات التى تواجه التعاون الدولى فى مجال التدريب فإنه يمكن التغلب عليها بإجراء المزيد من الحملات التوعوية للتنبيه بمخاطر الجرائم المعلوماتية والأضرار التى تسببها وبأهمية تدريب رجال العدالة الجنائية على مواجهتها، كما أنه وبمزيد من التنسيق بين الأجهزة المعنية بتدريب رجال تنفيذ القانون نرى ضرورة إيجاد برامج تدريبية مشتركة تناسب جميع الفئات. هذا بالإضافة إلى القيام ببعض العمليات المشتركة والتى من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر بشأنها.

- تحديث آليات التعاون

ذكرنا من قبل أن الجرائم الإلكترونية أضحت ترتكب فى بعض الأحوال على نحو عابر لحدود الدول. ذلك لأنه صار بالإمكان على سبيل المثال ارتكاب بعض أنماط السلوك التى تشكل الجرائم الإلكترونية فى إقليم دولة تقع فى جنوب شرقى قارة آسيا، فى حين تتحقق النتيجة فى إقليم دولة أخرى تقع فى شمال قارة أوروبا.

ويمكننا أن نضرب مثلًا لذلك، بإتلاف برامج الحاسب الآلى عن طريق استخدام الفيروسات الإلكترونية عن بعد؛ وقد أشرنا فى موضع سابق من هذا البحث، إلى أن الجرائم الإلكترونية العابرة لحدود الدول تثير إشكاليات قانونية عديدة، وتتسبب فى بروز عقبات فى طريق السلطات المختصة بالاستدلال والتحقيق والمقاضاة، خاصة فى مجالات المعاينة والضبط والتفتيش والبحث عن الأدلة وجمعها.

وجدير بالذكر هنا أن الدراسات التى أجريت خلال العقد الأخير من الزمن، فى شأن الجرائم الإلكترونية بوجه عام، تُفيد بشكل لا يدع مجالًا للشك، أن الاتفاقيات الدولية النافذة، الثنائية منها والإقليمية والجماعية على حد سواء، توجد فيها نقاط ضعف رئيسية، وتعانى من ثغرات قانونية خطيرة، جعلت هذه الاتفاقيات عاجزة بوضعها الراهن عن تحقيق المواجهة الجنائية الفعالة للجرائم الإلكترونية.

وفضلًا عما تقدم، فإن كل الجهود التى بذلت من قبل المنظمات الإقليمية والدولية، فى الثمانينيات والتسعينيات من القرن الماضى، وأوائل القرن

الحالى، لم تؤد إلى تحقيق نتائج ملموسة وفعالة تلبّى كل الطموحات فى هذا المجال.

والواقع أن غياب المواجهة القانونية الدولية – القوية الفعّالة – لمرتكبى الجرائم الإلكترونية العابرة لحدود الدول، أغرى مرتكبى هذه الجرائم على تنظيم أنفسهم فى شكل عصابات إجرامية، دون تقيّد بالحدود الجغرافية، وذلك مكّنهم أيضًا من الإفلات من الملاحقة والعقاب بشكل آمن بالنسبة لهم، وبشكل يُنذر بخطر كبير وعلى نحو يبعث على القلق الشديد فى نفس الوقت لجهة المجتمع الدولى، لذلك أضحى من الضرورى، إزاء هذا الوضع أن تسعى جميع الدول من أجل إيجاد صيغ ملائمة للتعاون الدولى فيما بينها، بهدف التصدى لهذه الجرائم، بحسبان أن التعاون الدولى هو السبيل الوحيد والمخرج الأمثل لمعالجة المشكلات القائمة ذات الصلة بالحماية الجنائية فى مواجهة جرائم الحاسب الآلى على المستوى الدولى.

لذلك فعلى الدول أن تكثف جهودها بهدف تحقيق تعاون أكبر فى مجال تسليم المجرمين، والتنفيذ المتبادل للأحكام القضائية، والإنابات القضائية. وكذلك تبادل المساعدة بين أجهزة العدالة الجنائية فيها. وكذلك أيضًا تبادل الخبرات والمعلومات حول مرتكبى الجرائم الإلكترونية، وملاحقتهم وضبطهم، وتضييق دائرة إفلاتهم من العقاب قدر الإمكان، وذلك من خلال ما يلى:

أ - اقتراحات بشأن تعزيز التعاون الإقليمي والدولي في مجال الجرائم الإلكترونية

أشرنا من قبل إلى أن الجرائم الإلكترونية تتميز في الوقت الراهن بأن لها بعدًا دوليًا، لأنها أضحت لا تعترف بالحدود بين الدول، ولا بالمسافات بين القارات. وتفصيل ذلك أن الحدود الفاصلة بين الدول غير قادرة البتة نتيجة للتطور التقني السريع والمطرد في مجال المعلوماتية على الحيلولة دون اختراق نظم المعالجة الآلية للمعلومات من الخارج، وتحديدًا انطلاقًا من أماكن تبعد آلاف الأميال عن مكان تحقق النتيجة، وربما يكون أوضح مثال على ذلك أن يقوم أحد الهواة أو المحترفين الذي يقيم في إحدى دول جنوب شرق آسيا بإدخال فيروسات إلكترونية (نظام برمجي تخريبي) في نظام إحدى الحواسب الآلية الموجودة في الدولة التي يقيم فيها، فتنتقل عدوى الفيروسات بسرعة مدمرة لتصيب البرامج في شتى أنحاء الشبكة الدولية في أوروبا وأمريكا الشمالية واليابان على سبيل المثال، بالدمار أو العطل وهذا من شأنه أن يفسح المجال لبروز عدة إشكاليات، ولعل أبرز مشكلات القانون الجنائي التي أثارتها وقائع ارتكاب جريمة من الجرائم الإلكترونية العابرة لحدود الدول (عبر الوطنية) تكمن في تحديد ضوابط الاختصاص القضائي، وكذلك تنظيم إجراءات المعاينة والضبط والتفتيش وجمع الأدلة وغيرها، والحق أن جهودًا مبكّرة نسبيًا، ولكنها متواضعة ومحدودة في الوقت نفسه بذلت على المستويين الإقليمي والدولي خلال العقود الثلاثة الأخيرة من الزمن سعيًا لرسم إطار عام للمشكلة، واستقصاء الحلول الممكنة لتكون خطوطًا إرشادية للمشرعين وواضعي السياسة

الجنائية فى مختلف الدول فى هذا الشأن غير أن تلك الجهود لم تفلح -حسب ما تؤكده الدراسات التى أجريت بشأنها - فى الوصول إلى تحقيق الهدف المنشود لأسباب عديدة لا يتسع المقام لذكرها ولكننا نكتفى بالإشارة فحسب إلى أن تلك الجهود كانت لمنظمات دولية إقليمية أو مؤتمرات علمية أو منظمات دولية فرعية متخصصة، وبالتالى فهى لم تكن تمثل جهدًا جماعيًا شاركت فيه كافة الدول الأعضاء فى الأمم المتحدة.

وفى ضوء ما تقدم أضحى من الواضح تمامًا أن وقائع الجرائم الإلكترونية العابرة لحدود الدول، يكاد يكون من شبه المستحيل ملاحقة مرتكبيها وضبطهم وجمع أدلة الجريمة بدون أن تمتد هذه الإجراءات إلى خارج الحدود، وكما أنه بات من الواضح أيضًا أن ذلك يتطلب بالضرورة وبحكم الواقع وطبيعة العلاقات بين الدول إيجاد صيغ مناسبة لتعاون قضائى جنائى دولى فعّال ومستمر، وبشرط أن تسهم فى تحقيقه كل الدول الأعضاء فى الأمم المتحدة.

وصفوة القول إن عولمة هذا النوع من الإجرام المستحدث العابر لحدود الدول تستتبع بالضرورة عولمة التصدى له - إذا جاز التعبير.

ب - اقتراحات بشأن تعزيز التعاون الإقليمى بين الدول العربية فى مجال الجرائم الإلكترونية

أما على المستوى الإقليمى وفيما يختص بالعالم العربى، فلا مناص من الإقرار بأن التعاون العربى الإقليمى هو اللبِنة الأولى والركيزة الأساسية فى مواجهة هذا النوع من الجرائم نظرًا لأنها غالبًا ما تتم من أماكن مُختلِفة وباستخدام تقنيات

حديثة، ومن ثم فإن المنطِقة العربية فى حاجةٍ ماسةٍ إلى إرساء وتعزيز آليات التعاون بين دول المنطِقة بهدف مُكافحة هذا النوع من الجرائم التى بدأت تستشرى فى الكيان العربى، لاسيما فى ظِل عدم وجود أية قوانين خاصة بمُكافحتِها أخذًا فى الاعتبار أن قائمة الدول المُصنفة وفقًا لاتفاقية مجلس أوروبا بشأن الإجرام السيبيرى تحت بند «لديها قوانين فعالة ومُتطورة» لا تتضمن أى من الدول العربية. وجديرٌ بالذِكر أن هناك محاولات جادة لإصدار اتفاقية خاصة بالتعاون الإقليمى العربى فى مجال مكافحة الجرائم التى تتم باستخدام الكمبيوتر أو شبكة الإنترنت، علاوة على صدور القانون العربى الاسترشادى النموذجى لمكافحة جرائم تقنية أنظمة المعلومات وما فى حكمها بيد أن هذا المشروع لم ير النور بعد؛ وقد ألمحنا من قبل إلى أن غالبية التشريعات العربية – باستثناء بعض الدول ومنها عُمان التى بادرت بإصدار قانون خاص بشأن جرائم الحاسب عام ٢٠٠١، وكذلك دولة الإمارات العربية المتحدة التى بادرت هى الأخرى بإصدار قانون بشأن مكافحة جرائم تقنية المعلومات عام ٢٠٠٦، وقطر التى أصدرت قانون بشأن مكافحة جرائم تقنية المعلومات عام ٢٠١٤– ما تزال تعانى من عجز كبير، واتساع مستمر فى دائرة الفراغ التشريعى الذى يعيبها فى مجال الحماية الجنائية لبرامج الحاسب الآلى فى الوقت الراهن؛ وأشرنا أيضًا إلى أن ذلك كله انعكس سلبًا وبشكل خطير على مدى قدرة وفاعلية تلك التشريعات على الصعيدين الموضوعى والإجرائى على حد سواء، فضلا عما يعانيه رجال القضاء والنيابة فى البلدان

العربية حاليًا من مشكلات قانونية فى مجال التحقيقات والمحاكمات ذات الصلة بجرائم الاعتداء على برامج الحاسب الآلى بسبب ذلك الفراغ.

ومما لا شك فيه أن غياب التدخل السريع والمباشر والصريح من جانب المشرع الوطنى فى كل دولة عربية لسد الثغرات التشريعية القائمة، كان من نتائجه الحتمية تفاقم الأزمة، وتزايد عدد هذه الثغرات الموجودة مع مرور الوقت.

وفى ضوء ما تقدم، نقترح على جهات الاختصاص فى الدول العربية بعض الأفكار، التى نأمل أن تسهم مع غيرها فى وضع أسس تعاون عربى فعّال فى هذا المجال، وفيما يلى تفصيل ذلك:

- نوصى بالعمل على تشكيل لجان وطنية فى كل الدول العربية تتولى حصر ودراسة الإشكاليات القانونية الناشئة عن التعامل مع الجرائم التى تشكل صورة من الجرائم الإلكترونية بوجه عام، ومحاولة اقتراح حلول له.
- توظيف نتائج الدراسات التى ستتوصل إليها اللجان الوطنية المشار إليها سلفًا فى عقد مؤتمر دولى إقليمى عربى يعنى بوضع مشروع اتفاقية عربية خاصة بالتعاون فى مجال الجرائم الإلكترونية.
- عرض مشروع الاتفاقية المذكورة أعلاه لاحقًا، وفقا للآلية المتبعة فى جامعة الدول العربية على مجلس وزراء العدل العرب لمناقشة-المشروع ليكون نموذجًا يحتذى به المشرع الوطنى فى كل دولة عربية.

- توحيد المصطلحات العربية المستخدمة فى مجال الجرائم الإلكترونية بوجه عام، ذلك أن اختلاف المصطلحات من شأنه أن يفسح المجال لاختلاف التفسير أيضًا.
- من المهم التنويه أيضًا أنه من المفيد والضرورى أن تحرص جهات الاختصاص فى كل دولة عربية على تبادل الخبرات، والاستفادة قدر الإمكان من تجارب الدول التى لها رصيد تراكمى سابق فى مجال المواجهة القانونية للجرائم الإلكترونية.

جـ - اقتراحات بشأن تطوير التعاون على المستوى الدولى فى مجال الجرائم الإلكترونية

ذكرنا من قبل أن الجرائم الإلكترونية أضحت ترتكب فى بعض الأحوال على نحو عابر لحدود الدول، ذلك لأنه صار بالإمكان على سبيل المثال ارتكاب بعض أنماط السلوك التى تشكل جريمة فى إقليم دولة تقع فى جنوب شرقى قارة آسيا، فى حين تتحقق النتيجة فى إقليم دولة أخرى تقع فى شمال قارة أوروبا. وبالتالى الجرائم الإلكترونية العابرة لحدود الدول تثير إشكاليات قانونية عديدة، وتسبب فى بروز عقبات شديدة فى طريق السلطات المختصة بالاستدلال والتحقيق والمقاضاة، خاصة فى مجالات المعاينة والضبط والتفتيش والبحث عن الأدلة وجمعها، وكذلك فى مجال تحديد الاختصاص من حيث المكان وغير ذلك.

وجدير بالذكر هنا أن الدراسات التى أجريت خلال العقد الأخير من الزمن، فى شأن الجرائم الإلكترونية بوجه عام، تُفيد بشكل لا يدع مجالًا للشك، أن الاتفاقيات الدولية النافذة، الثنائية منها والإقليمية والجماعية على حد سواء، توجد فيها نقاط ضعف رئيسية، وتعانى من ثغرات قانونية خطيرة، جعلت هذه الاتفاقيات عاجزة بوضعها الراهن عن تحقيق الحماية الجنائية الفعالة.

وفضلًا عما تقدم، فإن جميع الجهود التى بذلت من قبل المنظمات الإقليمية والدولية، فى الثمانينيات والتسعينيات من القرن الماضى، وأوائل القرن الحالى، لم تؤدى إلى تحقيق نتائج ملموسة وفعالة تلبّى كل الطموحات فى هذا المجال.

والواقع أن غياب المواجهة القانونية الدولية – القوية الفعّالة – لمرتكبى الجرائم الإلكترونية العابرة لحدود الدول، أغرى مرتكبى هذه الجرائم على تنظيم أنفسهم فى شكل عصابات إجرامية، دون تقيّد بالحدود الجغرافية، وذلك مكّنهم أيضًا من الإفلات من الملاحقة والعقاب بشكل آمن بالنسبة لهم، وبشكل يُنذر بخطر كبير وعلى نحو يبعث على القلق الشديد فى الوقت نفسه لجهة المجتمع الدولى.

لذلك أضحى من الضرورى، إزاء هذا الوضع أن تسعى كافة الدول من أجل إيجاد صيغ ملائمة للتعاون الدولى فيما بينها، بهدف التصدى لهذه الجرائم، بحسبان أن التعاون الدولى هو السبيل الوحيد والمخرج الأمثل لمعالجة المشكلات القائمة ذات الصلة بالحماية الجنائية ضد الجرائم الإلكترونية على المستوى الدولى.

تتمثل أهم المقترحات فى هذا المجال فيما يلى:

- على الدول الأعضاء فى الأمم المتحدة، أن تكثف جهودها بهدف تحقيق تعاون أكبر فى مجال تسليم المجرمين، والتنفيذ المتبادل للأحكام القضائية، والإنابات القضائية. وكذلك تبادل المساعدة بين أجهزة العدالة الجنائية فيها. وكذلك أيضًا تبادل الخبرات والمعلومات حول مرتكبى الجرائم الإلكترونية، وملاحقتهم وضبطهم، وتضييق دائرة إفلاتهم من العقاب قدر الإمكان.
- أن تتبنى جميع الدول الأعضاء فى الأمم المتحدة فكرة الدعوة إلى أن تصدر الجمعية العامة للأمم المتحدة قرارًا تكلف بموجبه لجنة القانون الدولى التابعة للأمم المتحدة بإعداد مشروع اتفاقية دولية فى شأن التعاون الدولى فى مجال الجرائم الإلكترونية، وطرح مشروع هذه الاتفاقية بعد إنجازه على مؤتمر دولى تنظمه ليصبح اتفاقية دولية.
- أن تبادر الأمم المتحدة بتبنّى (مشروع اتفاقية نموذجية) غير ملزمة لأية دولة، ولكنها إرشادية للمشرعين الوطنيين فحسب، تُعنى بوضع الأسس والعناصر الرئيسية لضمان التعاون الدولى فى مجال الجرائم الإلكترونية، والواقع أن ما ندعو إليه ليس بدْعًا من جانبنا، فقد سبق للأمم المتحدة أن تبنّت بموجب قرار صدر عنها عام (١٩٩٣) مشروع اتفاقية نموذجية بشأن تسليم المجرمين، أعدّ مشروعها مؤتمر الأمم المتحدة الثامن للجريمة ومعاملة المجرمين الذى عقد فى مدينة ميلانو بإيطاليا خلال العقد الأخير من القرن الماضى.

- الاعتراف فى بعض الحالات بحجية للتشريعات والأحكام الجنائية غير الوطنية: القاعدة التقليدية هى تلازم السيادتين التشريعية والقضائية فى المجال الجنائى، بما يعنى أن كل دولة لا تعترف سوى بأحكام قانونها الجنائى الوطنى، ولا تعتد، ولا تنفذ على إقليمها سوى الأحكام الجنائية الصادرة عن إحدى محاكمها الوطنية، ويجد ذلك سنده فى أن تطبيق القانون الجنائى يُعد تعبيرًا عن سيادة الدولة بوصفه يحمى المصالح الأساسية للمجتمع والدولة والحقوق. الجوهرية لأفراده، إضافة إلى أن قواعد القانون الجنائى تتعلق فى جملتها بالنظام العام، وهو ما يحول دون الخضوع لحكم قانون أجنبى وتطبيقه، أما فيما يتعلق بحجية الأحكام الجنائية الأجنبية فى شقها الإيجابى. فإنه يجب أن يُفسَحَ لها مكانٌ بين أحكام المعاهدات الدولية ذات الصلة، وهكذا يمكن أن يؤخذ فى الاعتبار بالآثار الجنائية غير المباشرة للأحكام الجنائية الأجنبية لاسيما فى الاعتبار بالآثار الجنائية غير المباشرة للأحكام الجنائية الأجنبية لاسيما فى مجال العود، ووقف التنفيذ وتقدير العقوبة فى ضوء ما يثبت من الخطورة الإجرامية للجانى، أما بالنسبة لحجية الأحكام الجنائية فى شقها السلبى، فقد اعترف بها بعض المشرعين، إذ يمتنع إقامة الدعوى الجنائية ضد من ارتكب جريمة فى الخارج متى ثبت أن المحاكم الجنائية الأجنبية قد برأته أو أدانته نهائيًا واستوفى عقوبته، فكأن هؤلاء المشرعين يعترفون بقوة الشىء المحكوم فيه ولو

تعلق الأمر بحكم أجنبى تطبيقًا لقاعدة امتناع محاكمة الشخص عن ذات الفعل مرتين.

ونعتقد أنه حان الأوان لتجاوز بعض المفاهيم التقليدية، وخاصة فيما يتعلق بتلازم السيادتين التشريعية والقضائية فى المجال الجنائى، وذلك بالتوجه نحو الاعتراف فى بعض الحالات وعلى نحو ما بحجية لتشريع جنائى عبر وطنى، بل وبحجية لحكم جنائى صادر عن محاكم دولة أخرى، وتتجلى أهمية ذلك على وجه الخصوص فى مجال الجرائم التبعية التى تفترض ارتكاب جريمة أصلية على إقليم الدولة ما، ثم وقوع الجريمة التابعة على إقليم دولة أخرى، ومثال ذلك جريمة الاعتداء على الملكية الفكرية، وقد ظهرت أفكار تنادى بوجوب الاعتراف فيما بين الدول بحجية للأحكام الجنائية الأجنبية على إقليم الدول الأخرى وحجة ذلك استفحال ظاهرة الجرائم الإلكترونية وضرورة تعاون دولى فيما بينها لمكافحتها حتى لا يفلت مرتكبوها من العقاب لمجرد أنهم أقاموا فى دولة غير تلك التى صدر ضدهم فيها حكم جنائى بالإدانة وصار ممكنًا الاعتراف بمثل هذه الحجية استنادًا إلى معاهدة دولية تبرم بين الدول.

المراجـــع

١ – نائلة عادل محمد فريد قورة، الجرائم الإلكترونية الاقتصادية، بيروت، لبنان، منشورات الحلبى الحقوقية، ٢٠٠٥، ص ٢٤٦.

٢ – يونـس عـرب، جرائم الكمبيوتر والإنترنت، المعنى والخصائص والصور واستراتيجية المواجهة القانونية، ص ٣١٧.

www.arablaw.org/Download/cybe crimes- General.doc

٣ – محمد فتحى عيد، الإنترنت ودوره فى إنتشار المخدرات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣، ص ١٩٤.

٤ – اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم (٥٥/٦٣)، الصادرة عن هيئة الأمم المتحدة، الجلسة العامة ٨١، ديسمبر ٢٠٠٠.

٥ – اللجنة الاقتصادية والاجتماعية لغربى آسيا (الإسكوا)، ورشة عمل حول التشريعات الإلكترونية تطبيقها فى منطقة الإسكوا، بيروت ١٥–١٦ ديسمبر ٢٠٠٨.

٦ – مؤتمر هيئة الأطراف فى اتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية، المنعقد بفيينا فى ١٨–٢٢ أكتوبر ٢٠١٠.

٧ – أنشطة مكتب الأمم المتحدة المعنى بالمخدرات والجريمة فى مجال التصدى للأشكال المستجدة من الجريمة، مؤتمر الأطراف فى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، فيينا، ١٨–٢٢ أكتوبر ٢٠١٠.

٨ – اتفاقية حقوق الطفل، النظر فى التقارير المقدمة من الدول بموجب الفقرة ١ من المادة ١٢ من البروتوكول الاختيارى لاتفاقية حقوق الطفل المتعلق ببيع وبغاء الأطفال فى المواد الإباحية، لجنة حقوق الطفل، الدورة السابعة والخمسون، ٢٠١١.

٩ – موقع منظمة التعاون الاقتصادى والتنمية http//:www.oecd.org.

١٠ – دليل البلدان النامية فى فهم الجريمة الإلكترونية، شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن المعلوماتى، دائرة السياسات والإستراتيجيات، قطاع تنمية الاتصالات، الصادر عن الاتحاد الدولى للاتصالات، أبريل ٢٠٠٩، ص٩٤.

12 - Ulrich Sieber, Computer Crimes, Cybers Terrorism, Child Pornography and Financial Crimes General (Report), April 2003, pp. 22-25.

– انظر أيضًا: عواطف محمد عثمان عبد الحليم، جرائم المعلوماتية تعريفها وصورها، جهود مكافحتها، مجلة العدل، العدد الرابع والعشرون، السنة العاشرة، ص ٥٠.

12 – Les rédacteur de la convention sur la cybercriminalité du Conseil de l'Europe se sont voulus plus proches de l'opinion du droit réel, estimant que le seul aspect spécifique de la cybercriminalité est l'utilisation des TIC comme moyen de commetter un délit. La Convention, qui est entrée en vigueur le ler juillet 2004, constitue le prinsipal insterument international dans ce domaine, voir: KURBALIJA jovan GELBESTEIN Eduardo, op. cit, p. 98.

١٣ – دانيال لاركين، محاربة جرائم الإنترنت، بحث مترجم ومنشور، بتاريخ ٢٠٠٨/٥/١٧، تاريخ الزيارة ٢٠١٥/٢/١ http://iipdigital.usembassy.gov/st/arabic.

١٤ – لمزيد من التفاصيل انظر: بحث محاربة جرائم الإنترنت، المرجع السابق.

١٥ – لمزيد من التفاصيل انظر: التعاون مع المنظمات الدولية، موقع:
http://www.iap-association.org/Arabic

١٦ – دليل فهم الجريمة السيبرانية للدول النامية، المرجع السابق، ص ٨٤.

١٧ – الجريدة الرسمية، السنة ٥٧، العدد ٤٦، ٢٠١٤/١١/١٣، ص ٣.

١٨ – فايز عبد الله الشهرى، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة – دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف للعلوم الأمنية، المجلد ٢٠، العدد ٣٩، ٢٠٠٥، ص ٢١، أنظر أيضًا: براء منذر كمال عبداللطيف، شرح قانون أصول المحاكمات الجزائية، عمان، دار الحامد، ٢٠٠٩.

١٩ – المؤتمر العلمى الأول حول العالم الرقمى وجرائم الشبكات الإلكترونية، عددًا من الموضوعات تتعلق بصفة عامة بالمواجهة الموضوعية والإجرائية للجرائم الإلكترونية، وجاء ذلك فى ستة محاور.

٢٠ – عبدالله عبدالكريم، جرائم الكمبيوتر والإنترنت: الجرائم الإلكترونية، لبنان، منشورات الحلبى الحقوقية، ٢٠٠٧، ص ٩٤ وما بعدها.

٢١ – سالم محمد سليمان الأوجلى، أحكام المسئولية الجنائية عن الجرائم الدولية فى التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٩٩٧، ص ٤٢٥.

٢٢ – المادة (٥) من اتفاقية الرياض العربية للتعاون القضائى ١٩٨٣.

٢٣ – مادة (٣٠) من القانون المذكور: فى حالة تلقى طلب من دولة أجنبية للحصول على مساعدة قانونية متبادلة، تتعلق بالجرائم المنصوص عليها فى هذا القانون، يكون تنفيذ ذلك الطلب طبقًا للقواعد التى يحددها هذا الفصل.

وتتضمن صور المساعدة القانونية المتبادلة، بشكل خاص.

٢٤ – صدرت هذه المعاهدة فى ١٩٩٠/١٢/١٤ فى الجلسة العامة ٦٨ للجمعية العامة للأمم المتحدة. وتقضى باتفاق أطرافها على أن يقدم كل منهم للأخر أكبر قدر ممكن من المساعدة المتبادلة فى التحقيقات، أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا فى اختصاص السلطة القضائية فى الدولة الطالبة للمساعدة.

٢٥ – صدرت هذه المعاهدة واعتمدت عام ١٩٩٩ من قبل مؤتمر وزراء خارجية دول المنظمة فى اجتماعهم المنعقد فى أواغادوغو فى الفترة من ١٩٩٩/٦/٢٨ إلى ١٩٩٩/٧/١.

٢٦ – اعتمد هذا النموذج من المجلس الأعلى لمجلس التعاون الخليجى فى دورته الرابعة والتى انعقدت بدولة الكويت فى الفترة من ٢١-٢٠٠٣/١٢/٢٢.

٢٧ – سالم محمد سليمان الأوجلى، المرجع السابق، ص ٤٢٧.

٢٨ – اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة ٤٥/١١٨ بتاريخ ١٩٩٠/١٢/١٤، وتتكون من خمس عشرة مادة تنظم خلالها كيفية نقل الإجراءات بين الدول من خلال بيان الوثائق المطلوبة، والشروط اللازم توافرها لإمكانية النقل وأثر نقل الإجراءات على الدولة الطالبة والدولة المطالبة وغيرها من التفاصيل التى تثيرها عملية نقل الإجراءات بين الدول.

٢٩ – حسنين إبراهيم عبيد، التعاون الدولى فى مجال مكافحة الجريمة، مقال منشور بمجلة القانون والاقتصاد، السنة ٥٣، ١٩٨٣، ص٢٦٤.

٣٠ – جميل عبد الباقى الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، القاهرة، دار النهضة العربية، ٢٠٠٢، ص٨٣.

٣١ – أحمد عبد الحليم شاكر على، دور الإنابة القضائية الدولية فى مكافحة الجريمة، بحث منشور فى مجلة الفكر الشرطى، المجلد (١٧)، العدد ٤، ٢٠٠٨، ص ١٥٣.

٣٢ – أنظر مثلا المادة (٢) من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات فى المسائل الجنائية ١٩٩٠ والمادة (٧) من النموذج الاسترشادى لاتفاقية التعاون القانونى والقضائى الصادر عن مجلس التعاون الخليجى ٢٠٠٣.

٣٣ – نقض ١٣ أكتوبر سنة ١٩٦٩ مجموعة أحكام النقض س٢٠، ص ١٠٦٩ رقم ٢١٠ وفيه قضت المحكمة بإمكانية سماع الشاهد المقيم فى الخارج عن طريق الإنابة الدولية.

٣٤ – المادة الثانية من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات فى المسائل الجنائية ١٩٩٠، البند الأول من المادة (٣٠) من معاهدة منظمة المؤتمر الإسلامى لمكافحة الإرهاب الدولى ١٩٩٩م، المادة (٩) من النموذج الاسترشادى لاتفاقية التعاون القانونى والقضائى الصادر عن مجلس التعاون الخليجى ٢٠٠٣.

٣٥ – جميل عبد الباقى الصغير، مرجع سابق، ص٨٦.

٣٦ – تعزيز التعاون الدولى فى إنفاذ القانون، وثيقة سبق الإشارة إليها، ص٣٣.

37 - Recommendation No.R (95)13,of the Committee of Ministers Team Member States Concerning Problems Criminal Procedure Law Connected with Information Technology" Adopted by the Committee of Ministers on 11 September 1995 at the 543.

٣٨ – جميل عبد الباقى الصغير، مرجع سابق، ص ٨٣.

39 - General Principles Relating to International Co-Operation (article 23).

٤٠ – محمد أبو العلا عقيدة، التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية بأكاديمية شرطة دبى، مركز البحوث والدراسات عدد رقم (٤) المنعقد فى الفترة من ٢٦–٢٨ ابريل ٢٠٠٣، دبى، الإمارات العربية المتحدة، ص ٢٤.

٤١ – هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائى الفنى، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، فى الفترة ١–٣ مايو ٢٠٠٠، المجلد الثانى، الطبعة الثالثة، ٢٠٠٤، ص ص ٤٣٩–٤٤٠.

٤٢ – فى تعريف التدريب انظر: صالح محمد النويجم، تقويم كفاءة العملية التدريبية فى معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها، رسالة ماجستير فى العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٥، ص ٩.

٤٣ – صالح محمد النويجم، المرجع السابق، ص ٧.

٤٤ – مثال ذلك التوصية الصادرة من اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية بدول مجلس التعاون الخليجى، الاجتماع الأول المنعقد بالأمانة العامة للمجلس بالرياض بالمملكة العربية السعودية فى الفترة من ٤ –٥ أبريل ٢٠٠٤، البند "د" من القرار الصادر بشأن الجرائم ذات الصلة بالحاسب الآلى – من مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة السجناء – هافانا.

٤٥ – محمد السيد عرفة، تدريب رجال العدالة وأثره فى تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٥، ص ٢.

٤٦ – هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائى الفنى وآليات التدريب التخصصى للمحققين، مرجع سابق، ص ٤٩٦.

٤٧ – هشام محمد فريد رستم، المرجع السابق، ص ٤٩٧.

48 - Donn B. Parker, Fighting Computer Crime, Charles Scribner Son, New York,1983, p. 231. Virginia. Quantico. Sieber. Urlich, op. cit. p. 143. Donnb. Parker: op. cit., p. 239 and Sieber. Urlich, op. cit., p. 143.

٤٩ – انظر: هشام محمد فريد رستم، مرجع سابق.

٥٠ – المعهد القضائى، مجلة القسطاس، العدد العاشر، جمهورية السودان، سبتمبر ٢٠٠٣، ص ٢٧٥.

٥١ – من أمثلة على ذلك:

- المؤتمر الدولى الأول لقانون الإنترنت، الغردقة، جمهورية مصر العربية، الفترة من ٢١ – ٢٥ أغسطس ٢٠٠٥، المنظمة العربية للتنمية الإدارية.
- المؤتمر الدولى لأمن المعلومات الإلكترونية، مسقط، سلطنة عمان، الفترة من ١٨ – ٢٠ ديسمبر ٢٠٠٥، المنظمة العربية للتنمية الإدارية.
- ورشة العمل الإقليمية، تطوير التشريعات فى مجال مكافحة الجرائم الافتراضية، مسقط، سلطنة عمان، الفترة من ٢ – ٤ أبريل ٢٠٠٦، هيئة تنظيم الاتصالات العمانية، مركز التميز العربى التابع للاتحاد الدولى للاتصالات.

٥٢ – انظر: علاء الدين محمد شحاتة وآخرون، دور وزارة الداخلية فى تدريب ضباط الشرطة غير المصريين، بحث مقدم لمعهد تدريب ضباط الشرطة، أكاديمية الشرطة، القاهرة، ١٩٨٧.

٥٣ – بروس سوارتز، موقع وزارة الخارجية الأمريكية، الصفحة الإعلامية، بتاريخ ٢٠٠٦/٨/٢٦.

http://usinfo.state.gov/journals/itgic/0801/ijga/art3.htm.

٥٤ – فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية – دراسة مقارنة، بيروت، منشورات الحلبى القانونية، ٢٠١٠، ص ٢١٥.

٥٥ – عبد الفتاح بيومى حجازى، الدليل الجنائى والتزوير فى جرائم الكمبيوتر والإنترنت، دراسة متعمقة فى جرائم الحاسب الآلى والإنترنت، الزقازيق، بهجت للطباعة والنشر، ٢٠٠٩، ص١٠٢.

٥٦ – براء منذر كمال عبد اللطيف؛ ناظر أحمد منديل، التعاون القضائى الدولى فى مواجهة جرائم الإنترنت، المؤتمر العلمى الأول حول تحولات القانون العام فى مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، ٢٠٠٩، ص١١.

57 - Rapport explicatif concernant la convention du 29 mai 2000 relative a l'entraide judiciaire en matiere penale entre les Etats members de l'Union europeene- Texte approuve par le Conseil le 30 novembre 2000, op. cit., p. 1 et s.

58 - Rapport explicatif, op. cit., p. 2. De Baynast (O.): La future convention d'entraide penale entre les Etats de l'Union europeenne, op. cit., p. 15.

59 - Rapport explicatif, op. cit., p. 10.

– انظر إلى: عادل يحيى قرنى، تقنية الاتصال المرئى المسموع وسيلة للتحقيق والمحاكمة الجنائية عن بعد، مجلة الفكر الشرطى، مجلد ١٨، العدد ٧١، ٢٠٠٩، ص٥٠.

٦٠ – عادل يحيى قرنى، المرجع السابق، ص ٥٢.

٦١ – عمر سالم، الإنابة القضائية الدولية فى المسائل الجنائية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، ٢٠٠١، ص١٩٥.

٦٢ – عادل يحيى قرنى، مرجع سابق، ص ص ٥٣ – ٥٤.

٦٣ – عادل يحيى قرنى، المرجع السابق، ص ٥٥.

٦٤ – حسين بن سعيد بن سيف الغافرى، الجهود الدولية فى مواجهة الجرائم الإلكترونية، ص ٤٣، تاريخ الزيارة١٠/٢/٢٠١٣.

www.minshawi.com/vb/attachment.php?attachmentid

٦٥ – جميل عبد الباقى الصغير، مرجع سابق، ص ٩١.

٦٦ - براء منذر كمال؛ ناظر أحمد منديل، التعاون القضائى الدولى فى مواجهة جرائم الإنترنت، مرجع سابق، ص ١٢.

٦٧ - انظر ما جاء بتوصية المجلس الأوربى رقم (R95)13 الصادرة فى ١١ سبتمبر ١٩٩٩ بشأن مشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات.

٦٨ - مؤتمر الأمم المتحدة الحادى عشر لمنع الجريمة والعدالة الجنائية، تدابير مكافحة الجرائم المتصلة بالحواسيب، المنعقد فى بانكوك فى الفترة ١٨-٢٥ أبريل ٢٠٠٥.

٦٩ - أنظر: براء منذر كمال عبد اللطيف، ناظر أحمد منديل، التعاون القضائى الدولى فى مواجهة جرائم الإنترنت، مرجع سابق، ص ١٥.

INTERNATIONAL JUDICIAL COOPERATION IN THE FIELD OF ELECTRONIC CRIMES

Hend Naguib

The invention of the computer and its connection with the internet is considered one of the most important achievements in the recent epoch. It played an important role in the globalization, making cultures closer and removing restrictions and geographical borders among people, but some professionals used it as a clever way to commit new types of crimes that are difficult to be discovered or to find sufficient clues to their committers.

In the epoch of technology and modern communication revolution, the crime becomes complicated and uses different ways as it benefits from the technical development appeared such as the electronic or technical crimes; that is why the judicial cooperation on the international level is very important to combat these crimes which cross all borders.