وزارة التعليم العالي والبحث العلمي
جامعة العربي التبسي– تبسة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر:

تخصص: قانون جنائي

المساعدة القضائية المتبادلة لمكافحة الجريمة الإلكترونية

إعداد الطالب:
زايدي توفيق

إشراف الأستاذة:
شعبان لامية

أعضاء لجنة المناقشة

اللقب والإسم	الرتبة العلمية	الصفة في البحث
شارني نوال	أستاذ مساعد –أ–	**رئيسـا**
شعبان لامية	أستاذ مساعد –أ–	**مشرفا ومقررا**
بوعزيز عبد الوهاب	أستاذ محاضر–ب–	**ممتحنـا**

السنة الجامعية: 2018/2017

بسم الله الرحمن الرحيم

الكلية لا تتحمل أي مسؤولية على ما يرد

في هذه المذكرة من آراء

شكر وعرفان

قال الله تعالى " وَإِذْ تَأَذَّنَ رَبُّكُمْ لَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ وَلَئِنْ كَفَرْتُمْ إِنَّ عَذَابِي لَشَدِيدٌ"

الآية 07 من سورة إبراهيم.

الشكر و الحمد للعلي القدير إذ سدد خطانا في إتمام هذا العمل المتواضع نتقدم بجزيل

الشكر و عظيم الامتنان لأستاذتنا الفاضلة شعبان لامية لتشريفنا بقبولها الإشراف على مذكرتنا،

لصبرها و تعاونها معنا، ولملاحظاتها القيمة وتوجيهاتها السديدة، فلها منا كل التقدير والإحترام،

ونسأل المولى عز وجل أن يمتعها بدوام الصحة و العافية.

كما نتقدم من الأستاذ الدكتور "بوعزيز عبد الوهاب " بعظيم الشكر والعرفان لتفضله بقبول

ترؤس لجنة المناقشة. الذي لطالما كان خير مثال لإلمامه بكافة خبايا القانون، سائلين من الله عز

وجل أن يحفظه و يديم عطائه.

كما نتقدم من القامة العلمية الدكتورة "شارني نوال" بخالص الشكر و الإمتنان لتكرمها بقبول

عضوية لجنة المناقشة والحكم على مذكرتنا، سائلين المولى عز وجل أن يحفظها.

مقدمة

نعيش اليوم في ظل عالمٍ جديدٍ تتداخل فيه المصالح وتتنوع فيه الأزمات، حيث لم تعد الدولة تستطيع تأمين هذه المصالح ومواجهة تلك الأزمات بمعزل عن بقية الدول، لذلك ظهرت الحاجة الملحة للتعاون فيما بينها في شتى المجالات، بما في ذلك التعاون في المسائل الجنائية لمكافحة الجريمة.

وقد نشأت الجريمة كظاهرة اجتماعية منذ بداية التاريخ البشري، حيث لا يخلو منها مجتمع، وليست محصورة في فئة أو وسط اجتماعي محدد، وهي أيضا ليست مرتبطة بوقت أو فترة معينة، إلا أنها قد تختلف كم اً ونوعاً من مجتمع لآخر، ومن زمن إلى آخر.

و تُعرف الجريمة بأنها" سلوك أو إمتناع محظور قانوناً يرتب جزاءات على مخالفته"، كما تُعرف أيضاً بأنها" ذلك الضرب من السلوك الذي يجرمه القانون الوضعي وتجريم أي فعل من طرف المشرع إنما يتم وفق معيار حماية الحقوق، باعتبارها تحتاج كلها إلى حماية، مع التفاوت في هذه الحماية بحسب التفاوت في درجة الحاجة.

وكان للتطورات التكنولوجية والصناعية الحديثة انعكاسها بصورة جلية وواضحة في مجال الجريمة، مما جعلها تتسم بخطورة إجرامية خاصة بالنظر إلى الأسلوب الذي تعتمد عليه.

فهو أسلوب متصف بالتنظيم وتسخير التقنيات الحديثة من حواسيب متطورة، وشبكة أنترنت، ووسائل اتصال مباشر وسريعة عبر الأقمار الاصطناعية، وهي أساليب تصعب السيطرة عليها أو الكشف عنها بسهولة.

لذلك لم تعد تستطيع الدولة بمفردها أن تقوم بمعزل عن باقي الدول بالتصدي لهذه الأنماط الجديدة والخطيرة من الجرائم، خاصة وأن التنظيمات الإجرامية لم يعد يقتصر نشاطها على حدود دولة معينة، بل أصبح يمتد بشكل أو بآخر إلى دولة أو دول أخرى سواء في مرحلة التخطيط أو التحضير أو التنفيذ، الأمر الذي دعا المجتمع الدولي إلى

وضع ضوابط وأسس من أجل ضبط الخارجين عن القانون والفارين بجريمتهم إلى دولة أخرى ، حتى لا يفلتوا من العقاب .

و باتت الجريمة الإلكترونية أحد الأنماط الخطيرة التي أضحت تؤرق العالم بأكمله، والذي عانى في الآونة الأخيرة من ويلاته وآثاره التدميرية الهائلة على بنيان الدول والمجتمعات، فألقت تلك الجرائم بظلالها على شتى مناحي الحياة السياسية والاجتماعية والاقتصادية، مما استدعى التحرك العاجل والسريع، من خلال منهجية علمية سليمة تستوعب متطلبات تحقيق الأمن على المستويات الداخلية والدولية.

وإدراكا للخطر الكبير الذي تسببه الجرائم الإلكترونية، والذي بات يهدد السلم والأمن في كثيرمن الدول، نظرا لما تخلفه من آثار تدميرية قد تطال بنيان الدولة و مؤسساتها وتوقف عجلة التنمية فيها، ونتيجة لقصور السياسات الجنائية الوضعية في التعامل مع الزيادة المطردة لحركة الجرائم الإلكترونية، وخصوصاً التي تتجاوز آثارها الحدود الإقليمية للدولة الواحدة، فقد بات واضحاً حتمية التعاون الدولي للتصدي لها من خلال وضع ضوابط وتحديد وسائل علمية وعملية لتكريس هذا التعاون .

وبالفعل فقد أصبحت الجريمة الإلكترونية اليوم تستأثر باهتمامات دولية و إقليمية و وطنية على كافة الأصعدة، وفي مختلف المجالات، فتصاعدت وتيرة التعاون الدولي في هذا المجال، وتبلور ذلك من خلال الجهود التي تبذلها دول العالم ومنظماته الإقليمية والدولية، الأمر الذي أفرز العديد من الاتفاقيات الدولية والإقليمية والثنائية المتعلقة بمكافحة الإرهاب، فضلاً عن قيام الدول بتطوير السياسات التشريعية الوطنية التي تدعم هذا التعاون، بما يكفل الحد من هذه الجريمة والقضاء عليها.

وانطلاقاً من ذلك؛ اتجهت الدول إلى إرساء العديد من الآليات والوسائل التي تهدف على تفعيل التعاون الدولي في مكافحة الجرائم الإلكترونية، وهذا ما ظهر جلياً سواء في مرحلة التجريم أو في مرحلة الملاحقة القضائية.

-فعلى صعيد التجريم:

تجلى التعاون الدولي من خلال إبرام العديد من الاتفاقيات الدولية والإقليمية والثنائية التي تجرم العديد من صور الأنشطة الإلكترونية، أبرزها اتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية: 2001/11/23 .

-أما على **صعيد الملاحقة القضائية:**

اقتضت مكافحة الجرائم الإلكترونية ضرورة تعاون الدول في مجال المساعدة القضائية المتبادلة بكافة صورها ووسائلها التقليدية منها والمستحدثة؛ كتسليم المجرمين، والإنابات القضائية الدولية، وتنفيذ الأحكام الجنائية الأجنبية، وتحديد الاختصاص الجنائي للنظر في هذه الجريمة، والتحقيق الجنائي عن بعد عبر وسيلة الـ Videoconference .

تتمثل **مشكلة الدراسة** فيما يلي:

- تزايد صور الأنشطة التي تمثل جرائم إلكترونية في الكثير من مناطق العالم، والتي لا يقتصر تأثيرها على الأشخاص المستهدفين فحسب، بل تؤثر أيضا على مصالح الدول والعلاقات الدولية وخطط التنمية الاقتصادية والاجتماعية داخل الدولة.
- ضعف فاعلية الآليات والوسائل المحلية والدولية المتعلقة بالتعاون الدولي في المسائل الجنائية فيما يتعلق بمكافحة الجرائم الإلكترونية.
- قصورالوسائل والأساليب والسياسات والتدابير الفاعلة في مواجهة الجرائم الإلكترونية، على المستويين الدولي والوطني.
- عدم وجود إستراتيجية أمنية فاعلة على المستويين الوطني والدولي لمواجهة الجرائم الإلكترونية .

وبناءا على ما تقدم تتضح **أهمية** اختيارنا لموضوع " المساعدة القضائية في الجرائم الإلكترونية "بإعتبار أن أنشطة الجريمة الإلكترونية تمثل في الغالب صور مستحدثة

لجرائم تقليدية والمتجددة بإستمرار نتيجة للتطور الهائل والمتزايد للتكنولوجيا ناهيك على أن الجريمة الإلكترونية تتسم بأنها من الجرائم التي يكتنفها الخفاء والسرية ذلك أن أنشطتها تمارس في عالم إفتراضي الامر الذي يجعل إكتشافها وملاحقتها في غاية الصعوبة وعن كونها عابر للحدود الأمر الذي جعلها مشكلة عالمية تتطلب تضافر الجهود الوطنية والدولية لمواجهتها، من خلال التنسيق بين التشريعات الجنائية المختلفة، وتنفيذ نصوص الإتفاقيات الدولية التي أبرمت لهذا الغرض.

ومن هذا المنطلق يُعَد موضوع المساعدة القضائية في الجرائم الإلكترونية من الموضوعات الشائكة التي تحتاج دائماً وبصورة مستمرة إلى الكثير من الدراسات والأبحاث التي يمكن أن تسهم في إيضاح بعض الغموض الذي يكتنفها.

ومن أجل ذلك كله آثرنا إختيار هذا الموضوع في جهدٍ متواضعٍ محاولة منا أن ننهل منهلاً طيباً من بحر العلم، آملين أن يساهم بحثنا هذا في إيضاح ما غمض من المسائل التي تنبثق من الموضوع محل البحث.

لذلك فهذه الدراسة **تهدف** إلى تحقيق عدة أهداف، لعل أهمها ما يلي:

- التعرف على أبعاد الجريمة الإلكترونية، من خلال إستجلاء مفاهيمها، وتحديد طبيعتها القانونية معرجين على إتساع نطاقها.
- البحث في المبادئ العامة والقواعد النظرية والعملية للمساعدة القضائية في المسائل الجنائية بشأن مكافحة الجرائم الإلكترونية .
- البحث في إجراءات ومجالات المساعدة القضائية في الجرائم الإلكترونية، والتي سعى ويسعى المجتمع الدولي إلى وضع إطارها وصوغ أحكامها بما يخدم ويعزز هذا التعاون.

و**الإشكال** الذي يطرح هنا هو فيما تتمثل المساعدة القضائية لمكافحة الجريمة الإلكترونية؟ وهو ما يعبر عن **الإشكال الرئيسي** للدراسة.

والذي منه تطرح جملة من **التساؤلات الفرعية** كل منها بعد دراسته يكشف لنا زاوية من زوايا المساعدة القضائية المتبادلة في المسائل الجنائية لمكافحة الجريمة الإلكترونية وهي:

فيما يتمثل مفهوم الجريمة الإلكترونية في التشريع الجزائري؟ وما هي مبادئ المساعدة القضائية لمكافحة الجريمة الإلكترونية؟ وفيما تتمثل إجراءات ومجالات المساعدة القضائية المتبادلة؟ وفيما يتمثل الإطار الموضوعي للمساعدة القضائية لمكافحة الجرائم الإلكترونية؟ وما هي الوسائل الحديثة للمساعدة القضائية في المسائل الجنائية لمكافحة الجريمة الإلكترونية؟ .

وللإجابة على الإشكال السابق إتبعنا **المنهج** العلمي الوصفي التحليلي من خلال تبني إطار نظري مبني على أسلوب الاستعراض والمناقشة التحليلية، واستخلاص الأفكار المتعلقة بموضوع الدراسة من خلال المؤلفات العامة والرسائل العلمية والمؤتمرات والندوات والأبحاث والدوريات المتخصصة والاتفاقيات والقرارات الدولية وشبكة الإنترنت وتجميع النصوص القانونية في بعض التشريعات الجنائية المقارنة للوقوف على موقف هذه التشريعات من الجزئيات المختلفة التي يشملها البحث موضوع الدراسة.

ولما كان موضوع الجريمة الإلكترونية من المواضيع المتشعبة في دراستها، لما لها من تأثير على الكثير من نواحي الحياة دولياً ومحليا، ونظرا لأن الجريمة الإلكترونية قد تم دراستها والخوض في كافة جوانبها من خلال المئات من الأبحاث في مختلف دول العالم فسوف تتركز دراستنا على موضوع المساعدة القضائية في المسائل الجنائية لمكافحة الجريمة الإلكترونية.

ولقد تم **تقسيم** دراستنا هذه إلى فصلين، وذلك على النحو التالي:

الفصل الأول خصص لدراسة "**أحكام المساعدة القضائية المتبادلة لمكافحة الجريمة الإلكترونية**" من خلال عرض مفهوم الجريمة الإلكترونية والمبادئ العامة للمساعدة

القضائية ناهيك على أننا درسنا فيه إجراءات ومجالات المساعدة القضائية المتبادلة في الجريمة الإلكترونية .

فيما خصصنا **الفصل الثاني" للإطار الموضوعي للمساعدة القضائية والوسائل المستحدثة لمكافحة الجريمة الإلكترونية** ".

وكان الأساس الذي إعتمدناه في تقسيم عملنا هذا هو أننا تناولنا المساعدة القضائية المتبادلة بشكل عام في **الفصل الأول** حيث تناولنا كافة أحكام المساعدة القضائية المتبادلة لمكافحة الجريمة الإلكترونية في حين أننا تناولنا الإطار الموضوعي للإنابة القضائية لمكافحة الجرائم الإلكترونية في **الفصل الثاني** قد تناولناه بشكل خاص إذ أسقطناه على جريمة الإرهاب الإلكتروني كمثال وهو ما سرنا عليه بنفس النسق حين تحدثنا عن الوسائل المستحدثة للمساعدة القضائية لمكافحة الجريمة الإلكترونية حتى يكون أكثر بيانا، وأما عن كوننا إقتصرنا في دراستنا هذه على بيان الإنابة القضائية دون غيرها من صور المساعدة القضائية كوننا نراها الصورة الأهم أو المحور الجوهري المكون للمساعدة القضائية المتبادلة.

الفصل الأول:

أحكام المساعدة القضائية

المتبادلة لمكافحة الجرائم الإلكترونية

المبحث الأول: مفهوم الجريمة الإلكترونية والأحكام والمبادىء العامة التي تحكم المساعدة القضائية المتبادلة لمكافحتها.

المبحث الثاني: الأحكام الإجرائية للمساعدة القضائية المتبادلة لمكافحة الجرائم الإلكترونية ..

لم يكن هناك قلق مع بدايات شبكة الإنترنت من جرائم يمكن أن ترتكب عليها أو بواسطتها لا لأنها آمنة في تصميمها وبناءها، بل نظرا لمحدودية مستخدميها ، علاوة على كونها كانت مقصورة على فئة معينة من المستخدمين – الباحثين ومنتسبي الجامعات– إلا أنه ومع توسع استخدامها ودخول جميع فئات المجتمع إلى قائمة مستخدميها بدأت تظهر على الوجود ما يسمى بالجرائم المعلوماتية على الشبكة أو بواسطتها ،جرائم 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 طبيعي خاصة إذا ما علمنا أن شبكة الإنترنت ذاتها لا تعرف الحدود أي أنها ذات طبيعة عالمية.

جرائم الحاسب الالي اكتسبت طابع الجرائم الدولية, على اعتبار أن البعض منها يشكل جرائم عابرة للحدود، الا أنه لا يعني اعتبارها من قبيل الجرائم التي تنظم في القانون الدولي الجنائي، وتم التنصيص, على بعض قواعدها ضمن إختصاصات المحكمة الجنائية الدولية التي ابرم نظامها الاساسي في روما عام 1998.

وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم, التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات. وتعزيز التعاون بينها وإتخاذ تدابير فعّالة للحد منها والقضاء عليها ولمعاقبة مرتكبيها.

وبناءا على ما سبق سوف نتناول من خلال هذا الفصل مفهوم الجريمة الإلكترونية والأحكام والمبادىء العامة التي تحكم المساعدة القضائية المتبادلة لمكافحتها في المبحث

الأول وفي المبحث الثاني سوف نتناول الأحكام الإجرائية للمساعدة القضائية المتبادلة لمكافحة الجرائم الإلكترونية.

المبحث الأول: مفهوم الجريمة الإلكترونية والأحكام والمبادىء العامة التي تحكم المساعدة القضائية المتبادلة لمكافحتها:

إن ظاهرة جرائم الكمبيوتر والأنترنت، أوجرائم التقنية العالية، أو الجريمة الإلكترونية ، ظاهرة إجرامية مستجدة نسبيا بحيث تعاني المجتمعات في الآونة الأخيرة من إنتهاك للحقوق والخصوصيات الإلكترونية، وذلك في ظل إنتشار الجريمة الإلكترونية، وجاء تطوّر هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا التي يسرت سبل التواصل وإنتقال المعلومات بين مختلف الشعوب والحضارات وسهلت حركة المعاملات، إلا أن هذا التقدم المذهل والمميز لايخلو من عيوب لأن استخدامه لايقتصر على الإنسان الخير بل الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه وإقتناصه الفرص لتحقيق أغراضه غير المشروعة ، فلم يتوان عن إستغلال التقنية لتطوير قدراته الإجرامية باستخدام شبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية، مما يلحق ضررا بالآخرين.

ولما كانت هذه الجريمة تتسم بكونها عابرة للحدود الأمر الذي دفع بالدول إلى العمل ملياً للحد من هذه الجرائم من خلال وضع آليات للتعاون الدولي أبرز هذه الآليات المساعدة القضائية المتبادلة في المسائل الجنائية ومن خلال هذا المبحث سوف نحاول التعرض الى مفهوم الجريمة الإلكترونية في **المطلب الأول** ومن ثم سوف نتناول أحكام ومبادىء المساعدة القضائية المتبادلة في **المطلب الثاني**.

المطلب الأول: مفهوم الجريمة الإلكترونية في التشريع الجزائري.

برز إلى الوجود نوع جديد من الجرائم وهو ما يصطلح على تسميته بالجرائم الإلكترونية ومجالها جهاز الكمبيوتر المستخدم لإختراق شبكة الأنترنت لذلك يمكن القول أن كل تطور ايجابي لا يخلو من سلبيات والآثار السلبية للانترنت كبيرة وخطيرة ذلك هو الأمر الذي ألقى رجال القانون مسؤولية تاريخية وإنسانية تجاه هذا الخطر الدائم إذ لا

يخفى على أحد بأن الجرائم الإلكترونية لم تعد مقتصرة على القرصنة لسرقة المعلومات والسطو على أرقام بطاقات الإئتمان لإستخدامها والإستغلال الجنسي للأطفال والإخلال بالآداب العامة ناهيك عن جرائم التجسس والإرهاب شملت مختلف المجالات[1].

الفرع الأول: تعريف المشرع الجزائري للجريمة الإلكترونية:

سنتطرق في هذا الفرع إلى تعريف الجريمة الالكترونية في التشريع الجزائري تعريفا فقهيا وأكاديميا وقانونيا.

أولا: التعريف الفقهي:

إن الجريمة الالكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثيلا في الجرائم التقليدية، فلهذا ظهر إختلاف في تعريف قائما من هذه التعاريف مايلي " : بأنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال. "

وهناك من يعرفها على أنها " كل عمل أو إمتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به، بإعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها.

أو أنها "إستخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع.[2]

ومن خلال هذه التعاريف تبنى الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها

[1] – زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، د ط ، 2011 ، ص42

[2] – زبيخة زيدان ، المرجع السابق ، ص43.

جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية، جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية.[1]

ثانيا : التعريف الأكاديمي.

كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية، ترتبت عنه خسارة تلتحق بالضحية أو مكسب يحققه الجاني، كما يمكن الإعتماد في التعريف الواسع للجريمة المعلوماتية على:

1-على ما تكون المعلوماتية موضوعا للاعتداء عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية.

2-عندما تكون المعلوماتية أداة ووسيلة للاعتداء عندما يستخدم الجاني أوجهاز معلوماتي لتنفيذ جريمته[2]

ثالثا : التعريف القانوني:

تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث [3].

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات، حيث أنه عرف من خلال نص المادة 2 من الفقرة من القانون رقم 09-04

---

[1] – زبيخة زيدان، المرجع السابق، ص44

[2] – المقدم عز الدين عز الدين، الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية 2015/11/01 في بسكرة .5

[3] – المقدم عز الدين عز الدين , المرجع السابق، ص 5.

المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[1]

مسميا إياه": المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين."[2]

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتي من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04 – 15 المؤرخ في العاشر من نوفمبر 2004 المتمم للأمر رقم (66-156) المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر 07.[3]

وفقا المشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى إشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها ، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات[4].

[1] – المادة 2 الفقرة بـ القانون رقم 09-04 المؤرخ في 14شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة.

[2] – نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية ، جامعة بسكرة 2015-2016، ص 4 .

[3] – عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دارالجامعة الجديدة ، كلية الحقوق جامعة الإسكندرية ، 2006 ، ص27 .

[4] – نشناش منية ، المرجع السابق، ص 4

أما فيما ينص الشرط الثاني لمجلس الشيوخ الفرنسي والمتعلق بضرورة توافر النظام على حماية فنية فيبدو أن النظام المشرع قد حسم موقفه إلى جانب الفقه الذي لا يشترط هذا الشرط لحماية نظام المعالجة الآلية للمعطيات الجنائية[1] .

موقف المشرع الجزائري من الجريمة الإلكترونية:

من خلال ما تقدم من تعريفات الجريمة الالكترونية في التشريع الجزائري نستنتج موقف المشرع من هذه الجريمة ، وهذا الموقف متمثل في أن التقدم التكنولوجي وإنتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة من الإجرام، مما دفع الكثير من الدول إلى النص على معاقبة هذا النوع من الجرائم، تسعى من خلال هذا المشروع إلى توفير الحماية الجزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وبالتالي قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 المتمم والمعدل لأمر 66/156 المتضمن لقانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، فقد أثار المشرع الجزائري إستخدامه لمصطلح الدلالة على كلمة المعلومات والنظام الذي يحتوي عليها ويخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة إرتكابها وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها.[2]

[1] – نشناش منية، المرجع السابق، ص 4

[2] – سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية، جامعة الحاج لخضر باتنة 2012 ـ 2013، ص41.

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة.

تم في مرحلة لاحقة إختيار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن من جرائم مكافحتها.[1]

ونجد المشرع الجزائري تطرق إلى تعريف الجريمة المساس بأنظمة المعالجة الآلية للمعطيات في المادة 2 من قانون رقم 04/09 وجرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات.[2]

الفرع الثاني: الطبيعة القانونية الخاصة للجريمة الإلكترونية.

لبيان الطبيعة القانونية للجريمة الالكترونية لابد من تقسيم هذا المطلب إلى فرعين نتطرق في الفرع الأول إلى طبيعة القانونية وفي الفرع الثاني إلى خصائص الجريمة الإلكترونية

أولا: الطبيعة القانونية الخاصة للجريمة الإلكترونية.

إن دراسة الجريمة الالكترونية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوبات وهو قسم الخاص وهو ذلك الفرع الذي يدرس كل جريمة على حدى متناولا كل الفصل الأول الإطار المفاهمي للجريمة الإلكترونية عناصرها الأساسية والعقوبة المقررة لها فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة.[3]

---

[1] – سعيد نعيم، المرجع السابق ، ص41.

[2] – نفس المرجع، ص41.

[3] – محمد زكي أبو عامر وعلي عبد القادر القهوجي : قانون العقوبات القسم الخاص، دار النهضة العربية القاهرة ، 1993، ص9

"إن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة، كما قد ترتكب هذه الجرائم في مجال الكلمات أو معالجة النصوص وهذا النوع الأخير من الجرائم لا يعد أن يكون طريقة أوتوماتيكية المستخدم من تحرير الوثائق والنصوص على الحاسب مع توفير إمكانيات التصحيح والمسح والتخزين والاسترجاع والطباعة."[1]

فهذه العمليات كلها هي وثيقة الصلة بالجرائم محل البحث وعليه لابد للجاني من فهمها فضلا عن أن الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الإعتداء أو تستخدم وسيلة له.[2]

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصيا وعام في آن واحد مما يؤدي إلى الاعتداء على الخصوصية والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة.

وبالتالي هذه الطبيعة الخاصة للأفعال المجرمة هل تدخل ضمن أحكام خدمات البريد أم التخابر الخاص أم يكون الهدف الأساسي للتحري عن نظام القانوني المناسب لطبيعة الجرائم المعلوماتية هو معرفة النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات فيها؟ ومن هذا النظام القانوني تتحدد المسؤولية التي يفترض تطبيقها على الأشخاص المسؤولين عن هذا النشر ومن خلال المجال التي

[1] – أ حمد السمدان، النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوقي، الكويت، 1987، ص 164.

[2] – جميل عبد الباقي، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001، ص 42.

ترتكب فيه الجريمة المعلوماتية ومحل الاعتداء عليها تظهر لنا الطبيعة القانونية الخاصة للجريمة.[1]

إن التطور المعلوماتي يفتح المجال لاقتناء وسائل الكترونية تمكن المتجاوزين لاستخدامها في ارتكاب جرائم مختلفة لأن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيها يتعلق بالمعالجة الآلية لبيانات وإدخال المعلومات ونقلها ومن ثم يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عن مواكبة التطور المعلوماتي أوبما يحويه من فراغ تشريعي في هذا المجال.[2]

أما من حيث التكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة إذا لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، إن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات وصعوبة إيجاد دليل مادي يدين مرتكب الجريمة لأنه من السهل على الجاني محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال قد تكون البيانات التي تجري البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة.[3]

ومن صعوبة ملاحقة مرتكبي الجرائم المعلوماتية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[4]

---

[1]– طوبي ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، دار صادر للمنشورات بيروت، ط 1, د س ن, ص 383.

[2] – مجلة جامعة بابل ، العلوم الإنسانية ، المجلد 14 ، العدد 6.ص 89.

[3] – نفس المرجع ، ص91 .

[4] – هلال عبد الله أحمد ، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، ط 1 , 2007، ص22 .

ثانيا:خصائص الجريمة الإلكترونية.

إن للجريمة الالكترونية خصائص كثيرة سنحاول حصرها و إبرازها في مايلي:

1/ الجرائم الإلكترونية من الجرائم عابرة للحدود:

وسعت شبكات المعلومات عملية الاتصال وتبادل معلومات بين الدول والأنظمة التي يفصل بينها آلاف الأميال، ومع القدرة التي يتمتع بها الحاسب أدى ذلك إلى إمكانية إرتكاب الجريمة الإلكترونية في أماكن متعددة من العالم وفي وقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقيم فيها الجاني[1].

إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود، فمسرح الجريمة لم يعد محليا بل أصبح عالميا إذ أن الفاعل لا يتواجد ماديا على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب من خلال الحاسوب والفاعل وبين المعلومات التي كانت محل الاعتداء، فالجاني يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد آخر وهذا الفعل قد يضر شخصا ثالثا في بلد آخر.[2]

ومن خلال هذه الخاصية الدولية يثار إشكال حول الإختصاص القضائي في محاكمة المجني عليه بمعنى بمعنى آخر ما هي الدولة المختصة بمحاكمة الجاني؟ هل هي الدولة التي ارتكب على إقليمها النشاط الإجرامي أم التي يوجد فيها المجني عليه؟.[3]

وبمعنى آخر أن هذه الجريمة لا تقع في دولة واحدة ولا تعترف هذه الجريمة بالحدود الجغرافية للدول إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر وقد يكون الضرر المحتمل في بلد ثالث[4].

---

[1] – خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، عنوان84 شارع زكرياء غنيم الإبراهيمية الإسكندرية، 2008، ص 82 .

[2] – سعيد نعيم ،المرجع السابق، ص 32.

[3] – نفس المرجع، ص 32.

[4] – مجلة جامعة بابل، المرجع السابق، ص 92.

2/ صعوبة إكتشاف وإثبات الجرائم الإلكترونية:

تمتاز الجرائم المعلوماتية بصعوبة الإكتشاف والإثبات وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام، هي رموز دقيقة ويصعب إكتشافها وإثباتها لهذا عادة ما يتم إكتشافها بالصدفة وغالبا ما يتم معاقبة مجرمين وذلك لعدم وجود أدلة قائمة في حقه.[1]

فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية . [2]

وصعوبة اكتشاف وإثبات الجرائم المعلوماتية راجع لعدة أسباب منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات.[3]

ويصعب في جرائم المعلوماتية العثور على دليل مادي للجريمة وذلك راجع إلى إستخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان، وهذا السلوك المادي في إرتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به[4]

---

[1] – معتوق عبد اللطيف ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ،مذكرة مكملة لنيل شهادة الماجستير وعلوم الجنائية ، 2011. ، 2012 ص24 .

[2] – سعيد نعيم، المرجع السابق، ص. 34

[3] – نفس المرجع ، ص 34.

[4] – هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة ، أسيوط ، ط1 ، 1994 ،ص 82.

3/ تتطلب وسائل خاصة في الحاسب الآلي وشبكة الأنترنت.

إن الجريمة المعلوماتية تستلزم لقيامها توفر الحاسب الآلي وكذلك شبكة الانترنت وسيلة إرتكاب الجريمة وأدواتها الرئيسية أماكن المعرفة التقنية فتكون ضرورية بحسب درجة خطورة الجريمة المعلوماتية. [1]

4/ تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها:

إن جريمة المعلوماتية لها طبيعة تقنية وبذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري ، لذلك لابد أن يكون المحقق متخصص في جريمة المعلوماتية حتى لا يتسبب في إتلاف الدليل الالكتروني.2

5 / تعد الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية:

إن هذه الجريمة تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي، وفي الواقع ليس هناك شعور بعدم أمان تجاه المجرمين في مجال المعرفة المعلوماتية لأن مرتكبيها ليسوا محترفي الإجرام.[3]

6/ دافع إرتكاب الجريمة المعلوماتية:

إن باعث الدافع الجريمة المعلوماتية قد يختلف عن دافع الجريمة التقليدية فقد يكون الدافع مخالفة النظام العام والخروج على القوانين وقد يكون ماديا يراد به إكتساب مبالغ طائلة أو الإهانة وتشهير والتأثر...إلخ يكن دون الإحتكاك المباشر بالمجني عليه [4].

[1] – معتوق عبد اللطيف، المرجع السابق، ص 15

[2] – نفس المرجع ، ص 15

[3] – معتوق عبد اللطيف ، المرجع السابق، ص 15

[4] – جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992 ، ص 62.

الفرع الثالث : إتساع نطاق الجريمة الإلكترونية:

تطور تكنولوجيا الإعلام أدى إلى إتساع نطاق الجريمة الإلكترونية فهي أصبحت لاتقتصر على جريمة واحدة وإنما إتسعت إلى عدة جرائم ترتكب عن طريق الهاتف وعن طريق الكمبيوتر.

ولا ترتكب هذه الجريمة من طرف شخص طبيعي فقط بل تعدت إلى الشخص المعنوي كذلك ، سنبين في هذا المطلب الجرائم التي تندرج ضمن الجريمة الإلكترونية بإختصار.

أولا : الجرائم المرتكبة من طرف الشخص الطبيعي:

1/ جريمة الدخول غير المشروع في المنظومة المعلوماتية في قانون العقوبات الجزائري:

نصت على هذه الجريمة الإلكترونية المادة 394 مكرر من قانون العقوبات ويلاحظ أن المشرع الجزائري جرم فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية وإعتبر[1] هذا التصرف في حد ذاته يشكل جريمة إذ يستخلص لأول وهلة أن مجرد إختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية يعد إنتهاكا للنظام المعلوماتي بطريقة غير مشروعة[2] .

2/ جريمة البقاء في المنظومة المعلوماتية وفقا لقانون العقوبات الجزائري:

لاحظنا أن نص المادة 394 مكرر يجرم الدخول وكذلك البقاء فيها ومما يتعين الوقوف عنده هنا هو أن المشرع فرق بين فعل الدخول غير المشروع وبين البقاء دون وجه قانوني أو مصلحة قانونية[3] .

---

[1] – مولود ديدان، قانون العقوبات ، قانون رقم09 – 01 المؤرخ في 25 فبراير 2009 ، د ط ، ص 120.

[2] – مولود ديدان، المرجع السابق ، ص 120

[3] – نفس المرجع، ص 120

3/ إدخال معطيات في نظام المعالجة الآلية أو إزالتها بطرق تدليسية:

نصت على هذه الجريمة المادة 394 مكرر 1 من قانون العقوبات الجزائري بنصها " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها [1] ."

4/ جرائم نشر المعطيات المخزنة أو معالجة أو المرسلة بواسطة منظومة معلوماتية وحيازتها والإتجار فيها تخزين معالجة وإرسال المعطيات:

طبقا لنص المادة 394 مكرر 2 من قانون العقوبات الجزائري حددت هذه المادة الأفعال المجرمة.

5/ جريمة تجميع أو توفير بيانات المخزنة أو معالجتها أليا:

نصت على هذه الجريمة المادة 394 مكرر 2 ونلاحظ أن المشرع وسع نطاق الحماية لما أسماه المعالجة الآلية للمعطيات إذ بسط هذه الحماية لتشمل المتصل بالمعلومات أو البيانات فضلا عن تجريمه للدخول غير المشروع في المنظومة أو في جزء منها أو البقاء فيها فإنه وتحسبا لما يترتب عن هذا الدخول أو البقاء من سلوكات إجرامية [2] .

6/ جريمة نشر المعطيات وإفشاءها.

نصت على هذه الجريمة المادة 394 مكرر 2 الفقرة 1 من قانون العقوبات.

7/ جريمة إعاقة سير المعلومات المرسلة عن طريق منظومة معلوماتية.

من ضمن الجرائم المنصوص عليها والمتضمنة بأحكام المادة 394 مكرر 2 من قانون العقوبات الجزائري التي يمكن إستخلاصها من إستقراء هذه المادة هي إعاقة أو إعتراض

[1] – مولود ديدان , المرجع السابق ، ص 120

[2] – زبيحة زيدان: المرجع السابق، ص56 .

طريق نظام المعلوماتي أو المعطيات المرسلة عن طريق نظام المعلوماتية بغرض قرصنتها والإتجار فيها [1].

8/جريمة حيازة البيانات أو المعطيات :

معنى حيازة البيانات بغرض إستعمالها ويبدوا أن الإستعمال يعد مجرما حتى وإن تم بغرض سليم ومشروع طالما أن المعطيات نفسها متحصلة من الجرائم المنصوص عليها في المادة 394 قانون العقوبات الجزائري أي عن طريق الدخول الغير المشروع في كل أو جزء من منظومة متعلقة بالمعالجة الآلية للمعلومات أو المعطيات وذلك عن طريق الغش وتتحقق جريمة حيازة المعطيات بتوافر أركانها.

ثانيا : جرائم الشخص المعنوي القانوني.

1/ جرائم المعلوماتية المرتكبة من طرف الشخص المعنوي المادة 394 مكرر4 :

من المؤكد التنويه بأن المشرع الجزائري إنتهج موفقا جديدا بخصوص تحميل الشخص المعنوي المسؤولية الجزائية منذ تعديله لقانون العقوبات بموجب القانون رقم06- 23 المؤرخ في 2006/12/20، وحدد بموجب المادة 18 مكرر منه التي تطبق على الشخص المعنوي في مواد الجنايات والجنح وهي:

- "الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة . "

واحدة أو أكثر من العقوبات التكميلية الآلية:

- حل الشخص المعنوي2 .
- غلق المؤسسة أو فرع من فروعها لمدة لاتتجاوز خمس 5 سنوات.

[1] – المادة 394 مكرر 2 الأمر 66 . 156 المؤرخ في 8 يونيو 1966 المتضمن لقانون العقوبات والمتمم لأمر رقم15 . 19 المؤرخ في 30 ديسمبر 2015.

[2]– مولود ديدان ، قانون العقوبات ، المرجع السابق ، ص120

- الإقصاء من الصفقات العمومية لاتتجاوز خمس 5 سنوات.
- المنع من مزاولة نشاط أو لمدة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لاتتجاوز خمس 5 سنوات.
- مصادرة الشيء الذي إستعمل في إرتكاب الجريمة أو نتج عنها .
- نشر وتعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لاتتجاوز عدة خمس السنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي إرتكبت الجريمة بمناسبته."
- والعقوبات التكميلية حددتها المادة وفقا للمادة 394 مكرر 6.[1]

2/ جرائم تكوين جمعية الأشرار المعلوماتيين لغرض التحضير للجرائم الماسة بالأنظمة المعالجة الآلية:

نصت على هذا النوع من الجرائم المادة 394 مكرر 5 من قانون العقوبات الجزائري على أنه " كل من شارك في مجموعة أو في إتفاق بغرض الأعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها[2]."

ويتضح من خلال هذه المادة بأن يطال من يشارك أي مجموعة أو في إتفاق الغرض منه التحضير أو الإعداد لإرتكاب الجرائم المعلوماتية المنصوص عليها في القسم السابع مكرر من قانون العقوبات ولكن يركز المشرع على توافر القصد الجنائي والمجسد في توافر شرط العلم لدى المشترك.

[1] – مولود ديدان ، قانون العقوبات ، المرجع السابق ، ص . 121

[2] – نفس المرجع، ص 121.

كما يلاحظ حرص المشرع على توافر شروط معينة بعد حصول الإتفاق أو الأجماع أي تشكيل فريق أو مجموعة بأن يجسد التحضير للجريمة فعل مادي أو عدة أفعال تستهدف سرقة البيانات أو تعطيل شبكة الإنترنت وعرقلة سير المعلومات أو بث الفيروسات[1].

المطلب الثاني : أحكام و مبادىء المساعدة القضائية المتبادلة .

إن المبادئ العامة التي تنظم الإلزام بتقديم المساعدة المتبادلة مقررة في الفقرة 1 فالتعاون متوافر "لأقصى حد ممكن" ومن ثم كما تقرر المادة 23 (المبادئ العامة المتعلقة بالتعاون الدولي)، فإن المساعدة المتبادلة من حيث المبدأ يجب أن تكون واسعة المدى كما يجب أن يتم تقييد العوائق وتحديدها، ثانيا، كما هو مقرر في المادة 23 فإن الالتزام بالتعاون ينطبق من حيث المبدأ على كل من الجرائم ذات المتعلقة بنظم الحاسوب والبيانات (مثل: الجرائم المقررة في المادة 14، الفقرة 2 تقسيم a–b)، وتجميع الدليل في هيئته الإلكترونية الناجم عن الجرائم، ولقد تم الاتفاق على تقرير التزام بالتعاون على هذا النحو الواسع للجرائم لأن هناك حاجة مماثلة لآلية إنسيابية للتعاون الدولي لهاتين الهيئتين، وعليه فالمادة 24 والمادة 35 تسمح للأطراف بتقديم نطاق مختلف لتنفيذ هذه الإجراءات[2].

نصوص أخرى في هذا الفصل تتولى توضيح أن الالتزام بتوفير المساعدة المتبادلة هي بشكل عام تتوافر بالتبعية لمعاهدات المساعدة القانونية المتبادلة والقوانين المتبادلة والقوانين والترتيبات، ووفقا للفقرة 2 فإنه يتطلب من كل طرف في هذه الاتفاقية إتخاذ أساس لأشكال محددة من التعاون تم شرحها في باقي الفصل، إذا لم يكن في المعاهدات

[1] – زبيحة زيدان ، المرجع السابق ، ص 104

[2] – هلالي عبد الله أحمد، إتفاقية بودابست مكافحة جرائم امعلومات معلقا، ط1، دار النهضة العربية، القاهرة، 2007 ص 196

والقوانين والترتيبات ما يماثل هذه النصوص، فوجود مثل هذه الآليات، وبصفة خاصة ما هو مقرر في المواد 29 إلى 35 (نصوص محددة، العناوين 1 و2 و3)، يعد أمرا حيويا لتعاون مؤثر فيما يتعلق بالجرائم ذات العلاقة بالحاسوب[1].

لا يستعين بعض الأطراف في هذه الاتفاقية بتشريع نافذ بقصد تطبيق نصوص تستند إلى الفقرة 2 وذلك إستنادا إلى أن المعاهدات الدولية التي تتضمن تفصيلا لنظم المساعدة المتبادلة تعد نافذة بطبيعتها، ومن المتوقع أن الأطراف إما أن يكونوا مؤهلون لمعاملة هذه النصوص كنصوص نافذة، تتوافر لها المرونة الكافية وفقا لتشريع المساعدة المتبادلة النافذ لتقرير الإجراءات المتعلقة بها وفقا لهذا الفصل أو أن يقوموا بإصدار أي تشريع يتولى هذا الأمر[2].

بيانات الحاسوب سريعة التبخر، إذ بمقتضى بعض النقر على لوحة المفاتيح أو بتشغيل برامج آلية فإنه يمكن أن يتم إلغائها أو جعل تعقب الجريمة أو مرتكبها مستحيلا وبحيث يؤدي ذلك إلى تدمير إثبات الجرم، بعض أشكال بيانات الحاسوب يتم تخزينها فقط لمدة قصيرة من الزمن قبل إلغائها، وفي حالات فإن الأضرار المحدد بالفرد أو بالملكية يمكن أن يتوافر إذا لم يتم تجميع الدليل فورا، وفي بعض الحالات المستعجلة فإنه يتم فقط إعداد الطلب ولكن يجب أن يتوافر أيضا الاستجابة له بشكل معجل، فالغرض من الفقرة 3 هو تسهيل تعجيل إجراء الحصول على المساعدة المتبادلة حتى لا يتم فقدان المعلومات المطلوبة أو الدليل بسبب القيام بإلغائها قبل إعداد المساعدة أو إرساله أو الرد عليه، وتتولى الفقرة 3 ذلك بمقتضى[3] تشجيع الأطراف لتقديم طلبات عاجلة للتعاون بإستخدام وسائل إتصالات عاجلة غير تلك التقليدية المعدة أكثر بطأ في التراسل أو

[1] – هلالي عبد الله أحمد، نفس المرجع، 196.

[2] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحرين على ضوء إتفاقية بودابست، ط2، دار النهضة العربية، القاهرة، 2013، ص 257.

[3] – هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلومات معلقا عليها، المرجع السابق ص 197، 198.

الكتابة، والوثائق المختومة بأسلوب الحقائب الدبلوماسية أو نظم تسليم البريد وإلزام الطرف المطلوب منه باستخدام وسائل عاجلة للاستجابة للطلبات في مثل هذه الظروف، ويلتزم كل طرف في هذه الإتفاقية بإيجاد القابلية لتنفيذ هذا الإجراء إذا لم تكن هناك معاهدات مساعدة متبادلة أو قوانين أو ترتيبات نافذة فلائحة الفاكس أو البريد الإلكتروني ذات دلالة بطبيعتها، وأية وسائل أخرى للاتصال يمكن أن يتم استعمالها بشكل مناسب في بعض الظروف المتاحة، ولما كانت التكنولوجيا تتطور فإن وسائل الإتصال عاجلة يتم تطويرها ويمكن إستخدامها لطلب المساعدة المتبادلة في هذه الفقرة، حيث يمكن للأطراف التقرير فيما بينهم كيفية تأمين مصداقية الإتصالات وما إذا كان هناك حاجة لحماية أمنية خاصة (بما في ذلك التشفير) الذي يمكن أن يكون ضروريا في بعض الحالات الحساسة، وفي النهاية فإن الفقرة تسمح أيضا للطرف المطلوب منه بأن يطلب تأكيد شكلي يرسل بالقنوات التقليدية للاستمرار في التراسل العاجل إذا إختار هو ذلك[1].

تقرر الفقرة 4 للمبدأ الذي يجعل المساعدة المتبادلة محلا لعبارات تنفيذ معاهدات المساعدة المتبادلة والقوانين المحلية، فهذه تقرر ضمانات لحقوق الأفراد المقررة لدى الطرف المطلوب منه المساعدة المتبادلة بحيث يمكن أن يكون في يوم ما محلا لطلب المساعدة المتبادلة، وعلى سبيل المثال، فالإجراء الاقتحامي مثل التفتيش والضبط، لا يتم تنفيذه على أساس الطرف الطالب لذلك، إلا إذا كان ذلك من المتطلبات الأساسية للطرف المطلوب منه الإجراء في إطار واقعية محلية وعلى الأطراف كذلك تأمين حماية الحقوق الفردية ذات العلاقة بالبنود التي تم ضبطها باستخدام نظام المساعدة المتبادلة.

لا تنطبق الفقرة 4 إذا "ما لم يتم تحديد ذلك في القسم فهذا الشرط لم يتقرر للإشارة بأن الاتفاقية تتضمن العديد من الاستثناءات المحددة على مبدأ العام، فالبداية في مثل هذا الاستثناء قد تم التعرض له في الفقرة 2 من هذه المادة، التي تلزم كل طرف بالتزود

[1] – هلالي عبد الله أحمد، نفس المرجع، ص 199.

بأشكال التعاون المقررة في المواد النافذة المفعول في هذا القسم (مثل التحفظ وتجميع البيانات في الزمن الفعلي والتفتيش والضبط الصيانة المقررة في الفقرة 7/27 الخاصة بالشبكات)، وبصرف النظر عما إذا كان هناك معاهدات تسليم مجرمين من عدمه، فإن الترتيبات المتكافأة أو قوانين المساعدة المتبادلة تسمح بمثل هذه الإجراءات، كذلك وجد استثناء آخر في المادة 27 ينطبق دائما حين تنفيذ الطلبات في الإطار الإقليمي للطرف المطلوب منه وفقا للقانون المحلي الذي ينظم التعاون الدولي حال عدم وجود معاهدة تسليم مجرمين أو ترتيبات متكافأة بين الطرفين، حيث تتوافر في المادة 27 نظام لشروط وأسس للرفض، وكذلك يوجد استثناء آخر لا يمكن إنكاره، وعلى الأقل كما هو محدد في الجرائم المقررة في المواد 2-11 من الاتفاقية، على أسس أن الطرف المطلوب منه أن يأخذ في الاعتبار الطلب بالنسبة للجرائم المالية، وفي النهاية فإن المادة 29 تعد استثناء بحيث أنه تسمح بالا يجوز إنكار التحفظ على أسس جنائية مزدوجة، بالرغم من إحتمال أن التحفظ مسموح به في هذا الإطار[1].

الفقرة 5 هي عبارة عن تعريف أساسي للتجريم المزدوج لأغراض المساعدة المتبادلة وفقا لهذا القسم، عندما يسمح الطرف المطلوب منه الإجراء تطلب التجريم المزدوج كشرط لتقديم المساعدة (على سبيل المثال، حال قيام الطرف المطلوب به بحفظ حقه في تطلب التجريم المزدوج بالنظر إلى التحفظ على البيانات وفقا للفقرة 4/29 "التحفظ المعجل على البيانات المخزنة في الحاسوب")[2]، فالتجريم المزدوج يعد قائما إذا كان السلوك المرتبط بالجريمة المقصودة بالمساعدة هو أيضا جريمة في قوانين الدولة الطرف المطلوب منها الإجراء، حتى ولو كانت قوانينها تقرر الجريمة من خلال فئة جريمة مختلفة أو تستخدم مصطلحات مختلفة لتسمية الجريمة، فهذا النص يعد ضروريا بقصد التأكيد بأن الأطراف

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظام المصري والبحريني عى ضوء إتفاقية بودابست، مرجع سابق، ص 269، 270.

[2] – هلالي عبد الله أحمد، نفس المرجع، ص 272، 273.

المطلوب منها الإجراء لم تتخذ إختبار تسليم صارم جدا حال تطبيق التجريم المزدوج، وبالإشارة إلى الاختلافات المقررة في النظم القانونية الوطنية، فإن التغاير في المصطلحات والفئات المقررة للسلوك الإجرامي يمكن أن يبرز، فإذا كان السلوك يشكل إنتهاكا جنائيا وفقا لكل من النظامين، مثل الإختلافات التقنية فإنه يجب ألا تكون عائقا للمساعدة وبحيث عوضا عن ذلك فإنه في حالات معيار التجريم المزدوج فإنه يجب أن يتم تطبيقها بشكل مرن بحيث يسهل قبول المساعدة.

تم إشتقاق هذه المادة من نصوص وردت فيما سبق في مقررات مجلس أوروبا، مثل المادة 10 من الاتفاقية حول غسل الأموال والتفتيش والضبط والمصادرة لناتج الجريمة (ETS NO 141) والمادة 287 من إتفاقية القانون الجنائي حول الفساد (ETS NO 173) وأمثل من ذلك تكرارا، فإن الطرف الذي يحوز معلومات قيمة التي يمكن أن تساعد طرف آخر في تحقيق أو إجراء جنائي والتي لم يكن الطرف الآخر على الذي يجري التحقيق أو يتولى الإجراء على الإطلاع عليها، ففي مثل هذه الحالات، لن يكون هناك حاجة لطلب المساعدة المتبادلة، فالفقرة 1 تشجع الدولة الحائزة للمعلومات على تمريرها إلى الدولة الأخرى دون حاجة إلى طلب مسبق.

فالمعتقد أن هذا نص مفيد لأنه، وفقا لقوانين بعض الدول، حيث أنه هناك حاجة للقبول الإيجابي للسلطات القانونية بقصد تقديم المساعدة حال عدم وجود طلب، فالطرف في هذه الاتفاقية ليس مجبرا على تمرير المعلومات تلقائيا إلى طرف آخر، ولكن يمكن أن يمارس حرية التصرف في ضوء الظروف المحيطة بالواقعة المتوافرة، وأكثر من ذلك، فإن الكشف الذاتي عن المعلومات لا يحول دون قيام الطرف الكاشف، إذا كان لديه إختصاص من التحقيق وتهيئة الإجراءات المتعلقة بالحقائق المكتشفة[1].

[1] – هلالي عبد الله أحمد، جرائم المعلومات عابرة الحدود، ط1، دار النهضة العربية، القاهرة، 2007، ص210.

تنظم الفقرة 2 حقيقة أنه في بعض الظروف فإن الطرف في هذه الاتفاقية يقوم فقط بإرسال المعلومات الذاتية إذا كانت المعلومات الحساسة قد تم إبقائها في إطار من السرية أو أن يتم وضع شروط على استخدام المعلومات[1]، وبشكل خاص، فإن السرية تعد ذات أهمية خاصة في الحالات التي قد تتعرض فيها المصالح الهامة للدولة حال القيام بنشر المعلومات على العامة من الناس، كما هو الشأن في حالة أن يكون هناك حاجة لحماية النمط الذي يتم به تجميع المعلومات أو أن يكون التحقيق متناولا عصابة إجرامية، فإذا كشف تحقيق متقدم بأن الطرف المطلوب منه لا يمكن الاستجابة مع الشرط المنشوط من قبل الطرف الطالب (على سبيل المثال، حالما لا يستطيع الاستجابة مع شرط السرية لأن المعلومات المعدة دليل أمام قضاء علني) فإنه يمكن للطرف المطلوب منه تقديم النصح للطرف الطالب حيث يكون له هنا الاختيار بالا يقدم المعلومات، فإذا يكون ذلك تشريف له، ومن المتنبأ به أن الشروط المقررة وفقا لهذه المادة يجب أن تكون متوافقة مع تلك التي يتم تقريرها من قبل الطرف المطلوب منه بالتبعية لطلب المساعدة من قبل الطلب الطالب.

و في ما يلي سوف نعالج مادتين هما: المادة 25 المتعلقة بالأحكام العامة التي تحكم المساعدة القضائية المتبادلة في فرع أول والمادة 26 الخاصة بالمعلومات التلقائية أي تلك التي تأتي عفوا أو بطريقة عفوية في فرع ثاني .

الفرع الاول : الأحكام العامة التي تحكم المساعدة القضائية المتبادلة[2]:

من خلال هذا الفرع سوف نستعرض نص المادة 25 أولا في حين سوف نستعرض التعليقات عليها ثانيا.

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء إتفاقية بودابست، مرجع سابق، ص 273.

[2] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية رقم 158 بتاريخ 2001/11/23.

أولا : نص المادة 25: المساعدة القضائية المتبادلة

1- يجب على كل الأطراف أن تتوفر لبعضها البعض مساعدة قضائية متبادلة إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الالكترونية للجريمة الجنائية.

2- يجب على كل طرف أيضا أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية للوفاء بالإلتزامات المنصوص عليها في المواد 27 إلى 35.

3- يمكن لكل طرف، في حالة الاستعجال، أن يقدم طلبا للمساعدة المتبادلة أو الإتصالات عن طريق وسائل سريعة للإتصال كالفاكس أو البريد الإلكتروني، وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق (بما في ذلك التشفير لو كان ضروريا)، مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوبا بواسطة الدولة الموجه إليها الطلب، ويجب على الدولة المقدم إليها الطلب أن توافق وأن ترد على الطلب المقدم إليها عن طريق أية وسيلة من الوسائل العاجلة للاتصال.

4- باستثناء ما يرد مخالفا ذلك صراحة في مواد هذا الفصل، فإن المساعدة المتبادلة تخضع للشروط المحددة عن طريق القانون الداخلي للطرف الموجه إليه الطلب أو عن طريق الإتفاقات المطبقة للمساعدة المتبادلة، بما في ذلك الأسباب التي بناء عليها يمكن للطرف الموجه إليه الطلب أن يرفض التعاون. يجب على الطرف الموجه إليه الطلب ألا يمارس حقه في رفض المساعدة القضائية المتبادلة بالنسبة للجرائم "المنصوص عليها في المواد من 2 إلى 11 من الاتفاقية، فقط إذا كان الباعث على تقديم الطلب يتصل بجريمة ذات طبيعة مالية.

5- عندما يسمح، وفقا لبنود هذا الفصل، للطرف المقدم إليه الطلب أن يخضع المساعدة المتبادلة لوجود تجريم مزدوج (مشترك) فإن هذا الشرط يعتبر مستوفيا إذا كان السلوك المكون للجريمة في الطلب المقدم للطرف المطلوب منه المساعدة، يوصف بأنه

جريمة جنائية في قانونه الداخلي، سواء أكان القانون الداخلي قد صنفه في نفس طائفة الجرائم أم لا، وسواء تم تجريده بنفس المصطلح الذي نص عليه قانون الطرف الملتمس أم لا[1].

ثانيا: التعليقات

لقد تم تحديد المبادئ العامة التي تحكم الإلتزام بالمساعدة القضائية المتبادلة في الفقرة الأولى من المادة 25، والإلتزام بالمساعدة يجب أن يتوافر "لأقصى حد ممكن" وهكذا كما في المادة 23 (المبادئ المتعلقة بالتعاون الدولي) فإن المساعدة المتبادلة يجب أن تكون – من حيث المبدأ– شاملة أو ممتدة، كما يجب تقليل المعوقات إلى أقصى حد ممكن، كذلك فإن الالتزام بالتعاون المنصوص عليه في المادة 23 ينطبق كمبدأ عام على كل من الجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية (بمعنى على الجرائم المشار إليها في المادة 14 فقرة 2 (أ–ب) وعلى تجميع الأدلة الالكترونية المرتبطة بجريمة جنائية، لقد أصبح فرض الإلتزام بالتعاون بالنسبة لهذه الطبقة العريضة من الجرائم، لوجود مسوغ لتوافر آليات التعاون الدولي في هذين النطاقين، ومع ذلك فإن المادتين 34 و35 تسمحان للأطراف بتعديل نطاق تطبيق هذه الإجراءات[2].

البنود الأخرى من هذا الفصل توضح أن الالتزام بتوفير المساعدة المتبادلة أن يتم تنفيذه –عموما– وفقا للشروط الواردة في المعاهدات، أو القوانين، أو إتفاقات المساعدة المتبادلة المطبقة أو المعمول بها.

وبمقتضى الفقرة الثانية من المادة 25 فإن كل طرف يكون مطالبا أن يضع موضع التنفيذ الأسس القانونية التي تسمح له بالموافقة على الأشكال المحددة للتعاون الذي يتم وضعه في باقي بنود هذا الفصل، إذا كانت الإتفاقيات أو الإتفاقات أو القوانين

[1] – إتفاقية بودابست، مرجع سابق.

[2] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري وابحريني على ضوء بودابست، مرجع سابق، ص 258.

الخاصة به تحتوي على مثل هذه النوعية من الشروط، أن إتاحة مثل هذه الآليات خاصة تلك المذكورة في المواد 29 إلى 35 (الشروط الخاصة العنوان1، 2، 3) يعتبر شيئا ضروريا للتعاون الفعال في القضايا الجنائية المتعلقة بالحاسب الآلي[1].

بعض الأطراف ليست في حاجة إلى تبني إجراءات تشريعية خاصة من أجل تطبيق البنود المشار إليها في الفقرة الثانية من المادة 25 وذلك لأن شروط الإتفاقيات الدولية التي تقوم بتنظيم تفاصيل المساعدة المتبادلة تعتبر في قوة القانون بطريقة آلية[2].

ومن هذا المنظور توجد ثلاثة إحتمالات أمام الأطراف: الأول بمقدورهم إعتبار هذه الشروط لها قوة القانون بطريقة آلية، والثاني أن يكون قد سبق لهؤلاء الأفراد أن نظموا تشريعا للمساعدة المتبادلة مرنا بطريقة كافية تسمح لهم بتوفير إجراءات المساعدة المتبادلة المقررة بطريقة كافية تسمح لهم بتوفير إجراءات المساعدة المتبادلة المقررة في تطبيق هذا الفصل، والثالث أنه بمقدور الأطراف أن يتبنوا بطريقة سريعة إجراءات تشريعية ضرورية لهذا الغرض.

البيانات المعلوماتية سريعة الزوال أو التبخر، إذ يكفي مجرد الضغط على بعض المفاتيح أو تشغيل برنامج أوتوماتيكي من أجل محوها، مما يؤدي إلى استحالة تتبع مرتكب جريمة أو تدمير أدلة إجرامه.

كذلك هناك بعض أشكال من بيانات الحاسب ويتم تخزينها لفترات زمنية قصيرة ثم يتم محوها، ولذا فإنه في بعض الحالات إذا لم يتم تجميع بسرعة، فإن أشخاصا أو أشياء يمكن أن يلحقها ضرر جسيم.

أيضا في الحالات العاجلة فإن الطلب والرد عليه يجب أن يكون عاجلا.

---

[1] – راجع باللغة الفرنسية المذكرة التفسيرية لإتفاقية بودابست 7 نوفمبر 2001.

Convention sur la cybercriminalité « STEno-185, Rapportexplicatif adopté le 8 novembre 2001, pp 80-83.

[2]- راجع باللغة الأنجليزية مسودة المذكرة التفسيرية إتفاقية بودابست ستراسبورج 14 فبراير 2001.

Draft explantary memorandum to the draft convention on Cybercrime », Strasbourg 14 February 2001.

لهذه الأسباب مجتمعة كان الغرض من الفقرة الثالثة من المادة 25 هو تسهيل عملية الإسراع في الحصول على المساعدة المتبادلة بحيث لا تضيع المعلومات أو الأدلة الأساسية بسبب محوها قبل إعداد وإرسال الرد على طلب المساعدة[1].

والفقرة الثالثة سالفة الذكر تعالج هذا الموضوع من خلال أمرين: الأول السماح للأطراف بتقديم طلب المساعدة عن طريق وسائل سريعة الاتصال بدلا من ولوج وسائل تقليدية أكثر بطئا في نقل المستندات المكتوبة داخل مظروف مختوم عن طريق الحقيبة الدبلوماسية أو عن طريق البريد.

والثاني: إلزام الطرف المقدم إليه طلب المساعدة أن يستخدم وسائل سريعة للاتصال للرد على هذا الطلب، كل طرف مطالب بأن يكون لديه القدرة على تطبيق هذا الإجراء إذا لم يكن قد سبق تقريره في الاتفاقيات أو التشريعات أو اتفاقات المساعدة الخاصة به، الفاكس والبريد الإلكتروني مشار إليه على سبيل البيان، وبالتالي فإن كل طريقة أخرى عاجلة للاتصال تتوافق مع ظروف الحال يمكن استخدامها، وهكذا فإنه كلما تطور التقدم التكنولوجي، كلما أفرز وسائل أخرى سريعة للاتصال يمكن استخدامها في مجال طلب المساعدة القضائية المتبادلة[2].

وبالنسبة للقاعدة المتعلقة بشروط التأكيد الرسمي والأمني المنصوص عليها في الفقرة الثالثة، يمكن للأطراف أن يقرروا فيما بينهم كيفية ضمان التأكيد الرسمي وضمان الأمن بما في ذلك التشفير وخاصة في القضايا الخطيرة.

وأخيرا تسمح الفقرة الثالثة للطرف المقدم إليه الطلب أن يطلب تأكيدا رسميا يتم إرساله عن طريق القنوات التقليدية ليتبع الإرسال السريع إذا إختار ذلك.

---

[1] – هلالي عبد الله أحمد، المواجهة الجنائية المعلوماتية في النظامين المصري والبحريني على ضوء إتفاقية بودابست، مرجع سابق، ص 261.

[2] – هلالي عبد الله أحمد، نفس المرجع، ص 261.

أما الفقرة الرابعة من المادة 25 فإنها تحدد المبدأ العام الذي بمقتضاه أن تضع المساعدة المتبادلة للشروط الواردة في الاتفاقيات وتلك الواردة في القانون الداخلي، ولأمراء في أن هذه التنظيمات تضمن حقوق الأفراد المتواجدين على أرض الطرف المطلوب منه المساعدة، والذين يمكن أن يكونوا موضوعا لطلب المساعدة.

وهكذا على سبيل المثال، فإنه بالنسبة للالتزامات الإجرائية التي يخضع لها المتهم مثل التفتيش والضبط، فإنه لا يتم إجرائه نيابة عن الطرف مقدم الطلب، إلا إذا كانت الشروط الأساسية للطرف المقدم إليه الطلب التي يتم تطبيقها في القضايا المحلية قد تم إستيفائها، كذلك يمكن للأطراف ضمان حماية حقوق الأفراد الذين لهم علاقة بالأشياء التي يتم ضبطها وتوفيرها من خلال المساعدة القضائية المتبادلة.

ومع ذلك، فإن الفقرة الرابعة من المادة 25 لا تنطبق في حالة "وجود شرط مخالف صراحة لما هو مقرر في هذا الفصل وهذا الشرط يستخدم للإشارة إلى أن الإتفاقية تحتوي –كقاعدة عامة– على عدة استثناءات هامة، وأول هذه الاستثناءات أن كل طرف يكون مطالبا بأن يقدم أشكال التعاون المنصوص عليها في المواد الأخرى من هذا الفصل، مثال ذلك التحفظ، التجميع في الوقت الفعلي للبيانات المعلوماتية التفتيش والضبط، إدارة الشبكة، وذلك بمعزل عن مسألة معرفة ما إذا كانت هذه الإجراءات قد سبق أن تقررت في اتفاقيات المساعدة الخاصة بهذا الطرف، أو في اتفاقاته النظيرة، أو في تشريعه الداخلي، استثناء آخر أوردته المادة 27 والذي يطبق دائما على تنفيذ الطلبات أو الالتماسات بدلا من القانون الداخلي للطرف المقدم له الإلتماس، والذي بحكم التعاون الدولي في غياب اتفاقية للمساعدة المتبادلة أو اتفاق نظير بين الطرف الملتمس والطرف المقدم إليه الالتماس، المادة 27 تقدم نظاما لشروط وأسباب الرفض[1].

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء إتفاقية بودابست، مرجع سابق ص 262.

وفقا لاستثناء آخر تقرر صراحة في الفقرة الرابعة من المادة 26، فإن الطرف المقدم إليه الإلتماس لا يمكن أن يرفض طلب المساعدة على الأقل فيما يتعلق بالجرائم المنصوص عليها في المواد من 2 إلى 11 من الإتفاقية، على أساس أن الطرف المقدم إليه الطلب يعتبر أن الطلب يتضمن جريمة تعد ذات طبيعة "مالية".

وأخيرا نورد المادة 29 استثناء يقرر أن التحفظ لا يتم رفضه على أساس التجريم المزودج، مع إمكانية التحفظ بهذا الخصوص.

الأصل أن الفقرة الخامسة من المادة 25 تضع تعريفا للتجريم المزدوج لأغراض المساعدة المتبادلة بالمعنى المقصود في هذا الفصل، فحيثما يتم السماح للطرف المقدم إليه الطلب بإخضاع المساعدة المتبادلة لشرط تجريم مزدوج، كأن يكون هذا الطرف يحتفظ بالحق في استلزم التجريم المزدوج كشرط من أجل تنفيذ التماس أو التحفظ على بيانات معلوماتية في تطبيق الفقرة الرابعة من المادة 29، أو التحفظ العاجل على بيانات معلوماتية مخزنة ففي كل تلك الحالات فإن هذا الشرط يعتبر متوافرا إذا كان السلوك المكون للجريمة محل المساعدة المتبادلة يشكل جريمة جنائية أيضا في القانون الداخلي للطرف المقدم له الطلب، حتى لو كان قانونه الداخلي يضع هذه الجريمة في طائفة مختلفة للجرائم أو كان يستخدم مصطلحا مختلفا في تحديد هذه الجريمة[1].

واستيفاء الشرط بهذه الكيفية يضمن عدم مغالاة الأطراف المقدم لها الطلب في اللجوء إلى معايير صلبة أو جامدة في تطبيق شرط التجريم المزوج، وبما أن الاختلافات بين النظم القانونية من الأمور المقصورة، فإن الاختلاف في المصطلحات، أو في فئات السلوك الإجرامي بين هذه النظم سيكون له وجود بالتأكيد، ولذا فإن مثل هذه الاختلافات ذات الطبيعة الفنية لا يجب أن تعرقل الإلتزام بالمساعدة المتبادلة طالما أن هذا السلوك يشكل جريمة جنائية لكلا النظامين القانونين.

[1] – هلالي عبد الله أحمد، نفس المرجع، ص 263.

وفي كل الحالات ينبغي مراعاة أنه في القضايا التي يتم فيها تطبيق شرط التجريم المزدوج، أن يكون هذا التطبيق بطريقة مرنة تضمن تسهيل عملية المساعدة القضائية.

الفرع الثاني: الأحكام المتعلقة بالمعلومات التلقائية :

من خلال هذا الفرع سوف نستعرض نص المادة 26 أولا في حين سوف نستعرض التعليقات عليها ثانيا.

أولا : نص المادة 26: المعلومات التلقائية [1]:

1- يمكن لأي طرف، في حدود قانونه الداخلي، ودون طلب مسبق، أن يرسل لأي طرف، معلومات يكون قد حصل عليها في نطاق التقنيات الخاصة به، إذا كان يرى أن هذه المعلومات يمكن أن تساعد الطرف المرسل إليه في استجلاء أو إجراء تنقيبات أو تحقيقات تتعلق بموضوع جرائم جنائية مقامة وفقا لهذه المعاهدة، أو عندما تكون هذه الجرائم يمكن أن يؤدي إلى طلب للمساعدة بواسطة هذا الطرف وفقا لهذا الفصل.

2- قبل إرسال هذه المعلومات، يمكن للطرف الذي يقوم بإعدادها أن يطلب أن تظل هذه المعلومات سرية، أو أن تستخدم وفقا لشروط معينة، وإذا كان الطرف المرسل إليه لا يستطيع تلبية هذه الشروط، فإنه يجب عليه إخطار الطرف الآخر بذلك، والذي عليه عندئذ أن يحدد ما إذا كانت المعلومات سوف يتم تقديمها من عدمه، وإذا قبل الطرف المرسل إليه المعلومات تحت شروط معينة، فإنه صبح مقيدا بهذه الشروط.

ثانيا: التعليقات:

هذه المادة تنبثق من شرط نصت عليها اتفاقيات سابقة لمجلس أوروبا، مثل ذلك المادة 10 من الاتفاقية المتعلقة بغسيل الأموال والتفتيش والضبط والمصادرة لنواتج

[1] -إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية، مرجع سابق.

الجريمة (STE N°141) والمادة 28 من الاتفاقية الجنائية الخاصة بالفساد (STE N°173).[1]

كثيرا ما يحدث أن يكون طرف لديه معلومات هامة، ويعتقد هذا الطرف أن تقديم هذه المعلومات يمكن أن يحقق فائدة من أجل التنقيب والتحري أو الإجراءات المفتوحة، والتي لا يعلم بوجودها الطرف صاحب الشأن.

في مثل هذه الحالات، لا يتم تقديم أية طلبات للمساعدة، ولذا تجيز الفقرة الأولى من المادة 26 للدولة التي تحوز معلومة أن تقوم بالاتصال بالدولة الأخرى المعنية دون انتظار كتقديم طلب مسبق.

أنه من المفيد إدراج هذا الشرط، لأنه وفقا للتشريع الداخلي لبعض الدول، إذ أن مثل هذا التأهيل الإيجابي يكون ضروريا من أجل إمكانية الموافقة على المساعدة المتبادلة في غياب وجود طلب، طرف لا يكون مطالبا بتقديم المعلومات للطرف الآخر بشكل تلقائي، إنما يملك حرية التصرف على ضوء الظروف الخاصة بالقضية محل البحث، علاوة على ذلك فإن الإفشاء التلقائي، للمعلومات لا يمنع الطرف الذي يرسلها من القيام بالتنقيب والتحري أو البدء في إجراءات التحقيق في الوقائع التي تم الإفصاح عنها[2].

وتنص الفقرة الثانية من المادة 26 على واقعة أنه في بعض الحالات، قد لا يقوم الطرف الذي لديه معلومات حساسة بإرسالها تلقائيا، إلا باشتراط أن تظل سرية، أو أن تستخدم وفقا لشروط معينة، وهكذا تصبح السرية في مثل تلك الحالات عاملا هاما في

[1] – راجع باللغة الفرنسية المذكرة التفسيرية لإتفاقية بودابست 7 نوفمبر 2001.
Convention sur la cybercriminalité « STEno-185, Rapportexplicatif adopté le 8 novembre 2001, pp 80-83.

[2] – راجع باللغة الأنجليزية مسودة المذكرة التفسيرية إتفاقية بودابست ستراسبورج 14 فبراير 2001.
Draft explantary memorandum to the draft convention on Cybercrime », Strasbourg 14 February 2001.

القضايا التي تكون فيها مصالح الدولة المانحة للمعلومات معرضة للخطر من جراء البوح بتلك المعلومات[1].

إذا كان الطرف المرسل إليه لا يستطيع تلبية تلك الشروط أو المحافظة على طابع السرية الذي يشترط الطرف الراسل، كأن تكون تلك المعلومات لازمة يوصفها أدلة في دعوى عمومية، فإنه يجب عليه في هذه الحالة إخطار الطرف الراسل بذلك، ويقع على هذا الأخير الإقدام أو الأحجام عن تقديم تلك المعلومات، على أنه إذا قبل الطرف المرسل إليه المعلومات تحت شروط معينة، فإنه يصبح مقيدا بهذه الشروط، ويجب عليه الوفاء بها.

المبحث الثاني: الأحكام الإجرائية للمساعدة القضائية المتبادلة لمكافحة الجرائم الإلكترونية :

إن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين، كان لا بد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، ولكي يتم ذلك ويكون هناك تعاون دولي ناجح في مجال تحقيق العدالة كان لزاما تنظيم هذا النوع من التعاون الدولي تشريعيا وقضائيا وتنفيذيا. فالدولة ما دامت عضوا في المجتمع الدولي لا بد لها من الإيفاء بالالتزامات المترتبة على هذه العضوية ومن ضمنها الارتباط بعلاقات دولية وثنائية تتعلق باستلام وتسليم المجرمين.

إن بطء الإجراءات الرسمية يجازف بفقدان الأدلة، وقد تكون بلدان متعددة متورطة في الأمر. ولذا تشكل متابعة وحفظ سلسلة الأدلة تحدياً كبيراً. بل حتى الجرائم "المحلية" قد

[1] راجع المسودات التالية:

Counil of europe draft Convention on Cyber-Crime, October 2, 2000.
Counil of europe draft Convention on Cyber-Crime, November 26, 2000.
Counil of europe draft Convention on Cyber-Crime, Décembre 25, 2000.

يكون لها بعد دولي، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التي مرت الهجمة من خلالها.

وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرَّم وهو في 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 إنجازاً، وهي الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أي أوامر تفتيش أو طلب تسليم المجرم). وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الإتصالات التي جرت مع الوقت في مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هي عملية أكثر إرهاقاً يتم اللجوء إليها عادة عملاً بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية. وهي تشترط في الغالب الأعم أن تكون الجريمة المعنية على درجة معينة من القسوة وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب. ويشار إلى هذا الأمر الأخير باعتباره "تجريما مزدوجا"

و في ما يلي سوف نتناول **إجراءات المساعدة القضائية لمكافحة الجريمة الإلكترونية** في **مطلب أول** و في **المطلب الثاني** سوف نتناول **مجالات المساعدة القضائية لمكافحة الجريمة الإلكترونية** .

المطلب الأول: إجراءات طلب المساعدة القضائية المتبادلة:

سوف نكرس هذا المطلب لدراسة مادتين الأولى المادة 27 المتعلقة بإجراءات طلبات المساعدة القضائية المتبادلة بين الأطراف في ظل غياب اتفاقيات دولية مطبقة والمادة 28 الخاصة بسرية المعلومات وتحديد أوجه استخدامها وذلك على النحو الآتي:

الفرع الأول: الإجراءات المتعلقة بطلبات المساعدة القضائية بين الأطراف في ظل غياب اتفاقية دولية مطبقة:

من خلال هذا الفرع سوف نستعرض نص المادة 27 أولا في حين سوف نستعرض التعليقات عليها ثانيا .

أولا : نص المادة 27: المتعلقة بإجراءات طلبات المساعدة القضائية بين الأطراف في ظل غياب اتفاقية دولية مطبقة [1]:

1-في حالة غياب أية معاهدة للمساعدة المتبادلة أو اتفاقية على أساس تشريعات معمول بها بين الطرف الطالب والطرف المقدم إليه الطلب، فإن الأحكام الواردة في الفقرات 2-9 من هذه المادة سوف يتم تطبيقها، ولن تطبق بنود هذه المادة عندما تكون هذه المعاهدة أو الاتفاقية أو التشريع موجودا، ما لم تتفق الأطراف المعنية على تطبيق كل هذه المادة أو أجزاء منها.

2-أ- يجب على كل طرف أن يعين هيئة مركزية أو هيئات تكون مسؤولة عن إرسال أو الرد على طلبات المساعدة المتبادلة أو تنفيذ هذه الطلبات أو إرسالها إلى السلطات المختصة.

ب- يجب على الهيئات المركزية أن تتصل ببعضها البعض بشكل مباشر.

[1] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية , مرجع سابق .

ج- يجب على كل طرف، في وقت التوقيع، أو أن يرسل لسكرتير عام مجلس أوربا أسماء وعناوين الهيئات المحددة تبعا لهذه الفقرة.

د- يجب على السكرتير العام لمجلس أوربا أن يشكل ويحفز سجلا للهيئات المركزية المحددة من قبل الأطراف، ويجب على كل طرف أن يتأكد أن التفاصيل المدرجة بالسجل صحيحة دوما.

3-طلبات المساعدة المتبادلة تبعا لهذه المادة سوف تنفذ تبعا للإجراءات المحددة بواسطة الطرف المقدم للطلب، باستثناء أن يكون ذلك لا يتوافق مع قانون الطرف المقدم إليه الطلب.

4-بالإضافة إلى شروط أو أسباب الرفض المنصوص عليها في الفقرة الرابعة من المادة 25 فإنه يمكن رفض طلب المساعدة بواسطة الطرف المقدم إليه الطلب إذا:

أ. كان الطلب يحتوي على جريمة يعتبرها الطرف المقدم إليه هذا الطلب جريمة سياسية أو جريمة تتصل بجريمة سياسية، أو.

ب.إذا كان الطرف المقدم إليه الطلب يعتقد أن تنفيذ هذا الطلب يمكن أن ينتهك سيادته، أو نظامه العام، أو مصالحه الأخرى الأساسية.

5- يمكن للطرف المقدم له طلب المساعدة أن يرجأ البت فيه إذا كان من شأن تنفيذه الإضرار بالتقنيات أو الإجراءات التي تقوم بها سلطاته.

6- قبل رفض أو قبول تعاونه، يجب على الطرف المقدم له طلب المساعدة، حينما يرى أن ذلك ملائما، وبعد التشاور مع الطرف المقدم للطلب، أن يرى ما إذا كان من الممكن أن يتم تنفيذ هذا الطلب جزئيا أو تبعا للشروط التي يرى أنها ضرورية.

7-يجب على الطرف المقدم إليه طلب المساعدة، أن يخطر الطرف المقدم للطلب على الفور بالنتيجة التي انتهى إليها بخصوص هذا الطلب، فإذا رفض طلب المساعدة أو تم تأجيله فيجب عليه أن يقدم أسباب هذا الرفض أو التأجيل، كما يجب على الطرف المقدم إليه الطلب أيضا أن يخطر مقدم الطلب بأية أسباب تجعل من المستحيل تنفيذ هذا الطلب أو تؤدي إلى أرجائه.

8-بمقدور الطرف المقدم بطلب المساعدة أن يطلب من الطرف المقدم له هذا الطلب أن يحافظ على سرية واقعة وموضوع كل طلب يقدمه في ظل هذا الفصل الحالي، وأن يظل سريا، باستثناء الإجراء الضروري اللازم لتنفيذ هذا الطلب، وإذا كان الطرف المقدم إليه الطلب لا يستطيع الالتزام بالسرية فإنه يجب عليه إخطار الطرف المقدم للطلب، والذي يكون بمقدوره أن يقرر إمكانية المضي في تنفيذ طلبه من عدمه,.

أ. في حالة الاستعجال، بمقدور السلطات القضائية للطرف الذي يقدم الطلب أن ترسل مباشرة طلبات المساعدة المتبادلة أو الاتصالات إلى سلطات الطرف المقدم له الطلب، وفي مثل هذه الحالات يجب إرسال نسخة من الطلب –في الوقت نفسه– إلى الهيئة المركزية للطرف المقدم له الطلب من خلال الهيئة المركزية للطرف الذي يقدم الطلب.

ب.كل طلب أو اتصال يتم عمله في ظل هذه الفقرة، يمكن أن يتم من خلال المنظمة العالمية للبوليس الدولي (أنتربول).

ج. عندما يقدم طلب للمساعدة القضائية المتبادلة طبقا للفقرة الفرعية (أ) من هذه المادة وتكون السلطة المقدم لها الطلب غير مختصة بالنظر فيه، فإنه يجب عليه أن تحيل هذا الطلب إلى السلطة الوطنية المختصة، مع الإخطار المباشر للطرف المقدم للطلب بذلك.

د. الطلبات أو الاتصالات التي تتم تطبيقا لهذه الفقرة والتي لا تفرض إجراء إلزاميا، يمكن أن ترسل مباشرة إلى السلطات المختصة للطرف المقدم إليه الطلب بواسطة السلطات المختصة للطرف مقدم الطلب.

هـ. يمكن لأي طرف، في لحظة التوقيع، أو أن يخطر سكرتير عام مجلس أوربا، من أجل فعالية الطلبات التي يتم عملها وفقا لهذه الفقرة، يجب أن ترسل لهيئته المركزية.

ثانيا: التعليقات:

تلزم المادة 27 الأطراف بتطبيق إجراءات وشروط معينة بالنسبة للمساعدة القضائية المتبادلة في حالة عدم وجود معاهدة أو اتفاقية تستند عليها التشريعات الموحدة أو المتمثلة وتكون سارية المفعول بين الطرف مقدم الطلب والطرف المقدم إليه الطلب، وهكذا تدعم هذه المادة المبدأ العام القائل بأن المساعدة القضائية المتبادلة يجب أن يتم تنفيذها تطبيقا لمعاهدات متطابقة أو اتفاقيات متناظرة لهذه المساعدة، ومن هذا المنظور لم يشأ واضعوا هذه الاتفاقية إنشاء نظام عام منفصل للمساعدة القضائية يتم تطبيقه بدلا من المعاهدات أو الاتفاقيات المطبقة بالفعل[1]، إذ أن الأمر يكون أكثر سهولة ويسرا إذا تم تطبيق المعاهدات أو الاتفاقيات التي سبق للأطراف معرفتها جيدا وبالتالي يتجنبون أية مخاطرة أو غموض يمكن أن ينجم عن تطبيق نظم منافسة ويبقى فقط – كما أشرنا سلفا– ما يتعلق بالآليات التي يتم الاحتجاج إليها بصفة خاصة للمساعدة القضائية الفعالة في المواد الجنائية المتعلقة بالمعلوماتية، مثال تلك المنصوص عليها في المواد من 29 إلى 35 تحت عنوان (أوضاع خاصة) فإن كل طرف يكون ملزما بإرساء الأسس القانونية التي من شأنها تسهيل تنفيذ تلك الأشكال من المساعدة القضائية المتبادلة، إذا كانت

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء إتفاقية بودابست، مرجع سابق ص 269.

معاهدات واتفاقيات أو قوانين المساعدة القضائية السارية المفعول لا تحتوي على مثل هذه الأوضاع الخاصة[1].

وترتيبا على ذلك، فإن معظم أشكال المساعدة القضائية المتبادلة المذكورة في هذا الفصل سوف يتم تنفيذها بمقتضى المعاهدة الأوروبية للمساعدة القضائية المتبادلة في المواد الجنائية (STE N°30) والبرتوكول الخاص بها (STE N°99) بين أطراف تلك الاتفاقيات، بعبارة أخرى فإن أطراف هذه الاتفاقية الذين قاموا بالتوقيع على معاهدات ثنائية للمساعدة القضائية المتبادلة، أو اتفاقيات أخرى متعددة تحت إشراف للمساعدة القضائية المتبادلة في المسائل الجنائية مثال ذلك الاتفاقيات المرتبطة بدول أعضاء في الاتحاد الأوروبي، سوف تمرون في تطبيق هذه البنود، مضافا إليها آليات معينة تطبق في الإجرام المعلوماتي، والتي سيأتي تفصيلها لاحقا إلا إذا اتفق الأطراف تطبيق كل أو بعض هذه المادة[2].

ويمكن أيضا أن تقوم المساعدة القضائية المتبادلة على أساس اتفاقيات تبرم بناء على تشريعات موحدة أو متماثلة، مثال ذلك نظام التعاون القائم بين دول الشمال (الدول الاسكندنافية) والذي تم الإعتراف به بواسطة الاتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية (المادة 25 الفقرة الرابعة)، والنظام القائم بين أعضاء الكومنولث[3].

---

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء إتفاقية بودابست، مرجع سابق ص 267.

[2] – هلالي عبد الله أحمد، الجوانب الموضوعية الإجرائية لجرائم المعلوماتية، د ط، دار النهضة العربية، القاهرة، 2003، ص 121

[3] – جميل عبد الباقي الصغير، الجوانب إجرائية المتعقة بالأنترنت، ط 1، دار النهضة العربية القاهرة، 2001، ص 97.

وأخيرا فإن الإشارة إلى معاهدات أو اتفاقيات المساعدة القضائية المتبادلة على أساس تشريعات موحدة أو متماثلة، لا يقتصر نطاقه على تلك المعاهدات أو الاتفاقيات نافذة المفعول وقت سريان هذه الاتفاقية الحالية، ولكن يمتد أيضا ليشمل تلك التي يمكن تبنيها لاحقا.

الفقرات من 2 إلى 10 من المادة 27 (بشأن الإجراءات المتعلقة بطلبات المساعدة القضائية المتبادلة في حالة غياب اتفاقيات دولية مطبقة) تقرر عددا من القواعد المعينة التي تنظم المساعدة القضائية في حالة غياب معاهدة أو اتفاقية للمساعدة القضائية ترتكز على أساس تشريعات موحدة أو مماثلة، تتضمن إنشاء هيئة مركزية، فرض شروط، أسباب وإجراءات في حالة الإرجاء أو الرفض، سرية الطلبات والاتصالات المباشرة، وهكذا فإنه فيما يتعلق بتلك المسائل يتم معالجتها صراحة، وفي ظل غياب معاهدة أو اتفاقية للمساعدة قائمة على أساس تشريعات موحدة أو متماثلة، فإن أحكام هذه المادة التي تطبق[1].

ومن ناحية أخرى، فإن المادة 27 لا تقدم قواعد تتعلق بمسائل أخرى تم التعامل معها من خلال تشريع محلي ينظم المساعدة القضائية الدولية، مثال ذلك عدم وجود أية شروط تتعلق بشكل أو محتوى الطلبات، أخذ شهادة الشهود في دولة الطرف مقدم الطلب أو دولة الطرف المقدم إليه الطلب، توفير وثائق رسمية، نقل الشهود المحتجزين، أو المساعدة في مسائل المصادرة وبالنسبة لهذه الموضوعات، فإن الفقرة الرابعة من المادة 25 تنص على أنه حالة غياب شرط معين في هذا الفصل، فإن القانون الداخلي للطرف المقدم إليه الطلب يحدد النماذج التفصيلية لهذا النوع من المساعدة [2].

[1] – جميل عبد الباقي الصغير، مرجع سابق، ص 98.

[2] – علي حسن الطوالبة، التعاون القضائي الدولي في محالمكافحة اجرائم الإلكترونية، دارالعوم، بغداد، 2010، ص 153.

تتطلب الفقرة الثانية إنشاء هيئة مركزية أو أكثر يناط بها مسؤولية إرسال أو الرد على الطلبات الخاصة بالمساعدة القضائية المتبادلة، فلقد أصبح إنشاء هذه الهيئات المركزية السمة الغالبة في الاتفاقيات الحديثة المتعلقة بالمساعدة الجنائية المتبادلة في المواد الجنائية، فهي أكثر فائدة لضمان رد الفعل السريع والذي يعد هاما وضروريا في مجال مكافحة الإجرام المعلوماتي وكل ما يتعلق بالحاسب الآلي.

ففي المقام الأول، فإن الإيصال المباشر للطلبات بين هذه الهيئات سيكون أكثر سرعة وفعالية من أن يتم نقلها عبر الطريق الدبلوماسي، كما أن هذه الهيئات سوف تولى عملية إرسال أو استقبال هذه الطلبات جل اهتمامها، كما أنها تضمن أن المسؤولين عن تطبيق القوانين في البلاد المشاركة قد صاغوا الطلبات في الوضع الأمثل لها وفقا للقواعد القانونية السارية المفعول لدى الطرف المقدم إليه الطلب، وبالأخص الطلبات العاجلة والخطيرة.

يتم تشجيع الأطراف على تحديد هيئة مركزية واحدة للمساعدة القضائية المتبادلة لاعتبارات الفعالية، وعموما فإن الهيئة المعينة لهذا الغرض وفقا لمعاهدة المساعدة القضائية المتبادلة أو للقانون الداخلي ستكون أكثر كفاءة عند تطبيق هذه المادة، ومع ذلك فبمقدور أي طرف أن يعين أكثر من هيئة مركزية حيثما كان ذلك ملائما وفقا لنظامه الخاص بالمساعدة القضائية المتبادلة، مع ملاحظة أنه في حالة إنشاء أكثر من هيئة مركزية فعلى الطرف الذي قام بذلك، أن يضمن التفسير الموحد للشروط الخاصة بالاتفاقية من كلتا الهيئتين، وكذلك التعامل بسرعة وكفاءة من هاتين الهيئتين بالنسبة للطلبات الواردة والمرسلة. وفي جميع الأحوال لكل طرف إبلاغ السكرتير العام لمجلس أوروبا بأسماء وعناوين، بما في ذلك عنوان البريد الالكتروني ورقم الفاكس بالنسبة للهيئة أو الهيئات المعنية باستقبال أو الرد على طلبات المساعدة القضائية المتبادلة وفقا لهذه المادة.

أحد الأهداف الجوهرية التي تسعى إليها الدولة التي تطلب مساعدة قضائية المتبادلة هو ضمان احترام أوضاع قانونها الداخلي، الذي يحكم قبولية الأدلة والذي يسمح باستخدام هذه الأدلة أمام قضائها . ولضمان إمكانية استيفاء قواعد هذه الأدلة، فإن الفقرة الثالثة من هذه المادة تلزم الطرف المقدم إليه الطلب بتنفيذ الطلبات وفقا للإجراءات المحددة بواسطة الطرف مقدم الطلب، إلا إذا كانت هذه الإجراءات لا تتوافق مع قانونه والجدير بالذكر أن هذه الفقرة لا تتعلق بالتزام احترام القواعد الإجرائية الفنية ولا تتعلق بضمان الإجراءات الجوهرية وهكذا على سبيل المثال، فإن الطرف المقدم للطلب لا يستطيع إلزام الطرف المقدم إليه الطلب تنفيذ عمليات التفتيش والضبط التي لا تستوفي الشروط القانونية الجوهرية الخاصة بالطرف المقدم إليه الطلب[1].

تنص الفقرة الرابعة من المادة 27 من هذه الاتفاقية على امكانية رفض طلبات المساعدة القضائية المتبادلة المقدمة وفقا لهذه المادة، ويمكن رفض هذه المساعدة وفقا للأسس المنصوص عليها في 4/25 بمعنى الأسس المنصوص عليها في قانون الطرف المقدم إليه الطلب، بما في ذلك الاعتداء على سيادة الدولة، الأمن، النظام العام، أو المصالح الأساسية الأخرى، وكذلك إذ اعتبر الطرف المقدم إليه الطلب أن الجريمة محل الطلب جريمة سياسية أو مرتبطة بجريمة سياسية، ومن أجل تعزيز مبدأ إعطاء نظام المساعدة القضائية المتبادلة أوسع نطاق ممكن، فإنه يجب تقليص أسباب الرفض التي وضعها الطرف المقدم إليه الطلب، بحيث تكون في نطاق محدود[2]، وأن تستخدم باعتدال وترتيبا على ذلك لا ينبغي التوسع في حالات الرفض بحيث تصبح إمكانية رفض المساعدة القضائية يتم بشكل مطلق، أو أن يتم وضع شروط ثقيلة للغاية بالنسبة لفئات الأدلة والمعلومات.

[1] – هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عيها، مرجع سابق، ص 211.

[2] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء إتفاقية بودابست، مرجع سابق، ص 270.

ووفقا لهذا التصور، فلقد أصبح من المقرر أنه بعيدا عن أسباب الرفض المشار إليها في المادة 28، فإن رفض المساعدة القضائية استنادا إلى حماية البيانات لا يمكن أن يثار إلا في الحالات الاستثنائية التي يكون فيها تعارض مع المصالح العامة.

تجيز الفقرة الخامسة للطرف المقدم إليه الطلب أن يقوم بتأجيل طلب المساعدة القضائية بدلا من رفضه، وذلك في حالة ما إذا كان التنفيذ الفوري للبنود المشار إليها في هذا الطلب سوف تلحق ضررا بتنقيبات أو إجراءات تحقيق تقوم بها سلطاته، وهكذا على سبيل المثال، إذا كان الطرف مقدم الطلب قد طلب الحصول على أدلة معينة أو أخذ شهادة أحد الشهود بغرض التحقيق أو المحاكمة، وكانت هذه الأدلة أو الشهادة نفسها ضرورية لمتابعة الدعوى بالنسبة للطرف المقدم إليه الطلب، ففي مثل هذه الحالة يكون التأجيل مبررا[1].

تنص الفقرة السادسة على أنه حيثما ترفض المساعدة القضائية أو يتم تأجيلها، فإنه بمقدور الطرف المقدم إليه الطلب، أن يقوم بتنفيذ هذه المساعدة بشروط معينة، وذلك بعد التشاور مع مقدم الطلب، كأن يقوم بتعديل الشروط التي وضعها مقدم الطلب ليتماشى مع الشروط يرى أنها ضرورية أو أن يقوم بتنفيذ جزئي لبنود طلب المساعدة[2] .

تلزم الفقرة السابعة الطرف المقدم إليه الطلب إعلام الطرف الطلب بنتيجة طلب المساعدة الذي قدمه، مع إبداء أسباب الرفض أو التأجيل. وتعزيز الغاية المتوخاة من هذا التسبيب إلى مساعدة طرف مقدم الطلب على فهم كيفية تفسير متطلبات تلك المادة لدى الطرف المقدم إليه الطلب، مما يعمل على إنشاء قاعدة للتشاور، بغرض تحسين فعالية

[1] – جميل عبد الباقي الصغير، مرجع سابق، ص 99.

[2] – نفس المرجع، ص 99.

المساعدة القضائية وتزويد الطرف مقدم الطلب معلومات تتعلق بالواقعة محل البحث لم تكن معلومة له مسبقا بشأن وجود أو وضع الشهود أو الأدلة[1].

قد يحدث أن طرفا ما يقدم طلب المساعدة القضائية بخصوص قضية ذات خطورة، أو أن قضية معينة يترتب على الإفصاح المبكر عن محتوياتها نتائج خطيرة، في مثل هذه الحالات، فإن الفقرة الثامنة ترخص للطرف مقدم الطلب أن يطلب من الطرف المقدم له الطلب أن محل وموضوع الالتماس سريا ومع ذلك فإن السرية لا يمكن أن تكون إلا في النطاق الذي يعوق الطرف المقدم إليه الطلب من الحصول على الأدلة والمعلومات المطلوبة، كأن يتم الإفصاح – على سبيل المثال– عن بعض المعلومات التي من خلالها الحصول على أمر قضائي للبدء في تنفيذ طلب المساعدة القضائية، أو عندما يحتاج الأشخاص الذين بحوزتهم الأدلة أن يحاطوا علما بمحتويات الطلب حتى يكون بمقدورهم تنفيذ ما يطلب منهم تنفيذه، وإذا كان الطرف المقدم له الطلب لم يكن في مقدوره المحافظة على سرية الطلب، يجب عليه إخطار مقدم الطلب بذلك، ولهذا الأخير إمكانية سحب طلبه أو تعديله[2] .

الهيئات المركزية المعينة وفقا للفقرة الثانية سوف تتصل مباشرة ببعضها البعض، ومع ذلك، فإنه في حالات الاستعجال، فإن القضاة والمدعين العموميين للطرف المقدم للطلب يمكنهم أن يرسلوا مباشرة لنظائرهم لدى الطرف المقدم إليه الطلب طلبات المساعدة القضائية المتبادلة، وفي هذه الحالة إذا طبق القضاة والمدعون العموميون هذا الإجراء فيجب إرسال نسخة من هذه الطلبات لكل من الهيئة المركزية التابعة لهم الهيئة المركزية التابعة للطرف المقدم إليه الطلب[3].

[1] – علي حسن الطوالبة، مرجع سابق، ص 157.

[2] – محمد فاضل، التعاون الدولي في مكافحة جرائم الأنترنت، ط1، دار الهدى، البحرين ، د س، نشر، ص 352.

[3] – علي حسن الطوالبة، مرجع سابق، ص 159.

ووفقا للبند "ب" يمكن إرسال الطلبات عن طريق الأنتربول (البوليس الدولي).

وإذا تسلمت الهيئات المركزية التابعة للطرف المقدم إليه الطلب طلبا لا يدخل اختصاصها فعليها أن تقوم بأمرين أولهما تحويل هذا الطلب إلى الجهة المختصة التابعة للطرف المقدم إليه الطلب وثانيهما إبلاغ الهيئات التابعة للطرف مقدم الطلب بعملية التحويل التي قاموا بها.

ووفقا للبند "د" يمكن إرسال طلبات المساعدة القضائية مباشرة بدون تدخل الهيئات المركزية، وأيضا إذا لم تكن هذه الطلبات تحمل طابع الاستعجال، طالما كانت الهيئة التابعة للطرف المقدم إليه الطلب قادرة على تلبية الطلب دون حاجة إلى اتخاذ تدابير قسرية.

وأخيرا فإنه وفقا للبند "هـ" يكون بمقدور أي طرف أن يقوم بإبلاغ الآخرين، بأن يتم إرسال طالبات المساعدة القضائية مباشرة إلى الهيئة المركزية لإعتبارات الفعالية، وذلك من خلال السكرتير العام لمجلس أوربا.

الفرع الثاني: سرية المعلومات و تحديد أوجه إستخدامها:

من خلال هذا الفرع سوف نستعرض نص المادة 28 أولا في حين سوف نستعرض التعليقات عليها ثانيا .

أولا : نص المادة 28: المتعلقة بالسرية وتحديد الاستخدام[1]:

1- عندما لا تكون هناك معاهدة للمساعدة القضائية المتبادلة أو اتفاقية على أساس تشريعات موحدة أو متماثلة معمول بها بين الطرف الطالب للمساعدة والطرف المقدم إليه طلب المساعدة، فإن أحكام هذه المادة سوف تنطبق، ولن تنطبق أحكام

[1] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية، 2001/11/23.

هذه المادة عندما تكون هذه المعاهدة، أو الاتفاقية، أو التشريعات موجودة، ما لم تتفق الأطراف المعنية على تطبيق كل هذه المادة أو جزء منها.

2- بمقدور الطرف المقدم إليه الطلب أن يعلق تقديم المعلومات أو الوثائق استجابة لهذا الطلب على شرط:

أ. أن يتم الحفاظ على سرية المعلومات، حيث أن طلب المساعدة القضائية المتبادلة لن يتحقق في غياب هذا الشرط، أو ألا تستخدم هذه المعلومات في تحقيقات أو إجراءات غير المذكورة في الطلب.

3- إذا كان الطرف المقدم للطلب لا يستطيع تلبية أحد الشروط المشار إليها في الفقرة "2فعليه أن يخطر على الفور الطرف المقدم إليه الطلب، والذي يحدد حينئذ ما إذا كان يجب مع ذلك تقديم المعلومات والوثائق أم لا، وإذا وافق الطرف المقدم للطلب على هذا الشرط فإنه يجب أن يلتزم به.

4- كل طرف يقدم معلومات أو وثائق تبعا للشروط المشار إليها في الفقرة "2" يمكن أن يطلب من الطرف الآخر وفقا لهذا الشرط، أن يحدد أوجه استخدام هذه المعلومات أو الوثائق.

ثانيا: التعليقات:

هذا النص مقرر بصفة محددة لحدود استخدام المعلومات أو المواد، بقصد السماح للطرف المطلوب منه، في الحالات التي تكون فيها هذه المعلومات أو المواد ذات حساسية، وذلك لتأكيد أن استخدامها محدد في إطار ما هو مقرر للمساعدة، أو لتأكيد أنها لن يتم بثها لغير المسؤولين في السلطات لدى الطرف الطالب، وتسمح هذه القيود بوجود ضمانات متوافرة بذاتها لحماية البيانات.

كما هو الشأن في المادة 27، فإن المادة 28 تنطبق فقط عندما لا يكون هناك معاهدة مساعدة متبادلة، أو ترتيبات على أساس رسمي أو تشريع المعاملة بالمثل نافذا بين الطرف الطالب والمطلوب منه، فإذا كانت مثل هذه المعاهدة أو الترتيبات نافذة فإن نصوصها المتعلقة بالسرية واستخدام القيود تنطبق عوضا عن النصوص المقررة في هذه المادة، إلا إذا اتفق الأطراف على خلاف ذلك، وهذا يتفادى التشابك بين معاهدات المساعدة القانونية المتبادلة الجماعية والثنائية (MLATs) وكذلك الترتيبات المشابهة، وبذلك تسمح للمهنيين باستمرار العمل وفقا للنظام المفهوم والعادي عوضا عن السعي إلى تطبيق وسيلتين قد تكونان متعارضتين[1].

تسمح الفقرة 2 للطرف المطلوب منه، حال الاستجابة لطلب المساعدة المتبادلة، بتقرير نوعين من الشروط:

الأول: يجوز للطرف المطلوب منه طلب اعتبار المعلومات أو المواد التي يتم تزويدها سرية عندما لا يتم للطلب حال عدم وجود مثل هذا الشرط، مثلما هو الشأن في هوية شخص المرشد، وليس من المناسب تطلب السرية المطلقة في الحالات التي يلتزم فيها الطرف المطلوب منه بتزويد المساعدة المطلوبة، كما قد تعد، في العديد من الحالات مهددة لقدرة الطرف الطالب على نجاح التحقيق أو الاتهام في الجريمة مثلما هو الشأن حال استخدام الدليل في محاكمة عامة (بما في ذلك الكشف الإجباري)[2].

ثانيا: يمكن أن يقوم الطرف المطلوب منه المساعدة القيام بإضافة التزام في شكل شرط بأن المعلومات أو المواد لن يتم استخدامها في تحقيقات أو إجراءات غير تلك وردت في الطلب، ولكي يمكن تطبيق هذا الشرط فإنه يجب أن يتقرر بناء على طلب الطرف

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني، على ضوء اتفاقية بودابست، مرجع سابق، ص 277.

[2] – هلالي عبد الله أحمد،، نفس المرجع، ص 277.

المطلوب منه، وفي غير ذلك فإنه لا يوجد مثل هذا القيد على الاستعمال من قبل الطرف الطالب، وفي الحالات التي يتم فيها تقرير ذلك، فإن هذا الشرط يتم لتأكيد أن المعلومات والمواد يمكن فقط أن يتم استخدامها للأغراض المقررة في الطلب، وبذلك يتم رفض استخدام المواد لأغراض أخرى بدون رضا الطرف المطلوب منه، وهناك استثناءان على حدود الاستخدام تم الاعتراف بهما من قبل المفاوضين وتم إدراجهما ضمنا في عبارات هذه الفقرة. الأول: فإنه وفقا للمبادئ القانونية الأساسية في العديد من الدول فإنه إذا كانت المواد المطلوبة تعد دليل براءة لشخص تمت إدانته فإنه يجب أن يتم كشفها للدفاع أو السلطة القضائية، وبالإضافة إلى ذلك، فإن أغلب المواد وفقا لنظم المساعدة المتبادلة معدة للاستخدام في المحاكمة، وفي العادة أثناء المحاكمة العلنية (بما في ذلك الإلزام بالحضور)، فإذا اتخذ هذا الكشف مكانا فإن المواد المذكورة يكون قد تم تمريرها إلى النطاق العلني، وفي هذه الحالات فإنه لن يكون ممكنا تأكيد السرية في التحقيق أو الإجراءات المستهدفة من قبل المساعدة المتبادلة[1].

تقرر الفقرة 3 أنه إذا كان الطرف الذي يتم تحويل المعلومات إليه لا يمكنه الإذعان للشرط المقرر، فإنه يجب أن يعلن الطرف المزود، الذي يتوافر له الإمكانية لعدم تزويد المعلومات، فإذا وافق الطرف المستلم على الشرط فإنه يكون له شرف تطبيقه.

تسمح الفقرة 4 بإمكانية قيام الطرف الطالب بطلب الحصول على تفسير حول استخدام المعلومات أو المواد التي تم استلامها وفقا للشروط المقررة في الفقرة 2، وذلك بقصد التأكد من أن الطرف المطلوب منه قد احترم الشرط، ومن المتفق عليه أن الطرف المطلوب منه لا يمكن له الإفراط في البرهان كما هو الحال في السماح بالدخول كل مرة على المعلومات.

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني، على ضوء اتفاقية بودابست، مرجع سابق، ص 278.

المطلب الثاني: مجالات المساعدة المتبادلة لمواجهة جرائم المعلوماتية :

نتناول في هذا الفرع مجالين هامين هما:

المجال الأول: المساعدة المتبادلة في مجال الإجراءات الوقتية العاجلة (المادتان 29-30) و حملناه عنوان الفرع الاول .

المجال الثاني: المساعدة المتبادلة في مجال سلطات التحقيق (المواد 31-34) و حملناه عنوان الفرع الثاني .

والهدف من المطلب الحالي هو تقرير آليات خاصة بقصد اتخاذ خطوة دولية موحدة ومؤثرة ذات فعالية في حالة الجرائم المرتبطة بالحاسوب والدليل في هيئته الالكترونية.

الفرع الأول: المساعدة المتبادلة في مجال الإجراءات الوقتية العاجلة :

سنتناول في هذا الفرع مادتين المادة 29 المتعلق بالتحفظ العاجل على بيانات معلوماتية مخزنة في نظام معلوماتي يوجد داخل أراضي طرف آخر، والمادة 30 الخاصة بالإفضاء العاجل لسرية بيانات المرور المتحفز عليها في دولة أخرى. وذلك على النحو الآتي:

أولا: التحفظ المعجل على البيانات المخزنة في الحاسوب :

من خلال هذا الجزء من البحث سوف نستعرض نص المادة 29 ومن ثم نتناول التعليقات عليها.

أ- نص المادة 29 المتعلقة بالتحفظ العاجل على بيانات الحاسب المخزنة[1]:

1-يمكن لأي طرف أن يطلب من طرف آخر أو يأمر أو يفرض بطريقة أخرى التحفظ العاجل على البيانات المخزنة بواسطة نظام معلوماتي يوجد داخل أراضي ذلك الطرف،

[1] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية , مرجع سابق .

والتي بخصوصها ينوي الطرف الملتمس أن يرسل طلبا للمساعدة المتبادلة من أجل تفتيش هذه البيانات أو الوصول إليها، أو ضبطها أو الحصول عليها، أو إفشاء سريتها.

2-طلب التحفظ على البيانات المقدم تبعا للفقرة الأولى يجب أن يحدد:

أ. السلطة التي تطلب التحفظ.

ب. الجريمة محل التحقيق الجنائي مع ملخص للوقائع المتصلة بها.

ج. البيانات المعلوماتية المخزنة الواجب التحفظ عليها وطبيعة علاقتها مع الجريمة.

د. أية معلومات متوافرة تسمح بتحديد هوية البيانات المعلوماتية المخزنة أو موقع النظام المعلوماتي.

هـ. ضرورة إجراء التحفظ.

و. من واقع أن هذا الطرف ينوي إرسال طلب للمساعدة المتبادلة من أجل تفتيش هذه البيانات أو الوصول إليها، أو ضبطها أو الحصول عليها، أو إفشاء سريتها.

3-عند تلقي الطلب من الطرف الملتمس، يجب على الطرف المقدم إليه الطلب أن يتخذ كافة الإجراءات اللازمة من أجل التحفظ بشكل عاجل على البيانات المحددة، طبقا لقانونه الداخلي، ومن أجل تلبية هذا الطلب، فإن التجريم المزدوج (أي اعتبار الفعل جريمة من كلا الطرفين) لا يعد شرطا مسبقا لهذا التحفظ.

4-أي طرف يشترط التجريم المشترك كشرط لتلبية طلب المساعدة المتبادلة من أجل تفتيش البيانات أو الوصول إليها أو ضبطها أو الحصول عليها إفشاء سريتها، بمقدوره فيما يتعلق بجرائم أخرى غير تلك المشار إليها في المواد من 2 إلى 11 من هذه الاتفاقية أن يحتفظ بحقه في رفض طلب التحفظ على البيانات تبعا لهذه المادة، في الحالات التي يكون لديه فيها سبب معقول للاعتقاد أنه في لحظة إفشاء سرية هذه البيانات، فإن شرط التجريم المزدوج لم يكن قد م الوفاء به.

5-علاوة على ذلك يمكن رفض طلب التحفظ على البيانات فقط إذا كان:

أ. الطلب يتعلق بجريمة يعتبرها الطرف المقدم إليه الطلب جريمة سياسية، أو جريمة تتصل بجريمة ذات طبيعة سياسية أو.

ب. إذا كان الطرف المقدم إليه الطلب يعتقد أن تلبية الطلب قد يمس سيادته، أو أمنه أو نظامه العام، أو مصالح أخرى جوهرية.

6-إذا كان الطرف المقدم إليه الطلب يعتقد أن مجرد التحفظ لا يكفي من أجل ضمان التوافر المستقبلي للبيانات، أو أنه سيلحق به ضررا بأية صورة كانت، فعليه أن يخطر على الفور الطرف الملتمس بذلك، والذي بمقدوره عندئذ أن يقرر ما إذا كان يجب المضي قدما في تنفيذ الطلب من عدمه.

7-كل تحفظ على البيانات يتم بمقتضى طلب مشار إليه في الفقرة الأولى من هذه المادة، يصبح صالحا لمدة 60 يوما على الأقل، حتى يتسنى للطرف الملتمس عرض طلب التنقيب عن البيانات أو الوصول إليها أو ضبطها أو الحصول عليها أو كشف سريتها، وبعد تلقي مثل هذا الطلب، يجب الاستمرار في التحفظ على البيانات حتى يتم اتخاذ قرار بشأنه.

ب - التعليقات:

تنص هذه المادة على آلية على المستوى الدولي تعادل تلك منصوص عليها في المادة 16 على المستوى القومي، فالفقرة الأولى من هذه المادة تسمح لكل طرف أن يطلب، والفقرة الثالثة تقرر أن على كل طرف أن يكون لديه الطرق القانونية للحصول على التحفز العاجل على بيانات مخزنة لدى نظام معلوماتي في إقليم طرف المقدم إليه الطلب، حتى لا يتم تغيير هذه البيانات، أو نقلها حذفها، خلال الفترة الزمنية اللازمة لإعداد ونقل وتنفيذ طلب المساعدة المتبادلة بخصوص الحصول على هذه البيانات، إن عملية التحفظ عبارة عن إجراء محدود أي طبيعة وقتية معينة للتدخل بطريقة أكثر سرعة من مجرد تنفيذ التماس أو طلب المساعدة المتبادلة التقليدي، إذ أشرنا سلفا فإن البيانات

المعلوماتية تتسم بأنها سريعة الزوال، إذ في بعض نقرات عادة على مفاتيح الحاسب[1]، أو استخدام بعض البرامج الآلية، حتى يتم حذف هذه البيانات أو تغييرها أو نقلها مما يؤدي إلى استحالة تتبع مرتكب الجريمة، أو تدمير الأدلة القاطعة على إجرامه، كذلك هناك بعض أشكال للبيانات المعلوماتية لا يتم تخزينها لفترات قصيرة من الزمن قبل محوها، لهذه الأسباب مجتمعة تم الاتفاق على وجود آلية تضمن توافر هذه البيانات أثناء الفترة الطويلة والمعقدة لتنفيذ الالتماس الرسمي للمساعدة والذي قد يمتد لعدة أسابيع أو شهور.

وإذا كان هذا الإجراء يعد أكثر سرعة من إجراء المساعدة المتبادلة التقليدي، فإنه أيضا يمكن أن يعد أقل تدخلا، فهو لا يتطلب من مسؤولي المساعدة المتبادلة للشخص المقدم إليه الطلب الاستحواذ على بيانات من الجهة القائمة عليها، إنما كل ما هنالك هو أن الطرف المقدم إليه الطلب يضمن أن هذه الجهة – وغالبا ما تكون مورد خدمات أو شخص ثالث– أن يتحفظ على البيانات ولا يقوم بمحوها، انتظارا لصدور أمر بتحويلها إلى السلطات المكلفة بتطبيق القانون في مرحلة لاحقة[2].

كذلك فإن هذا الإجراء يتسم بكونه عاجلا ويحترم حق الإنسان المعنى بهذه البيانات في الخصوصية، لأن تلك البيانات لا يتم كشف سريتها أو فحصها من قبل أي أحد من الموظفين الحكوميين إلا بعد استيفاء المعايير المطبقة بالنسبة لكشف السرية وفقا لمعاهدات المساعدة المتبادلة متعددة الأطراف، ومن ناحية أخرى فإن الطرف المقدم إليه الطلب يكون مسموحا له استخدام إجراءات أخرى لضمان التحفظ العاجل على البيانات،

[1] – هلالي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني، على ضوء اتفاقية بودابست، مرجع سابق، ص 282.

[2] – راجع باللغة الفرنسية المذكرة التفسيرية لإتفاقية بودابست 7 نوفمبر 2001.
Convention sur la cybercriminalité « STEno-185, Rapportexplicatif adopté le 8 novembre 2001, pp 80-83

بما في التنفيذ العاجل لأمر تفتيش هذه البيانات، فالشرط الأساسي في كل هذا هو تسريع الإجراءات إلى أقصى حد ممكن لمنع البيانات من الضياع بشكل يتعذر معه استردادها[1].

الفقرة الثانية تحدد محتوى الطلب الخاص بالتحفظ وفقا لهذه المادة، مع الأخذ في الاعتبار أن الأمر يتعلق بإجراء وقتي، وأن مثل هذا الطلب ينبغي أن يتم إعداده ونقله بسرعة، كما أن المعلومات التي يتم تقديمها تحت شكل ملخص لا تحتوي إلا على الحد الأدنى من المعلومات اللازمة التي تسمح بالتحفظ على البيانات، بالإضافة إلى تحديد هوية السلطة التي تطلب التحفظ والجريمة التي من أجلها اتخاذ هذا الإجراء، كما يجب أيضا أن يحتوي هذا الطلب على ملخص مختصر للوقائع، والمعلومات بشكل يكفي لتحديد البيانات الواجب التحفظ عليها، ومكانها، مع توضيح أن هذه البيانات وثيقة الصلة بالتحقيق أو بالدعوى الخاصة بالجريمة المعنية، كذلك يجب بيان أن عملية التحفظ عملية ضرورية، وأخيرا ينبغي على الطرف الملتمس أو مقدم الطلب أن يتعهد بتقديم طلب المساعدة المتبادلة وذلك حتى يكون مقدوره الحصول على البيانات[2].

الفقرة الثالثة تشير إلى أن مبدأ التجريم المزدوج، أي اعتبار الفعل جريمة من كلا الطرفين لا يتطلب أو لا يستلزم كشرط مسبق في حالة التحفظ العاجل على البيانات، وذلك على أساس أن تطبيق مبدأ التجريم المزدوج يكون غير منتج في مواد التحفظ، بداية من وجهة نظر عملية معاصرة للمساعدة المتبادلة، يمكن القول بوجود اتجاه يستبعد قاعدة التجريم المزدوج بالنسبة لكل الوسائل الإجرائية ما عدا الأكثر تطفلا أو تدخلا في الحياة

[1] – راجع باللغة الأنجليزية مسودة المذكرة التفسيرية إتفاقية بودابست ستراسبورج 14 فبراير 2001.
Draft explantary memorandum to the draft convention on Cybercrime », Strasbourg 14 February 2001.

[2] – راجع المسودات التالية:
Counil of europe draft Convention on Cyber-Crime, October 2, 2000.
Counil of europe draft Convention on Cyber-Crime, November 26, 2000.
Counil of europe draft Convention on Cyber-Crime, Décembre 25, 2000.

الخاصة، كالتفتيش والضبط والتنصت، وكما يرى واضعو الاتفاقية، فإن التحفظ على البيانات لا يعد في هذا الخصوص من قبيل التطفل أو التدخل في الحياة الخاصة[1].

أن كل ما يفعله الحارس على البيانات أو القائم عليها هو المحافظة على هذه البيانات بأن تبقى في حيازته بشكل قانوني وأن يتم كشفها وفحصها من قبل مسؤولي الطرف المقدم للطلب، إلا بعد تنفيذ طلب المساعدة المتبادلة الرسمي والذي يهدف إلى كشف سرية هذه البيانات[2].

كذلك –ومن وجهة نظر عملية أيضا– فغالبا ما يستغرق التأكد من وجود مبدأ التجريم المزدوج فترة زمنية طويلة للحصول على التوضيحات اللازمة لإثبات وجود هذا المبدأ بشكل قاطع لا يقبل العكس.

وهكذا، على سبيل المثال في المراحل الأولى للتحقيق، فإن الطرف الملتمس يمكن أن يكون على دراية أنه قد تم اقتحام حاسب على أرضه، ولكن يمكن أيضا أن لا يكون باستطاعته فهم طبيعة ومدى الأضرار التي لحقت به، ومن هذا المنظور إذا كان الطرف المقدم إليه الطلب – سيقوم على سبيل المثال– بتأجيل التحفظ العاجل على بيانات المرور التي سوف تتبع مصدر الاقتحام في انتظار الإثبات الحاسم لوجود مبدأ التجريم المزدوج، فإن البيانات الهامة سوف يتم محوها بشكل آلي بواسطة موردي أو مزودي الخدمات الذي يحتفظون بها فقط لعدة ساعات أو أيام بعد عملية الإرسال، ولذلك فإنه حتى يفرض أن استطاع الطرف المقدم للطلب إثبات مبدأ التجريم المزدوج فيما بعد، فإنه لن يكون في مقدوره استعادة بيانات المرور وبالتالي لا يمكن تحديد هوية مرتكب الجريمة على وجه الإطلاق.

وتأسيسا على ما تقدم، فإنه يجب على الأطراف –كقاعدة عامة– تجنب مبدأ التجريم المشترك فيما يتعلق بالتحفظ العاجل على البيانات ومع ذلك فإن الفقرة الرابعة

[1] –جميل عبد الباقي الصغير، مرجع سابق، ص 201

[2] – علي حسن الطوالبة، مرجع سابق، ص 197.

تورد استثناءا محدودا يتعلق بإمكانية التمسك بمبدأ التجريم المشترك كشرط للرد على طلب المعاونة المتبادلة، وبالتالي لكل طرف أن يحتفظ بحقه في رفض طلب التحفظ على البيانات تبعا لهذه الفقرة، في الحالات التي يكون لديه فيها سبب معقول للاعتقاد أنه في لحظة إفشاء سرية هذه البيانات فإن شرط التجريم المزدوج لم يكن قد تم الوفاء به.

بيد أن نطاق هذا الاستثناء محدود بجرائم

غير تلك الواردة في المواد من 2-11 هذه الاتفاقية إذ بالنسبة لهذه الجرائم التي تم ذكرها في المواد 2-11 يفترض أن شرط التجريم المزدوج قد تم استيفائه بطريقة آلية بين الطرفين.

ومن ناحية أخرى، فإنه وفقا للفقرة الخامسة بمقدور الطرف المقدم إليه الطلب أن يرفض فقط طلب التحفظ العاجل على البيانات إذا كان في تنفيذ هذا الطلب الأضرار بسيادته، أو آمنه، أو نظامه العام أو أية مصالح أخرى جوهرية، وكذلك إذا كان الطلب يتعلق بجريمة سياسية، أو جريمة تتصل بجريمة ذات طبيعة سياسية، وفي غير هذه الأسباب لا يحق لأي طرف التذرع بأسباب أخرى لرفض طلب تحفظ[1].

قد يحدث في بعض الأحيان، أن يدرك الطرف المقدم إليه طلب، أن حارس البيانات أو القائم على البيانات قد يخاطر بالتدخل بطريقة قد تهدد سرية تنقيبات أو تحقيقات الطرف الملتمس أو بأية طريقة كانت، على سبيل المثال إذا كانت البيانات المراد حفظ عليها تحت حراسة مزود خدمات يأتمر بأمر منظمة جنائية أو بواسطة الشخص المستهدف من التحقيقات ذاته، في مثل هذه الحالات، فإنه بمقتضى الفقرة السادسة فإن الطرف الملتمس لابد أن يتم إخطاره على وجه السرعة، حتى يمكنه تقدير ما

[1]- look at the council of europe's cyber –crmé convention and the need for International Regime to fight cyber crime-information- systems security- nov/ des 2002-vol 11 issue 55.

إذا كان عليه أن يقوم بتنفيذ طلب التحفظ، أم أنه يبحث عن شكل آخر من أشكال المساعدة يكون أكثر تدخلا ولكن أكثر أمنا كالتفتيش والمصادرة[1].

وأخيرا، فإن الفقرة السابعة تلزم كل طرف بضمان أن البيانات المعنية يتم التحفظ عليها وفقا لهاته المادة أن تظل متحفظا عليها لمدة لا تقل عن 60 يوما، في انتظار تلقي طلب المساعدة المتبادلة الرسمي الذي يطلب بمقتضاه كشف سرية هذه البيانات وتستمر عملية التحفظ على البيانات حتى بعد استلام طلب المعاونة المتبادلة، وذلك حتى يتم الفصل في شأنه.

ثانيا: الكشف المعجل على حركة البيانات محل التحفظ :

من خلال هذا الجزء من البحث سوف نستعرض نص المادة 30 و من ثم نتناول التعليقات عليها .

أ- نص المادة 30 المتعلقة بالإفشاء العاجل لسرية بيانات المرور المتحفظ عليها[2]:

1-إذا اكتشف الطرف المقدم إليه الطلب، أثناء تنفيذ طلب مقدم تطبيقا للمادة 29 للتحفظ على بيانات المرور المتعلقة باتصال معين، أن مزود خدمة في دولة أخرى ساهم في نقل الاتصال فإنه يجب عليه، أن يقوم بالإفشاء الفوري عن قدر كاف من البيانات المتعلقة بالمرور للطرف الملتمس، بغية التعرف على هذا المزود للخدمة وعلى المسار الذي تم عبره هذا الاتصال.

2-الإفشاء العاجل لسرية بيانات المرور تطبيقا للفقرة الأولى يمكن أن يتم رفضه فقط:

أ. إذا كان الطلب ينصب على جريمة يعتبرها الطرف المقدم إليه الطلب ذات طبيعة سياسية، أو جريمة تتصل بجريمة سياسية.

[1] -هلالي عبد الله أحمد، المواجهة الجنائية المعلوماتية في النظامين المصلاري والبحريني على ضوء اتفاقية بودابست، مراجع سابق، ص 283.

[2] - إتفاقية بودابست، بشأن مكافحة الجرائم الإلكترونية، 2001/11/23

ب. إذا كان الطرف المقدم إليه الطلب يعتبر أن تنفيذ هذا الطلب من شأنه المساس بسيادته أو أمنه، أو نظامه العام، أو أي مصالح جوهرية أخرى.

ب – التعليقات :

هذه المادة تنشئ مستوى دولي من السلطات يعادل السلطات التي أنشئت على المستوى القومي وفقا للمادة.

غالبا ما يقوم الطرف المقدم إليه الطلب بالتحفظ على بيانات المرور المتعلقة بنقل الاتصال بواسطة مزودي الخدمة بفرض تتبع مصدر الاتصال وتحديد هوية فاعل الجريمة أو تجميع الأدلة القاطعة[1].

...أنه قد يكتشف أثناء ذلك أن بيانات المرور التي وجدت في إقليمه تشير إلى أن الاتصال قد تم إرساله بواسطة مزود خدمات في دولة ما، أو حتى بواسطة مزود خدمة يتواجد على أراضي الطرف الملتمس ذاته، في مثل هذه الحالات يجب على الطرف المقدم إليه طلب أن يعد بشكل عاجل للطرف الملتمس قدر كاف من البيانات المتعلقة بالمرور من أجل تمكينه من التعرف على هوية مورد الخدمات في هذه الدولة الثالثة والطريق الذي بمقتضاه تم نقل الاتصال[2].

كذلك إذا كان الاتصال قد تم نقله عبر دولة ثالثة، فإن هذه المعلومات تسمح للطرف الملتمس، أن يصدر لهذه الدولة طلب تحفظ من خلال المساعدة المتبادلة العاجلة لتلك الدولة الأخرى كي تتبع المصدر الحقيقي للاتصال.

وإذا كان الاتصال قد تم نقله إلى الطرف الملتمس، فسيكون بدوره التحفظ وإنشاء البيانات الجديدة المتعلقة بالمرور عن طريق إتخاذ الإجراءات المحلية أو القومية.

---

[1] – راجع باللغة الفرنسية المذكرة التفسيرية لإتفاقية بودابست 7 نوفمبر 2001.

Convention sur la cybercriminalité « STEno-185, Rapportexplicatif adopté le 8 novembre 2001, pp 80-83

[2] – راجع باللغة الأنجليزية مسودة المذكرة التفسيرية إتفاقية بودابست ستراسبورج 14 فبراير 2001.

Draft explantary memorandum to the draft convention on Cybercrime », Strasbourg 14 February 2001.

وبمقتضى الفقرة الثانية، فإن الطرف المقدم إليه الطلب لا يمكن رفض الإفشاء العاجل أو الفوري للبيانات المتعلقة بالمرور إلا إذا كان هذا الطرف أن من شأن هذا الإفشاء أن يحدث ضررا بسيادته، أو نظامه العام، أو أية مصلحة أخرى من مصالحه الأساسية ذلك إذا اعتبر هذا الطرف أن الجريمة المقدم بخصوصها الطلب جريمة سياسية، أو أنها تتصل بجريمة سياسية، وكما هو الحال في المادة 29 فإنه في غير هذه الأسباب لا يحق لأي طرف التذرع بأسباب أخرى لرفض طلب الإفشاء العاجل لسرية بيانات المرور[1].

الفرع الثاني : المساعدة القضائية المتبادلة في مجال سلطات التحقيق :

سنتناول في هذا الفرع4 مواد على التوالي هي المادة 31 بشأن المساعدة المتبادلة المتعلقة بالولوج إلى البيانات المعلوماتية المخزنة في إقليم دولة أخرى، والمادة 32 بشأن الوصول عبر الحدود إلى البيانات المعلوماتية المخزنة على إقليم دولة أخرى بتصريح أو من خلال إتاحتها للجمهور، والمادة 33 بشأن المساعدة المتبادلة بخصوص جمع بيانات المرور في الوقت الفعلي والتي تكون مرتبطة باتصالات معينة على أرض الغير و المادة 34 بشان المساعدة المتبادلة استنادا إلى مراقبة محتوى البيانات وذلك على النحو الآتي:

أولا : المساعدة المتبادلة استنادا إلى الدخول على البيانات المخزنة في الحاسوب :

من خلال هذا الجزء من البحث سوف نستعرض نص المادة 31 و من ثم نتناول التعليقات عليها .

أ– نص المادة 31 الخاصة بالمساعدة المتبادلة المتعلقة بالولوج إلى البيانات المعلوماتية المخزنة[2]:

---

[1] – راجع المسودات التالية:

Counil of europe draft Convention on Cyber-Crime, October 2, 2000.
Counil of europe draft Convention on Cyber-Crime, November 26, 2000.
Counil of europe draft Convention on Cyber-Crime, Décembre 25, 2000.

[2] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية , مرجع سابق .

1. بمقدور كل طرف أن يطلب من الطرف الآخر أن يفتش أو أن يقوم بالولوج إلى البيانات المعلوماتية المخزنة في نظام معلوماتي يتواجد على أرض هذا الطرف الآخر، لضبطها أو الحصول عليها أو الكشف عنها، بما في ذلك البيانات التي تم التحفظ عليها تبعا للمادة 30.
2. يجب على الطرف المقدم إليه الطلب أن يستجيب لهذا الطلب من خلال تطبيق المعاهدات الدولية والاتفاقيات والتشريعات المشار إليها في المادة 23، وعلى نحو يتوافق مع البنود الأخرى المتصلة بذلك في هذا الفصل.
3. يجب الاستجابة أيضا للطلب على وجه السرعة الممكنة في الحالات التالية:

أ. إذا كانت هناك أسباب تدعو إلى الاعتقاد أن البيانات المعينة معرضة لمخاطر الفقد أو التعديل.

ب. إذا كانت المعاهدات، أو الاتفاقيات، أو التشريعات المشار إليها في الفقرة الثانية تنص على التعاون الفوري.

ب – التعليقات :

يجب على كل أن تكون لديه المقدرة على القيام بالتفتيش والولوج إلى البيانات المعلوماتية المخزنة في نظام معلوماتي داخل النطاق الإقليمي، لمصلحة الطرف الآخر، تماما مثلما هو الحال في المادة 19 المتعلقة بتفتيش وضبط البيانات المعلوماتية المخزنة والتي بمقتضاها أن يكون لديه المقدرة على القيام بذلك لأغراض محلية, فالفقرة 1 تصرح لكل طرف أن يطلب هذا النوع من المساعدة المتبادلة، والفقرة 2 تتطلب من الطرف المقدم إليه هذا الطلب أن يكون لديه المقدرة على تلبيته[1].

[1] – هلالي عبد الله أحمد، المواجهة الجنائية المعلوماتية في النظامين المصلاري والبحريني على ضوء اتفاقية بودابست، مراجع سابق، ص 288.

ومن ناحية أخرى، فإن الفقرة 2 تتبع المبدأ القائل إن الشروط التي يتم من خلالها هذا التعاون يجب أن تكون تلك التي تقررها المعاهدات والاتفاقيات والتشريعات الوطنية المطبقة والخاصة بالمساعدة المتبادلة في المولد الجنائية[1].

وبمقتضى الفقرة 3 من هذه المادة فإنه يجب الرد على مثل هذا الطلب بصفة عاجلة في حالتين: الأولى إذا كان هناك اعتقاد بأن البيانات المتعلقة بالقضية محل البحث يمكن أن يتم ضياعها أو تعديلها، والحالة الثانية إذا كانت المعاهدات والاتفاقيات والتشريعات تقرر هذا التعاون العاجل أو الفوري.

ثانيا: الدخول العابر للحدود إلى البيانات المخزنة في الحاسوب بالرضا أو عندما تكون معروضة للجمهور:

من خلال هذا الجزء من البحث سوف نستعرض نص المادة 32 و من ثم نتناول التعليقات عليها .

أ – نص المادة 32 المتعلقة بالوصول عبر الحدود إلى البيانات المعلوماتية المخزنة بتصريح أو من خلال إتاحتها للجمهور[2]:

يمكن لأي طرف دون تصريح من الطرف الآخر:

أ. أن يصل إلى البيانات المعلوماتية المخزنة والمتاحة للجمهور (مصدر مفتوح) بغض النظر عن موقعها الجغرافي، أو.

ب. أن يصل، أو أن يتلقى عبر نظام معلوماتي يقع على إقليمه، بيانات معلوماتية مخزنة في دولة أخرى، إذا حصل هذا الطرف على موافقة قانونية وإرادية من شخص لديه سلطة قانونية للكشف عن هذه البيانات إلى هذا الطرف من خلال هذا النظام المعلوماتي.

[1] – هلالي عبد الله أحمد، نفس المرجع ، ص 288.

[2] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية , مرجع سابق .

ب – التعليقات:

السؤال حول معرفة كتى يكون مسموحا لأي طرف أن يدخل أو يلج بشكل فردي بيانات معلوماتية مخزنة على أرض طرف آخر مسبق أن تمت مناقشته بشكل مطول من قبل واضعوا هذه الاتفاقية.

لقد تواصلوا من خلال مراجعتهم للحلول المختلفة إلى تحديد الحالات التي يمكن أن يقبل فيها الولوج بشكل فردي، وتلك التي لا يجوز أن يكون مقبولة.

والواقع، أن هذه النتيجة التي توصلوا إليها مرت بمخاض عسير، وذلك لأن واضعوا هذه الاتفاقية وجدوا أنه ليس من الممكن خلق أو صياغة نظام قانوني عالمي ملزم يمكن تطبيقه في هذا المجال، ويعزى هذا على وجه الخصوص إلى نقص الخبرة العملية مثال هذه الحالات أو المواقف حتى الآن، هذا بالإضافة إلى أن الحل مثل يعتمد –في غالب الأحيان– على الظروف الخاصة بكل حالة على حدة، ولذا يصبح من الصعب صياغة أو وضع قواعد تخص هذا المضمار[1].

وفي النهاية خلص واضعوا هذه الاتفاقية إلى أنه لا يوضع في المادة 32 إلا الحالات التي اتفق الجميع على أن الولوج بشكل فردي مسموحا بخصوصها.

ومن هذا المنظور تنص المادة 32 على نوعين من الحالات:

عندما تكون البيانات المعلوماتية التي تم الوصول إليها متاحة ,والنوع الثاني عندما يتم الوصول إلى هذه البيانات المخزنة خارج النطاق الإقليمي لطرف معين أو تلقيها من خلال نظام معلوماتي يقع على إقليمه، بناء على موافقة قانونية إرادية من شخص يملك سلطة قانونية للكشف عنها[2].

[1] – هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عيها، مرجع سابق، ص 212.

[2] – هلالي عبد الله أحمد، المواجهة الجنائية المعلوماتية في النظامين المصلاري والبحريني على ضوء اتفاقية بودابست، مراجع سابق، ص 288.

والسؤال الذي يرد بعد هذا الذي تقدم من هو هذا الشخص الذي يملك سلطة قانونية للكشف عن هذه البيانات المعلوماتية؟ للإجابة على هذا السؤال نقول إن طبيعة هذا الشخص تتنوع بتنوع الظروف والحالات.

فعلي سبيل المثال بالنسبة لحالة البريد الإلكتروني لأحد الأشخاص، يمكن أن يتم تخزينه في دولة أخرى عن كريق مورد أو مزود خدمات، كما يمكن لشخص ما أن يقوم بتخزين البيانات الخاصة به عمدا في إقليم دولة أخرى، في مثل هذه الحالات بمقدور هؤلاء الأشخاص استعادة هذه البيانات شريطة أن يكون لديهم سلطة قانونية للقيام بهذا الإجراء، كما يمكن بمقدورهم أيضا أن يقوموا بالكشف عن هذه البيانات، بمحض إرادتهم للسلطات المكلفة بتنفيذ القانون أو أن يسمحوا لهذه السلطات بالولوج أو بالدخول إلى هذه البيانات.

ثالثا: المساعدة المتبادلة استنادا إلى تجميع حركة البيانات في الزمن الفعلي:

من خلال هذا الجزء من البحث سوف نستعرض نص المادة 33 ومن ثم نتناول التعليقات عليها.

أ – نص المادة 33 المتعلقة بالمساعدة المتبادلة بخصوص جمع بيانات المرور في الوقت الفعلي[1]:

1-يجب على الأطراف أن تقدم المساعدة المتبادلة إلى بعضها البعض بالنسبة لجمع بيانات المرور في الوقت الفعلي، والتي تكون مرتبطة باتصالات معينة على أرضهم، ومرسلة عن طريق نظام معلوماتي، ووفقا للأوضاع المنصوص عليها في الفقرة 2 فإن هذه المساعدة، سوف تحكمها الشروط والإجراءات المنصوص عليها في القانون الداخلي.

[1] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية، 2001/11/23

2-يجب على كل طرف أن يقدم هذه المساعدة على الأقل فيما يتعلق بالجرائم الجنائية من حيث جميع بيانات المرور في الوقت الفعلي التي يمكن أن تكون متاحة في قضية موازية على المستوى الداخلي.

ب: التعليقات:

في حالات كثيرة قد لا يكون بمقدور المحققين ضمان تتبع خط سير الاتصال للوصول إلى مصدره بإتباع أثره من خلال التسجيلات الخاصة برسائل سابقة، وذلك لقيام مورد الخدمات بحذف بيانات المرور بشكل آلي من سلسلة الاتصال التي تمر بها عملية نقل الرسالة، ولذا بات من الضروري بالنسبة للمحققين لدى كل طرف أن لديهم القدرة على الحصول على بيانات المرور خلال الوقت بالنسبة للاتصالات التي تمر عبر نظام معلوماتي لدى أطراف أخرى[1].

وكنتيجة لذلك، فإنه بمقتضى المادة 33 يكون كل طرف ملزما بالتجميع في الوقت الفعلي للبيانات المتعلقة بالمرور من أجل الطرف الآخر.

وإذا كانت هذه المادة تلزم الأطراف بالتعاون في هذا النطاق، ولكن كما في الأوضاع الأخرى، لابد أن يؤخذ في الاعتبار نماذج المساعدة الجارية أو الممول بها، فالقيود والشروط المتعلقة بهذا التعاون تقررها بصفة عامة المعاهدات والاتفاقيات والتشريعات المطبقة في تنظيمها للمساعدة القضائية المتبادلة في المسائل الجنائية[2].

في العديد من الدول، يتم توفير المساعدة المتبادلة لأمر جوهري يتعلق بالتجميع في الوقت الفعلي للبيانات الخاصة بالمرور، لأن هذا التجميع يكون أقل تطفلا أو تدخلا من اعتراض بيانات المحتوى أو التفتيش أو الضبط.

---

[1] – راجع باللغة الفرنسية المذكرة التفسيرية لإتفاقية بودابست 7 نوفمبر 2001.

Convention sur la cybercriminalité « STEno-185, Rapportexplicatif adopté le 8 novembre 2001, pp 80-83

[2] – راجع باللغة الأنجليزية مسودة المذكرة التفسيرية إتفاقية بودابست ستراسبورج 14 فبراير 2001.

Draft explantary memorandum to the draft convention on Cybercrime », Strasbourg 14 February 2001

والواقع أنه لما كان التجميع في الوقت الفعلي للبيانات المتعلقة بالمرور قد يكون أحيانا الطريقة الوحيدة لتجديد هوية مرتكب الجريمة، ولما كان هذا الإجراء ذي طبيعة أقل تدخلا أو تطفلا، فإن الفقرة 2 استخدمت مصطلح "على الأقل" لتشجيع الأطراف على السماح بأوسع نطاق ممكن للمساعدة المتبادلة بهذا الخصوص، حتى في ظل غياب مبدأ التجريم المزدوج[1].

رابعا: المساعدة المتبادلة استنادا إلى مراقبة محتوى البيانات :

من خلال هذا الجزء من البحث سوف نستعرض نص المادة 34 و من ثم نتناول التعليقات عليها .

أ – نص المادة 34: الخاص بالمساعدة المتبادلة في مسألة اعتراض بيانات المحتوى[2]:

يجب على الأطراف تقديم المساعدة المتبادلة لبعضها البعض، إلى المدى المسموح به في معاهداتهم وقوانينهم الداخلية المطبقة، فيما يتصل بجمع أو تسجيل بيانات المحتوى في الوقت الفعلي للاتصالات الجارية عبر نظام معلوماتي.

بـ – التعليقات :

نظرا للطابع الأكثر تطفلا أو تدخلا لعملية اعتراض بيانات المحتوى فقد تم تحديد الالتزام بتوفير المساعدة المتبادلة المتعلقة بهذا الخصوص إذ يجب أن يكون تقديم المساعدة المتبادلة في الحدود تسمح بها المعاهدات والقوانين الداخلية المطبقة للأطراف.

أن التطبيق العملي للمساعدة المتبادلة المتعلقة باعتراض بيانات المحتوى له تداعياته، فقد تم اتخاذ قرار بخصوص هذا الإجراء، وذلك بأن يتم تنظيمه وفقا للقوانين

---

[1] – راجع المسودات التالية:

Counil of europe draft Convention on Cyber-Crime, October 2, 2000.
Counil of europe draft Convention on Cyber-Crime, November 26, 2000.
Counil of europe draft Convention on Cyber-Crime, Décembre 25, 2000

[2] – إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية , مرجع سابق .

الداخلية المعمول بها من حيث مدى التزام بتقديم هذا النوع من المساعدة والقيود التي ترد عليها[1].

[1] – هلالي عبد الله أحمد، المواجهة الجنائية المعلوماتية في النظامين المصلاري والبحريني على ضوء اتفاقية بودابست، مراجع سابق، ص 295، 296.

خلاصة الفصل الأول:

فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالإنترنت غالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة. ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها. وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه. وعندما يكون مقدموا الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى. بمعنى الحاجة إلى ما يسمي التعاون القضائي وهو ما عمدنا الى توصيفه في الفصل الأول من خلال بياننا لإجراءات المساعدة القضائية المتبادلة في المسائل الجنائية لمكافحة الجريمة الإلكترونية وبيان مجالاتها في المبحث الثاني منه بعد أن عرجنا على مفهوم الجريمة الإلكترونية وبيان المبادئ العامة التي تحكم المساعدة القضائية فيها في المبحث الأول منه.

الفصل الثاني:

الجانب الموضوعي للإنابة القضائية والوسائل المستحدثة للتعاون الدولي في مكافحة الجريمة الإلكترونية

المبحث الأول : الإطار الموضوعي للإنابة القضائية.

المبحث الثاني: الوسائل المستحدثة للتعاون الدولي لمكافحة الجريمة الإلكترونية.

باعتبار المساعدة القضائية وسيلةً من وسائل التعاون القضائي الدولي فإنها قد اكتسبت أهميةً كبيرةً وذلك من حيث كونها تعمل على تذليل الصعوبات والعراقيل التي تواجه القائمين بالتحريات والتحقيقات وجمع الأدلة اللازمة لإدانة مرتكبي الجريمة المنظمة عبر الوطنية، وتكتسب المساعدة القضائية المتبادلة أهميةً بالغةً في ظل الجهود الدولية الساعية إلى تدويل الجريمة وربط أطراف العالم بالمعاهدات، كما أن لها دوراً كبيراً في التقارب والتجانس في الأفكار والجهود بما يخدم أعضاء المجتمع الدولي، فضلاً عن أنها تقف حائلاً أمام المجرمين ووسائلهم المتطورة للإفلات من العقاب، فتبادل المساعدة القضائية بين الدول يشكل أمراً هاماً في التصدي لهذه الجريمة بشتي صورها.

وقد اعتُبر تنفيذ الالتزامات المترتّبة على المعاهدات وتوافر القدرات الوطنية والإرادة السياسية للدول الأطراف مقوّمات أساسية لتيسير التعاون الدولي.

فقد حرص المجتمع الدولي على تيسير التعاون الدولي في المسائل الجنائية في مجال مكافحة الجرائم الإلكترونية ، ووضع برامج العمل الازمة لتطبيق المبادئ اساسية لجدول أعمال القرن 21.

وعليه كان لابد من خلق نظم جدية وإستحداث تقنيات تكنلوجية تواكب النمط التكنولوجي المكون لانشطة الجريمة الإلكترونية ومن هذه التقنيات نجد ابرزها تقنية الـ videoconference التي أضحى إستخدامها يشكل مرحلة جديدة من مراحل تطور الإجراءات الجنائية، بشكل يعكس الرغبة في الاستفادة من المعطيات التكنولوجية الحديثة في مجالات تطوير مرافق العدالة الجنائية.

وعليه فإننا خصصنا هذا الفصل لدراسة **الإطار الموضوعي للإنابة القضائية** في **المبحث الأول** في حين تناولنا في **المبحث الثاني الوسائل المستحدثة للتعاون الدولي لمكافحة الجريمة الإلكترونية.**

المبحث الأول : الإطار الموضوعي للإنابة القضائية:

تعد الإنابات القضائية الدولية صورة من أهم صور التعاون الدولي في مكافحة الجريمة، والتي تتم على المستوى القضائي دون التشريعي بين الدول، على اعتبار أنها تعاون بين الأجهزة القضائية المختلفة للدول[1].

فالأصل أن تتولى المحكمة المرفوعة إليها الدعوى دراستها والتحقيق بشأنها توصلا لإصدار الحكم فيها، ولكنه قد تنشأ في بعض الأحيان موانع أو عقبات تحول دون قيامها بالتحقيق اللازم وباستقصاء الأدلة في صدد تلك الدعوى، إما بسبب عدم وجود الشهود المطلوب استماعهم أو الشيء المطلوب معاينته أو التحقيق بشأنه، وفي هذه الحالة يمكن للمحكمة القيام بانتداب محكمة أخرى أو قاضٍ آخر للقيام بالإجراءات اللازمة بدلا عنها[2].

وبالقياس على النيابة التي تتم بين الأفراد في إطار علاقات القانون الخاص، ولإعتبارات التعاون الدولي في مكافحة الجريمة وعدم قدرة الدولة منفردة على مكافحة الجرائم العابرة للحدود، فقد اتجهت الدول فيما بينها إلى إمكانية أن ينيب بعضها بعضا في اتخاذ بعض الإجراءات الجنائية على أرضها ولكن لمصلحة دولة أخرى[3]

فالإنابة القضائية الدولية في المسائل الجنائية أهمية بالغة في تعزيز التعاون القضائي بين السلطات القضائية للدول، وبالتالي تكتسب أهمية بالغة في مجال التعاون الدولي في مكافحة الإجرام لذلك سنلقي الضوء على دور الإنابات القضائية الدولية في التعاون الدولي في مكافحة جرائم الإرهاب، وذلك من خلال المطلبين التاليين:

---

[1] – عكاشة محمد عبد العال، الإنابات القضائية في العلاقات الخاصة الدولية، دار المطبوعات الجامعية، الإسكندرية، 1994 ، ص8.

[2] – إدوارد عيد، الإنابات والإعلانات القضائية، وفقًا للقانون الدولي الخاص واتفاقية الدول العربية في عام 1953 ، معهد البحوث والدراسات العربية، 1969 ، ص 9

[3] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دار النهضة العربية، الطبعة الأولى، 2001، ص2.

المطلب الأول :الإطار المفاهيمي للإنابات القضائية الدولي في المسائل الجنائية

المطلب الثاني :دور الإنابات القضائية الدولية في التعاون الدولي لمكافحة الجرائم الإلكترونية

المطلب الأول: الإطار المفاهيمي للإنابة القضائية الدولية في المسائل الجنائية

سنوضح في هذا المطلب تعريف الإنابات القضائية الدولية في المسائل الجنائية وشروط تطبيقها، كما يلي:

الفرع الأول :تعريف الإنابة القضائية الدولية وأساسها القانوني

الفرع الثاني :شروط تطبيق الإنابة القضائية الدولية في المسائل الجنائية

الفرع الأول :تعريف الإنابة القضائية وأساسها القانوني :

أولا :تعريف الإنابة القضائية الدولية في المسائل الجنائية:

الإنابة القضائية بشكل عام هي" :عمل بمقتضاه تفوض المحكمة أو القاضي (محكمة أخرى) أو قاضيًا آخر (للقيام مكانها، وفي دائرة اختصاصها، بأحد أو بعض إجراءات التحقيق أو الإجراءات القضائية الأخرى التي يقتضيها فصل الدعاوي المرفوعة أمامها، والتي تعذر عليها مباشرتها بنفسها بسبب بعد المسافة أو أي مانع آخر[1]

[1]- Pengelley, Pamela D. , A Compelling Situation: Enforcing American Letters Rogatory in Ontario. Canadian Bar Review, 2006. Vol. 85, No. 2, p. 346.

أيضا: أدوار عيد، الإنابات والإعلانات القضائية، مرجع سابق، ص 9.

كما تُعرف بأنها" :طلب من السلطة القضائية المنيبة إلى السلطة المنابة قضائية كانت أو دبلوماسية – أساسه التبادل، ومفاده اتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة في الخارج وكذلك أي إجراء قضائي آخر يلزم اتخاذه، للفصل في المسألة المثارة أو المحتمل إثارتها في المستقبل، أمام القاضي المنيب، الذي ليس بمقدوره القيام به في دائرة اختصاصه[1]

فالإنابة القضائية الدولية تفترض علاقة بين دولتين وتحديداً بين سلطتين قضائيتين متماثلتين في الاختصاص من دولتين مستقلتين، ويتم نقل طلب الإنابة إما بالطرق الدبلوماسية أو بالطريق القضائي المباشر[2]، وذلك وفقًا للأوضاع التي تحددها غالبًا نصوص معاهدة أو اتفاقية بين دولتين أو مجموعة دول أو ما يحدده القانون الوطني إذا وجدت نصوص تنظم مسائل الإنابات القضائية الدولية.

والإنابات القضائية الدولية في المسائل الجنائية تفترض موضوعًا تنصب عليه يتمثل في اتخاذ إجراء من إجراءات التحقيق الابتدائي أو النهائي، فقد يكون طلب معاينة

[1] – عكاشة محمد عبد العال، الإنابة القضائية في نطاق العلاقات الخاصة الد ولية، مرجع سابق، ص 16.
وتسمى الإنابة أيضًا بالتفويض الالتماسي، أي أن توجه محكمة محلية إلى أخرى في بلد أجنبي التماساً مكتوباً، راجية منها أن تأخذ بمعرفتها شهادة شاهد مقيم في دائرة اختصاصها حول مسألة معينة، وأن ترسل إليها تلك الشهادة لتستعين بها في الدعوى المنظورة أمامها، معربة عن استعدادها لتقديم أي مساعدة مماثلة تطالب فيها في المستقبل. انظر: د. حازم مختار الحاروني، نطاق تطبيق القاضي الجنائي للقانون الأجنبي، رسالة دكتوراه، جامعة القاهرة، 1987 ، ص 513.

[2] – تجدر الإشارة هنا إلى أنه لا يجب الخلط بين الإنابة القضائية الصادرة بواسطة السلطات القضائية للدولة مع تلك التي تم تتم عن طريق أعضاء السلك الدبلوماسي أو القنصلي بهدف سماع شهادة أحد رعاياها في واقعة معينة، حيث إن تلك الإجراءات التي تحدث بمعرفة الهيئات الدبلوماسية لا تخضع للأحكام الخاصة بالإنابة القضائية الدولية، ما لم ينص صراحة على ذلك في اتفاقية بين دولتين أو بين مجموعة دول، إذ أن أعضاء البعثة الدبلوماسية لا يحق لهم بمباشرة إجراء من إجراءات التحقيق على أرض دولة أخرى، كما أنهم لا يعتبرون أجانب بالنسبة للدولة التي يمثلونها في الخارج. للتفصيل أكثر انظر: د. عمر سالم، الإنابة القضائية الدولية في المواد الجنائية، مرجع سابق، ص 34.

أو ندب الخبراء أو سماع الشهود أو التفتيش أو الاستجواب أو القبض، كما يمكن أن يكون موضوعها الاضطلاع على الأوراق والملفات والمستندات الموجودة في دولة أجنبية[1]

مما يعني أن الإنابات القضائية بهذا المعنى ليست إنابات في تنفيذ الحكم، كما لا يمكن اعتبارها إجراء من إجراءات الاستدلال[2]

وقد تطرقت اتفاقية التعاون القضائي الموقعة بين الدول العربية في عام 1983 ، إلى موضوع الإنابة القضائية عندما نصت على أنه "لكل من الدول المرتبطة بهذه الاتفاقية أن تطلب إلى أية دولة منها أن تباشر في أرضها نيابة عنها أي إجراء قضائي يتعلق بدعوى قيد النظر[3]...

وتتناول الإنابة استماع الشهود المقيمين في البلد المناب أو تحلفيهم اليمين أو تعيين خبير أو تدقيق مستندات، ولكن لا يجوز أن تتضمن الإنابة أعمالا تنفيذية، كتنفيذ الأحكام الأجنبية، لأن ذلك سيتعدى نطاق الإجراءات المتعلقة بدعوى لم تزل قيد النظر أمام المحكمة المنيبة، فلا يمكن أن يشمل إذا إجراءات التنفيذ التي تخرج عن نطاق سير الدعوى[4] وإذا كان موضوع الإنابة يعتبر من إجراءات التحقيق، فإن إجراءات الإنابة القضائية

---

[1] – د. عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقاً لمعطيات التكنولوجيا المعاصرة، رسالة دكتوراه جامعة القاهرة، ص 252–253.

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 15.

-HUET (A) , et KORING - JOULIN Renee, droit penal international, 1993 no ,213p. 328

وقد حددت المادة الثالثة من الباب الثاني من الاتفاقية الأوربية للمساعدة القضائية في المسائل الجنائية موضوع الثاني من الاتفاقية الأوروبية للمساعدة القضائية في المسائل الجنائية موضوع الإنابة القضائية عندما تحدثت عن إجراءات التحقيق، والاطلاع على الأوراق والمستندات بصفة مطلقة، كما تحدثه القوة الثانية من ذات المادة على إمكانية الدولة أن تطلب سماع الشهود أو الخبراء بعد أداء القسم أو اليمين.

[3] – المادة السادسة من اتفاقية الرياض للتعاون القضائي بين الدول العربية.

[4] – عكاشة محمد عبد العال، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، مرجع سابق، ص 58.

بذاتها ليست من إجراءات التحقيق، وإنما هي طلب تقدمه جهة قضائية إلي جهة قضائية أخرى في دولة أجنبية، باتخاذ إجراءات قضائية من إجراءات التحقيق[1].

ثانيا :الأساس القانوني للإنابة القضائية الدولية:

يكمن الأساس القانوني للإنابات القضائية الدولية في مصدرين أساسيين، هما:

الاتفاقيات الدولية والقوانين الوطنية.

1 -الاتفاقيات الدولية:

تمثل الاتفاقيات الدولية المتعلقة بالمساعدة القضائية بين الدول، أساساً قانونياً للإنابة القضائية[2] ، فالاتفاقية الدولية بعد التصديق عليها تصبح سارية المفعول ملزمة شأنها شأن القوانين الداخلية، حيث تتمتع بالقوة التنفيذية التي تلزم بها السلطات القضائية الوطنية عند عرض المسألة عليها[3] وفي حالة ما إذا رفضت دولة طلب المساعدة القضائية في مسألة معينة، فإنه يستوجب عليها تسبيب رفضها وإيضاح بواعثها من هذا الرفض، وعادةً ما تحتج الدول في رفضها لطلب الإنابة القضائية بمبدأ سيادة الدولة وأمنها، حيث تتضمن أغلب الاتفاقيات الدولية شرطًا أساسيًا يجعل تنفيذ الإنابة القضائية رهنًا بإرادة الدولة المنفذة، وهذا الشرط هو أن لا تنطوي هذه المساعدة على المساس بسيادة الدولة أو نطاقها أو مصالحها[4].

2- القوانين الوطنية:

تمثل القوانين الوطنية المصدر الثاني للإنابة القضائية الدولية، ويعني ذلك وجود تشريعات خاصة في القوانين الوطنية تنظم مسألة الإنابة القضائية، حيث يتم اللجوء إليها

---

[1] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 20.

– عكاشة محمد عبد العال، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، مرجع سابق، ص 18.

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع اسبق، ص 23.

[3] – حازم مختار الحاروني، نطاق تطبيق القاضي الجنائي للقانون الأجنبي، مرجع سابق، ص 520

[4] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 24.

في حال غياب اتفاقية دولية تربط بين الدولتين أو في حالة وجود هذه الاتفاقية إلا أن نصوصها تتضمن ضرورة الالتجاء إلى القوانين الوطنية بشروط معينة[1]

الفرع الثاني : شروط تطبيق الإنابة القضائية الدولية في المسائل الجنائية :

للإنابة القضائية الدولية شروط معينة ولازمة لابد من توافرها لإمكانية تنفيذها في الدولة المطلوب منها، وهذه الشروط تتشابه لا بل تكاد تتطابق إلى حد كبير مع شروط الإنابة القضائية في القانون الداخلي، ويمكن إجمالها بما يلي:

أولا – شروط الاختصاص:

يستوجب حتى تكون الإنابة القضائية الدولية صحيحة، أن يكون الفصل في الواقعة موضوع الإنابة، من اختصاص الدولة الطالبة وأن يكون هناك صلة بين هذه الدولة والقضية أو الجرم المطلوب من أجله تنفيذ الإنابة .ورغم أن هذا الاختصاص يتحدد وفق معايير يضعها قانون الدولة الطالبة، فإن الدولة المطلوب منها تنفيذ الإنابة لها أن ترفضها إذا رأت أن هذا الاختصاص غير مقبول وفقًا لقواعد القانون الدولي أو وفق المبادئ الأساسية التي تحكم تطبيق القانون الجنائي من حيث المكان، والمتمثلة في مبدأ الإقليمية، ومبدأ الشخصية، ومبدأ العينية[2]

ولا يكفي اختصاص قانون الدولة الطالبة في الواقعة موضوع الإنابة، وإنما يلزم أيضًا لقبول طلب الإنابة، أن تكون السلطة القضائية هي المختصة في الواقعة موضوع الإنابة، وبالتالي لا تقبل طلبات الإنابة إذا كانت الواقعة من اختصاص جهة إدارية في الدولة الطالبة. ففي مصر مثلا تختص كل من المحاكم والنيابة العامة في تقديم طلبات الإنابة القضائية[3].

---

[1] – نفس المرجع، ص 25.

[2] – د. عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 59.

[3] – تنص المادة (546) من مشروع قانون الإجراءات الجنائية المصري على أنه: "يجوز للمحكمة أو النيابة) العامة كل في حدود اختصاصه، طلب الإنابة القضائية في السلطة القضائية بدولة أجنبية، وترسل طلبات الإنابة إلى وزير العدل توجيها إلى السلطة الأجنبية بالطرق الدبلوماسية".

وبالمقابل من ذلك، فإنه من غير الممكن تنفيذ الإنابة القضائية في الدولة المطلوب منها إذا كان الإجراءالمطلوب لا يدخل في اختصاص الجهة التي وجه إليها الطلب، وقد أكدت اتفاقية الرياض للتعاون القضائي العربي على ذلك حيث نصت على أنه" إذا تبين عدم اختصاصها، فللجهة المطلوب إليها تنفيذ الإنابة، أن تحيل الطلب من تلقاء نفسها إلى الجهة المختصة، وإذا تعذر عليها ذلك، تحيلها إلى وزارة العدل، وتخطر فورا الجهة الطالبة بما تم في الحالتين[1] "

والحقيقة يبدو هذا الشرط منطقياً إذ من المتعذر أن يتم إجراء التحقيق الابتدائي أو النهائي في قضية معينة بواسطة سلطة لا تختص أصلا بالنظر بهذه القضايا، فهذا يؤدي إلى وجود عيب شكلي في إجراءات وسير الدعوى.

ثانيا: عدم تعارض تنفيذ الإنابة مع النظام العام:

يجب ألا يكون في تنفيذ الإنابة القضائية الدولية خرق للنظام العام في الدولة المطلوب منها التنفيذ، فإذا رأت الدولة أن هذا التنفيذ يتعارض مع نظامها العام كان لها أن ترفضه[2].

وتتجه الاتفاقيات الدولية والقوانين الوطنية إلى النص صراحة على هذا الشرط بالنسبة للدولة المطلوب منها تنفيذ الإنابة، وذلك إذا اتضح لها أن في التنفيذ مساسا بنظامها العام أو بمصالحها الجوهرية.

---

[1] – المادة (15 / أ) في اتفاقية التعاون القضائي العربي المعقودة في الرياض عام 1983.

[2] – يُعرف النظام العام بأنه: مجموعة المصالح والركائز الأساسية التي يقوم عليها المجتمع في النواحي) السياسية والاقتصادية والاجتماعية والخلقية، وفقًا لما يرسمه النظام القانوني لهذا المجتمع.

انظر: عماد طارق البشري، فكرة النظام العام في النظرية والتطبيق، المكتب الإسلامي للطباعة والنشر،2005، ص 7.

وفكرة النظام العام فكرة مرنة يختلف مداها من قانون وطني إلى آخر، حيث يعتمد على الإعتبارات واقعية أكثر منها قانونية، هذه الإعتبارات تحددها الدولة وفقًا لما تراه مناسبًا لتأمين مصالحها[1].

وقد أشارت الاتفاقية العربية لمكافحة جرائم الإرهاب إلى هذا الشرط صراحة عندما نصت على أن" تلتزم كل من الدول المتعاقد بتنفيذ الإنابات القضائية المتعلقة بالجرائم الإرهابية ويجوز لها رفض طلب التنفيذ في أي من الحالتين التاليتين(أ)..(ب): إذا كان تنفيذ الطلب من شأنه المساس بسيادة الدولة المكلفة بتنفيذه أو بأمنها أو بالنظام العام فيها[2].

كما نصت الاتفاقية الأوروبية للمساعدة القضائية لعام 1959 على هذا الشرط عندما جاء في الفقرة (ب) من مادتها الثانية على أنه يمكن رفض طلب المساعدة إذا قدرت الدولة المطلوب منها التنفيذ، أن تنفيذ الطلب من شأنه إحداث اعتداء على النظام العام أو أية مصالح أساسية أخرى[3]

أما مشروع قانون الإجراءات الجنائية المصري فقد نص أيضًا في المادة (543) على رفض تنفيذ الإنابات القضائية" إذا كانت الإجراءات المطلوبة محظورة بمقتضى القانون أو متعارضة مع مبادئ النظام العام ."كما جاء في قانون الإجراءات الجنائية الفرنسي في مادته 296-2 المضافة بالقانون 99-515 والصادر عام 1999 أنه" يجب على السلطات القضائية التي تفصل في طلب مساعدة قضائية دولية في المسائل الجنائية

[1] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 151 . أنظر أيضًا
--DUSSAIX (R.), Qvelques problemes a l' application pratique du point de vue judiciaire de la convention Eouropeene relatifs d' entvaide judiciaire en matiere penal, in (problemes relatifs a l' application pratique de la convention europeene d' entraide judiciaire en matiere penal) Conseil de Eurpe, 1971 p. 40.

[2] – ١) المادة (10/ب) في الاتفاقية العربية لمكافحة جرائم الإرهاب الم وقعة في 1998/04/22.

[3]- Assistance may be refused: b. if the requested Party considers that execution of the request is likely to prejudice the sovereignty, security, order public or other essential interests of its country

وتقدر أن تنفيذ هذا الطلب ينطوي على مساس بالأمن أو النظام العام أو مصالح أساسية أخرى للأمة، أن تتخذ الإجراءات الضرورية الواجب اتخاذها في هذا الطلب[1].

إلا أنه وعلى الرغم من أن فكرة النظام العام تخضع لتقدير الدولة المنفذة، إلا أنها في حال رفضت طلب الإنابة تلتزم ببيان سبب هذا الرفض، وهذا ما أشارت إليه الاتفاقية العربية لمكافحة جرائم الإرهاب عندما نصت على أن" كل رفض للإنابة القضائية يجب أن يكون مسبباً[2] وكذلك ذهبت المادة(19) في الاتفاقية الأوروبية للمساعدة القضائية حين نصت على أنه" :يجب تقديم السبب عند رفض طلب المساعدة[3]

ثالثا :مراعاة الشروط الشكلية:

يتوجب على السلطات القضائية، عند تقديمها لطلب الإنابة، أن تلتزم بشكل معين في الإجراءات وذلك لضمان صحتها .حيث توجه الإنابة بطلب مكتوب من السلطة القضائية بإحدى الطريقتين التاليتين:

الطريقة الأولى: يوجه طلب الإنابة من السلطة القضائية إلى وزارة العدل في بلدها، والتي تحيلها بدورها إلى وزارة الخارجية التي تتولى إرسالها بالطريق الدبلوماسي إلى وزارة الخارجية في البلد المطلوب تنفيذ الإنابة فيه، ومنها إلى وزارة العدل فإلى المحكمة المنابة[4] وغالباً ما تحصل هذه الطريقة في حالة عدم وجود اتفاق قضائي بين الدولتين، أي على سبيل المجاملة الدولية أو مبدأ المعاملة بالمثل[5] ولوزارة العدل هنا أن تقوم

---

[1]- Artecle 696 - 2: inséré par Loi n. 99 - 515 du 23 juin 1999 art. 30 Journal Officiel du 24 2 juin 1999.

-Les autorités judiciaires sollicitant un acte urgent d'entraide judiciaire en matière pénale peuvent, dans le cadre des conventions en vigueur, saisir les autorités compétentes de l'Etat requis, afin d'obtenir, dans les meilleurs délais, le retour des pièces d'exécution de l'acte sollicité.

[2] – المادة (23) من الاتفاقية العربية لمكافحة الإرهاب الموقعة في 1998/04/22.

[3]- Art 19" Reasons shall be given for any refusal of mutual assistance "

[4] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 85.

إدوار عيد، الإنابات والإعلانات القضائية، مرجع سابق، ص 22.

[5] – إدوار عيد، الإنابات والإعلانات القضائية، مرجع سابق، ص 22.

بفحص الطلب وتدقيقه قبل إرساله وتتأكد من استيفاء جميع الشروط الشكلية والموضوعية فيه[1].

الطريقة الثانية : وهي الطريقة القضائية الخالصة حيث يتم الاتصال بين السلطتين القضائيتين بشكل مباشر في الدولتين الطالبة والمطلوب فيها تنفيذ الإنابة القضائية، حيث يوجه طلب الإنابة مباشرة من المحكمة المنيبة الى المحكمة المنابة[2] وتتميز هذه الطريقة في أنها أكثر سرعة وأشد فعالية، وغالباً ما تتم عندما يكون هناك اتفاق قضائي بين الدولتين.

وقد بين قانون الإجراءات الجنائية الفرنسي من خلال المادة 694 الأسلوب الذي يتوجب إتباعه، ففي حال ما طلبت السلطات القضائية الفرنسية المساعدة القضائية فإنه يتوجب عليها تقديم الطلب عبر وزارة العدل إلى السلطة القضائية للدولة الأجنبية، أما في حال تلقت السلطات الفرنسية طلبا من دولة أجنبية فإن ذلك يتم عبر القنوات الدبلوماسية، وفي حالة الاستعجال يمكن أن تنتقل طلبات المساعدة التي تطلبها السلطات الفرنسية أو الأجنبية إلى سلطات الدولة المختصة بشكل مباشر دون اللجوء الى القنوات الدبلوماسية مالم ينص أي اتفاق دولي على خلاف ذلك[3].

---

[1] – ومن ذلك ما جاء في المادة (546) في مشروع قانون الإجراءات الجنائية المصري ".. وترسل طلبات الإنابة إلى وزير العدل لتوجيهها إلى السلطة الأجنبية بالطرق الدبلوماسية ولوزير العدل تقدير مدى ملائمة توجيه طلب الإنابة إلى السلطة الأجنبية من حيث تأثيرها على المصالح الأساسية للدولة وعلاقاتها الدولية ولصحة الإجراء الذي نفذ بناء وعلى طلب الإنابة أن يكون مستوفياً

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 82.

[3]- Article 694 - Modifié par Loi n°2004-204 du 9 mars 2004 - art. 17 JORF 10 mars 2004.
"En l'absence de convention internationale en stipulant autrement:
1-Les demandes d'entraide émanant des autorités judiciaires françaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du ministère de la justice. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie;
2- Les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires françaises sont transmises par la voie diplomatique. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie.

أما مشروع قانون الإجراءات الجنائية المصري فقد ميز أيضًا بين الظروف العادية والظروف المستعجلة، إلا أنه لم يحدد الجهة التي يتم إخطارها لاتخاذ الإجراءات التي تقتضيها حالة الضرورة أو الصفة المستعجلة[1]، حيث تقضي المادة542 من المشروع بأنه "إذا رغبت إحدى الدول الأجنبية في إجراء تحقيق بمعرفة السلطة القضائية المصرية، يقدم طلب الإنابة من السلطات المختصة في تلك الدولة بالطرق الدبلوماسية إلى وزير العدل، ويبين في الطلب الإجراءات المطلوب اتخاذها والتحقيقات المراد القيام بها وظروف الواقعة والنصوص القانونية المنطبقة عليها، ويرفق به ما يستلزمه تنفيذ الإنابة من أوراق ومستندات ولوزير العدل أن يحيل الطلب إلى الجهة القضائية المختصة لاتخاذ ما تراه بشأنه ويجوز في حالة الاستعجال بناء على طلب الدولة الطالبة الإجراءات التي تستدعيها الضرورة قبل ورود الطلب والمرفقات المشار إليها في الفقرتين السابقتين لحين ورودها."

أما على صعيد مكافحة جرائم الإرهاب، فقد جاءت الاتفاقية العربية لمكافحة جرائم الإرهاب مسايرة للأخذ بالطريقتين، حيث نصت على أن" يوجه طلب الإنابة القضائية من وزارة العدل في الدولة الطالبة، إلى وزارة العدل في الدولة المطلوب إليها، ويعاد بنفس الطريق[2] "

وفي حالة الاستعجال، يوجه طالب الإنابة القضائية مباشرة من السلطات القضائية في الدولة الطالبة، إلى السلطات القضائية في الدولة المطلوب إليها، وترسل صورة هذه

En cas d'urgence, les demandes d'entraide sollicitées par les autorités françaises ou étrangères peuvent être transmises directement aux autorités de l'Etat requis compétentes pour les exécuter. Le renvoi des pièces d'exécution
aux autorités compétentes de l'Etat requérant est effectué selon les mêmes modalités. Toutefois, sauf convention internationale en stipulant autrement, les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires françaises doivent faire l'objet d'un avis donné par la voie diplomatique par le gouvernement étranger intéressé.

[1] – عمر سالم، الإنابة القضائية في المسائل الجنائية، مرجع سابق، ص 91.

[2] – المادة (1/30) من الاتفاقية العربية لمكافحة الإرهاب.

الإنابة في نفس الوقت إلى وزارة العدل في الدولة المطلوب إليها، وتعاد الإنابة مصحوبة بالأوراق المتعلقة بتنفيذها بالطريق المنصوص عليها في البند السابق[1] كما يمكن أن يوجه طلب الإنابة القضائية مباشرة من الجهات القضائية، إلى الجهة المختصة في الدولة المطلوب إليها، ويجوز أن تحال الردود مباشرة عن طريق هذه الجهة[2]

ونلفت هنا إلى أن البند الثاني في المادة 30 من الاتفاقية العربية لمكافحة الإرهاب جعلت عودة نتيجة تنفيذ الإنابة القضائية في حالة الطالب المستعجل، عبر الطريق العادي حين نصت على أنه ..." وتعاد الإنابة القضائية مصحوبة بالأوراق المتعلقة بتنفيذها بالطريق المنصوص عليها في البند السابق ."وهذا المسلك لا يتماشى مع صفة الاستعجال الواردة فيه، بل كان من المستحسن– من وجهة نظرنا – أن يكون توجيه الطالب والعودة عن طريق الاستعجال ودون الرجوع إلى وزارة العدل.

وكذلك فعلت الاتفاقية الأوروبية للمساعدة القضائية في المسائل الجنائية حين نصت المادة15 منها على أن" طالبات الإنابة القضائية ترسل من وزارة العدل في الدولة الطالبة إلى وزارة العدل في الدول المطلوب منها تنفيذ الإجراءات، ويتم إعادة نتيجتها بالطريق ذاته ."وفي حالة الاستعجال، فإن طلبات الإنابة يتم إرسالها مباشرة عن طريق السلطات القضائية في الدولة الطالبة، إلى السلطات القضائية في الدولة المطلوب منها التنفيذ، وتتم إعادة هذه الإنابات مصحوبة بالأوراق المتعلقة بالتنفيذ بالطرق العادية أي عن طريق وزارة العدل في الدولتين.

[1] – المادة (2/30) من الإتفاقية العربية لمكافحة الإرهاب.

[2] –المادة (3/30) من الاتفاقية العربية لمكافحة الإرهاب.

كما يمكن أن يتم تنفيذ هذه الإنابات عن طريق منظمة الشرطة الدولية "الإنتربول[1]"

ربعا :ألا تكون الجريمة موضوع الإنابة من الجرائم المستبعدة من نطاق الإنابات القضائية الدولية

تنص أغلب النصوص الوطنية والاتفاقيات الدولية المتعلقة بالمساعدة القضائية عموما والإنابات القضائية بشكل خاص على استبعاد بعض الجرائم من نطاقها، والجرائم المستبعدة من نطاق الإنابة القضائية الدولية هي ذاتها الجرائم المستبعدة في نطاق تسليم المجرمين، وأكثر هذه الجرائم شيوعاً هي الجرائم السياسية والجرائم العسكرية[2].

وما يهمنا في بحثنا هو الجرائم السياسية لما فيها من تشابك في بعض عناصرها مع جرائم الإرهاب التي ترتكب بدافع سياسي، حيث استبعدت المادة 30 من القانون الفرنسي الصادر سنة 1927 الجرائم السياسية في نطاق الإنابات القضائية الدولية

[1] - Art 15. : 1 - Letters rogatory referred to in Articles 3, 4 and 5 as well as the applications referred to in Article 11 shall be addressed by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party and shall be returned through the same channels.
2- In case of urgency, letters rogatory may be addressed directly by the judicial authorities of the requesting Party to the judicial authorities of the requested Party. They shall be returned together with the relevant documents through the channels stipulated in paragraph 1 of this article.
3-Requests provided for in paragraph 1 of Article 13 may be addressed directly by the judicial authorities concerned to the appropriate authorities of the requested Party, and the replies may be returned directly by those authorities. Requests provided for in paragraph 2 of Article 13 shall be addressed by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party.
4- Requests for mutual assistance, other than those provided for in paragraphs 1 and 3 of this article and, in particular, requests for investigation preliminary to prosecution, may be communicated directly between the
judicial authorities.
5- In cases where direct transmission is permitted under this Convention, it may take place through the International Criminal Police Organization (Interpol)

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 256.

عزت مصطفي الدس وقي، شرح قانون الأحكام العسكرية، الكتاب الأول، قانون العقوبات، الطبعة الأولي، دار النهضة العربية، القاهرة، 1991 ص 44.

[1]وكذلك فعلت المادة 543 من مشروع قانون الإجراءات الجنائية المصري إذ اعتبرت أن إحدى الحالات التي يجوز فيها للدولة رفض طلب الإنابة القضائية التي لا يجوز التسليم فيها طبقًا للفقرتين أ ولا وثالثًا من 552[2]

أما الاتفاقية الأوروبية للمساعدة القضائية فقد استبعدت في الفقرة الأولى من مادتها الثانية كل من الجرائم السياسية والجرائم الأخرى المرتبطة بالجرائم السياسة في نطاق الإنابة القضائية الدولية[3] فيما خلت الاتفاقية العربية لمكافحة جرائم الإرهاب من هذا الاستثناء حيث اكتفت في تحديد حالتين يجوز فيها للدولة رفض الإنابة القضائية وهما حالة ما إذا كانت الجريمة موضوع الطلب محل اتهام أو تحقيق أو محاكمة لدى الدولة المطلوب تنفيذ الإنابة، وحالة إذا كان تنفيذ الطلب في شأنه المساس بسيادة الدولة المكلفة بتنفيذه أو بأمنها أو بالنظام العام فيها[4]

---

[1]- Art 30 " En cas de poursuites répressives, non politiques

[2] – حددت المادة 552 في مشروع قانون الإجراءات الجنائية المصري الحالات التي لا يجوز التسليم فيها)

وهي:

أولا: إذا كانت الجريمة المطلوب تسليمه من أجلها جريمة سياسية أو مرتبطة بجريمة سياسية أو كان المطلوب تسليمه لاجئ سياسي وقت تقديم طلب التسليم

ثانيًا: إذا كانت الجريمة المطلوب التسليم من أجلها عسكرية بحته.

ثالثا: إذا كانت أسباب جدية للاعتقاد أن طالب التسليم و ان استند إلى إحدى جرائم القانون العام إنما قد قدم بهدف محاكمة أو معاقبة الشخص لإعتبارات تتعلق بالعنصر أو الديانة أو الجنسية أو الرأي السياسي أو أن يكون من شأن توافر أي في هذه الإعتبارات تسوئ مركز الشخص المطلوب تسليمه.

[3]- "Assistance may be refused: (a if the requested Party considers that execution of the request is likely to prejudice the sovereignty, security, order public or other essential interests of its country "

[4] – المادة 10 من الاتفاقية العربية لمكافحة الإرهاب.

المطلب الثاني: دور الإنابات القضائية الدولية في التعاون الدولي لمكافحة الجرائم الإلكترونية :

لم تتضمن أغلب الاتفاقيات الدولية المعنية بمكافحة جرائم الإرهاب عرضاً واضحا وتفصيليا لما يتعلق بالانابات القضائية الدولية، حيث اكتفت بالإشارة إلى ضرورة تعزيز التعاون والمساعدة القضائية فيما بينها.

لم تتضمن أغلب الاتفاقيات الدولية المعنية بمكافحة جرائم الإرهاب عرضًا واضح وتفصيل يا لما يتعلق بالانابات القضائية الدولية، حيث اكتفت بالإشارة إلى ضرورة تعزيز التعاون والمساعدة القضائية فيما بينها.

وقد كانت الاتفاقية العربية لمكافحة جرائم الإرهاب، والصادرة بقرار من مجلسي وزراء العدل والداخلية العرب في اجتماعهما المشترك الذي عقد بمقر الأمانة العامة لجامعة الدول العربية بتاريخ 1998/40/22 من الاتفاقيات الدولية التي تضمنت أحكاما تفصيلية للإنابات بين الدول الموقعة عليها.

ولا تختلف فكرة الإنابة القضائية في اتفاقية مكافحة الإرهاب عن الإنابة القضائية في القواعد العامة للقانون، إلا أنها هنا متخصصة بنوع واحد من الجرائم الخطيرة والتي تتطلب تبسيط أمور المساعدات القضائية فيما بين الدول، وهي جرائم الإرهاب .

ونستعرض فيما يلي:

الأحكام الواردة في الاتفاقية العربية لمكافحة جرائم الإرهاب فيما يتعلق الإنابات القضائية الدولية:

الفرع الأول: المسائل التي تتناولها الإنابة:

تنص المادة 9 من الاتفاقية على ما يلي" : لكل دولة متعاقدة أن تطلب إلى أية دولة أخرى متعاقدة، القيام في إقليمها نيابة عنها .بأي إجراء قضائي متعلق بدعوى ناشئة عن جريمة إرهابية وبصفة خاصة.

أ – سماع شهادة الشهود والأقوال التي تؤخذ على سبيل الاستدلال.

ب – تبليغ الوثائق القضائية.

ج – تنفيذ عمليات التفتيش والحجز.

د – إجراء المعاينة وفحص الأشياء

هـ – الحصول على المستندات أو الوثائق أو السجلات اللازمة أو نسخ مصادقة منها."

نتبين من هذا النص أن الإنابة تكون جائزة لأي إجراء يتعلق بالتحقيق، أو باستقصاء الأدلة، أو سماع شهود مقيمين في البلد المناب، أو استجواب المتهمين، أو المعاينة والحصول المستندات الضرورية والكائنة لدى الدوائر الرسمية في البلد المناب واللازمة لكشف ملابسات الجريمة، وكذلك التفتيش والحجز .أي أن الإنابة تكون جائزة بصدد أي إجراء قضائي يتعلق بسير المحاكمة في الدعوى.

ولكن وفقًا لنص هذه المادة لا يجوز أن تتضمن الإنابة أعمالا تنفيذية، كتنفيذ الأحكام الجنائية الأجنبية، لأن نطاق الإنابة لا يتعدى الإجراءات القضائية المتعلقة بدعوى لم تزل قيد النظر أمام السلطات القضائية للدولة المنيبة .أما تنفيذ الأحكام فيكون خاضعا لقواعد خاصة نصت عليها اتفاقية أخرى موقعة بين الدول العربية هي اتفاقية الرياض للتعاون القضائي عام 1983.

الفرع الثاني : حالات رفض الإنابة:

يجوز للسلطات القضائية للدولة المنابة رفض طلب الإنابة القضائية المقدمة من دولة عربية أخرى في حالتين[1]

أ– إذا كانت الجريمة موضوع الطلب محل اتهام أو تحقيق أو محاكمة لدى الدولة المطلوب إليها تنفيذ الإنابة.

[1] – المادة (10) من الاتفاقية العربية لمكافحة الإرهاب.

ب- إذا كان تنفيذ الطلب من شأنه المساس بسيادة الدولة المكلفة بتنفيذه أو بأمنها أو بالنظام العام فيها.

وفي الواقع، كما أشرنا سابقا، فإن مسألة النظام العام تخضع في تقديرها لسلطة الدولة المنابة، ومن ثم فإن هذا البند يمكن أن يكون شماعة لرفض طلبات الإنابة على اعتبار أن تنفيذها يمكن أن يمس بالنظام العام.

كما نلحظ أن الاتفاقية العربية لمكافحة الإرهاب لم تنص على اعتبار الجرائم السياسية، والتي تتشابه عناصرها مع عناصر جرائم الإرهاب التي ترتكب بدافع سياسي، من الحالات التي يجوز فيها رفض الإنابة، على غرار ما فعلته الاتفاقية الأوربية للمساعدة القضائية.

الفرع الثالث: إجراءات تنفيذ الإنابة:

ينفذ طلب الإنابة وفقا لأحكام القانون الداخلي للدولة المطلوب إليها التنفيذ، وعلى وجه السرعة، ويجوز لهذه الدولة تأجيل التنفيذ حتى استكمال إجراءات التحقيق والتتبع القضائي الجاري لديها في نفس الموضوع، أو زوال الأسباب القهرية التي دعت للتأجيل، على أن يتم إشعار الدولة الطالبة بهذا التأجيل [1]"فتنفيذ الإنابة القضائية فيما يتعلق بجرائم الإرهاب، يتم وفقًا لقواعد الإجراءات المنصوص عليها في قانون بلد المحكمة المنابة، وعلى ذلك يتبع في استماع الشهود واستجواب المتهمين والاطلاع على المستندات والأوراق وجميع إجراءات سير التحقيق، الإجراءات المقررة في قانون بلد المحكمة المنابة.

الفرع الرابع : الأثر القانوني للإجراءات المنفذ بطريق الإنابة:

"يكون للإجراء الذي يتم بطريق الإنابة، وفقا لأحكام هذه الاتفاقية، الأثر القانوني ذاته، كما لو تم أمام الجهة المختصة لدى الدولة طالبة الإنابة .[2]"فالسلطة القضائية للدولة المنيبة تأخذ بالإجراءات الذي قامت به السلطة القضائية في الدولة المنابة كإجراء

[1] – المادة (11) من الاتفاقية

[2] –المادة (12 / أ) من الاتفاقية

رسمي مثبت لمضمونه إثباتا تامًا لا لبس فيه بعد أن تُضمِنه إلى أوراق الدعوى القائمة أمامها، وينتج هذا الإجراء أثره القانوني كما لو قامت به المحكمة المنيبة بنفسها، وتستند إليه في سير قضاء الدعوى أو القضية كأي إجراء آخر صادر عنها .وعلى ذلك لا يعتبر الإجراء المنفذ من السلطة القضائية التي قامت به، أنه صادر من سلطة أجنبية وخاضع للإجراءات والقواعد التي تخضع لها تنفيذ الأحكام الجنائية الأجنبية .كما لا يجوز استعمال ما نتج عن تنفيذ الإنابة إلا في نطاق ما صدرت الإنابة بشأنه[1]

المبحث الثاني : الوسائل المستحدثة للتعاون الدولي لمكافحة الجريمة الإلكترونية :

كان للتطور العلمي والتكنولوجي الكبير الحاصل في عصرنا الراهن أثره الواضح على كافة مرافق الحياة المعاصرة، الأمر الذي أدى إلى استفادة الجماعات الإجرامية من المعطيات التكنولوجية الحديثة في تأمين أنشطتها الإجرامية[2]، لذا كان لازمًا على القواعد الجنائية أن تخرج في طابعها التقليدي المفرط الذي يميل إلى الثبات والاستقرار، والذي أدى إلى قصور تلك القواعد عن ملاحقة التطور العلمي الحاصل، مما جعل بعض التشريعات الجنائية تحاول إعادة النظر في المبادئ القانونية المستقرة، واستحدثت قواعد ووسائل جديدة تواجه هذه المشكلات بهدف استثمار هذا التطور في خدمة العدالة الجنائية[3].

---

[1] – المادة (12 / ب) من الاتفاقية.

[2]- Kelly Gable , Securing the Internet Against Cyber terrorism and Using Universal Jurisdiction as a Deterrent, Drexel university Earle Mack school of law, ,August 14, 2009, Working Paper Series, p2.

[3] – د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، 2000 ، ص 3 وما بعدها. د. عمر سالم، المراقبة الإلكترونية، طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية 2000 ، ص 1 وما بعدها. د. عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 173.
وبالفعل فقد أصبحت للوسائل الإلكترونية دور كبير في جميع الأدلة واستخدام الشهود ومراقبة المجرمين إلكترونيًا وتتبعهم وتنفيذ العقوبات السالبة بحقهم، حيث يتم حبس الشخص في محل إقامته خلال ساعات محددة مثلا مع خضوعه لرقابة إلكترونية كبديل عن تنفيذ هذه العقوبة في المؤسسات العقابية التقليدية. انظر: د. عمر سالم، المراقبة الإلكترونية، طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، مرجع سابق، ص 1

وتُعَد تقنية التحقيق والمحاكمة الجنائية عن بعد عبر وسيلة الVideoconference من أهم ثمار تلك الجهود، إذ تعتبر هذه الوسيلة خروجًا عن الطابع التقليدي المفرط في ميدان التحقيق والمحاكمة الذي اتسم به مرفق العدالة الجنائية، إلى طابع أكثر ليونةً وأوفر جهدا وأقل وقتًا، حيث يترتب على تطبيقها امتداد النطاق الجغرافي لجلسات التحقيق أو المحاكمة الجنائية إلى أكثر من دولة، والتي يتحقق بموجبها مبدأ المواجهة بين أطراف الدعوى، دون حاجة إلى التواجد الفعلي في مكان واحد، لهذا يطلق البعض على هذه الوسيلة تعبير" الجلسات التكنولوجية أو الإلكترونية[1] "

أما الوسيلة الثانية فجاءت نتيجة حتمية لما أفرزه استفادة الإرهابيين من التكنولوجيا الحديثة ونظام البنوك والمصارف، التي تيسر لهم انتقال الأموال المستخدمة لتسهيل تنفيذ عملياتهم من دولة إلى دولة، فكان لابد من وضع حد لتمويل الإرهاب.

كما فرضت قواعد البيانات المتعلقة بجرائم الإرهاب نفسها بقوة، كإحدى وسائل التعاون الدولي في عصر المعلوماتية، كونها توفر للمؤسسات والأجهزة الأمنية القدرة على بناء التنبؤات المستقبلية واستكشاف السلوك والاتجاهات المتعلقة بتلك الجرائم.

اتجه مرفق العدالة الجنائية في الآونة الأخيرة إلى إرساء قواعد قانونية جديدة تواجه المشكلات التي أسفر عنها التطور التكنولوجي والمعرفي الكبير، وذلك من خلال الأخذ بمعطيات التكنولوجيا الحديثة في الكشف عن الجرائم وملاحقة مرتكبيها ومحاكمتهم، دون الإخلال في الوقت ذاته بحقوق المتهم أو غيره من أطراف الخصومة الجنائية .وتجلى ذلك بشكل واضح من في مجال التحقيق أو خلال استخدام تقنية الاتصال المرئي

وفي ذلك يقول أحد الفقهاء: "أن المجرم يتطور بتطور العلم وتطور القيم الاجتماعية ومقتضى ذلك أن المجرم في العصر الحديث لم يعد غافلاً عن الوسائل العلمية التي تتبعها أجهزة الشرطة وأجهزة مكافحة الجريمة في تتبع المجرمين وتضييق الخناق عليهم واثبات التهمة في حقهم ، بل قد تتجاوز قدراتهم أحيانا في تجنب هذه الوسائل قدرات القائمين باستخدامها". انظر: د. لطفي جمعه ، دور الشرطة في حفظ السكينة والنظام ، مجلة الأمن العام المصرية ، العدد 24 ، ص 9

[1] – عادل يحيى، التحقيق والمحاكمة الجنائية عن بعد، دار النهضة العربية، الطبعة الأولى، 2006، ص 27

المسموع videoconference في مجال التحقق أو المحاكمة الجنائية عن بعد، حيث تبنت العديد من دول العالم استخدام هذه التقنية، نظرا للمزايا والفوائد الكبيرة التي يمكن أن تحققها[1]

وقد شكل استخدام تقنية الvideoconference مرحلة جديدة من مراحل تطور الإجراءات الجنائية، بشكل يعكس الرغبة في الاستفادة من المعطيات التكنولوجية الحديثة في مجالات تطوير مرافق العدالة الجنائية[2].

ويعتبر البروتوكول الإضافي الثاني للاتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية من أهم الاتفاقيات التي وضعت قواعد لاستخدام هذه التقنية في مجال التعاون الدولي في مكافحة الجريمة[3]

[1] – استخدمت هذه التقنية في إيطاليا أول مرة عام 1992 بموجب المرسوم رقم 306 لسنة 192) والمادة 147 مكرر الوردة ضمن المواد الخاصة بتطبيق قانون الإجراءات الجنائية، حيث كانت تقتصر على التحقيق عن بعد من خلال سماع الشهود. ونظرا للنتائج الإيجابية التي حققتها هذه التقنية فقد اتسع نطاق استخدامها بموجب القانون رقم 11 لسنة 1998 ، ليشمل إج ا رءات محاكمة المجرمين الخطرين وهم داخل المؤسسات العقابية التي قد تبتعد عن قاعة المحكمة مئات الأميال، دون المساس بحقوق الدفاع. كما على نطاق واسع في مجال التحقيق videoconference تستخدم الولايات المتحدة الأمريكية تقنية والمحاكمة الجنائية على المستوى الداخلي وكذلك في مجال المساعدة القضائية الدولية في المسائل الجنائية عند وجود اتفاقية دولية حيث توجد 94 نيابة من النيابات الفدرالية الأمريكية مجهزة بهذه التقنية الحديثة. كما أقرت بعض الدول ككندا وأست ا رليا ونيوزلندا، استخدام هذه التقنية في مجال محاكمة الأحداث وذلك لتلافي الأضرار النفسية السيئة التي قد تترتب على حضورهم شخصيًا جلسات المحاكمة. كما أقرت بلجيكا استخدامها على مستوى المساعدات القضائية الدولية في المجال الجنائي، لكنها لم تقر بذلك المستوى الداخلي. أنظر: عادل يحيى، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 16.

[2] - Tokson, Matthew J., Virtual Confrontation: Is Videoconference Testimony by an Unavailable Witness Constitutional? (June 11, 2007). University of Chicago Law Review, Vol. 74, No. 4, 2007. P1581.

[3] – ونشير هنا إلى أن النظام الأساسي للمحكمة الجنائية الدولية سمح أيضا باستخدام تقنية التحقيق والمحاكمة الجنائية عن بعد Videoconference في حالات معينة لكنه لم يضع ضوابط أو قواعد تفصيلية لهذا الاستخدام كما فعل البروتوكول الإضافي للاتفاقية الأوربية للتعاون الدولي في المسائل الجنائية، حيث جاء في المادة (29) فقرة 2 من نظام روما: "يدلي الشاهد في المحاكمة بشهادته شخصيا، إلا بالقدر الذي تتيحه التدابير المنصوص عليها في المادة 68 أو في القواعد الإجرائية وقواعد الإثبات، ويجوز للمحكمة

ونظرا للدور الذي يمكن أن تلعبه هذه التقنية في تعزيز التعاون الدولي في مكافحة الجريمة وإمكانية تسخيرها في التعاون الدولي في مكافحة جرائم الإرهاب، فإننا سنبحث فيها من خلال هذا المبحث وذلك في مطلبين منفصلين على النحو التالي:

المطلب الأول :ماهية تقنية الVideo conference وأهميتها :

المطلب الثاني :قواعد التحقيق والمحاكمة الجنائية عن بعد عبر الVideoconference في البروتوكول الإضافي الثاني للاتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية:

المطلب الأول :ماهية تقنية الVideo conference وأهميتها :

يقتضي تحديد ماهية تقنية الاتصال والتحقيق عن بعد محاولة التعريف بهذه التقنية ومن ثم الوقوف على أهميتها في المجال الجنائي والتعاون في مكافحة الجريمة.

الفرع الأول :تعريف التحقيق الجنائي عن بعد Video conference :

ال Video conference أو تقنية الاتصال المرئي المسموع هي" وسيلة أو آلية حديثة لمباشرة الإجراءات التحقيق أو المحكمة الجنائية عن بعد، يتم الاستعانة بها، في بعض الحالات، لسماع شهادة الشهود والمتعاونين مع العدالة لكشف غموض الجرائم الخطيرة لاسيما المنظم منها .بل وكذلك محاكمة المتهمين، رغم تواجدهم داخل المؤسسة العقابية، أمام محكمة قد تبتعد عن هذه المؤسسة أو تلك المؤسسات مئات الأميال[1]

فالتحقيق الجنائي عن بعد (Videoconference) تعَد خروجًا على القاعدة العامة في جلسات الحقيق والمحاكمة والتي تتم في نطاق جغرافيا واحد، بخصوص المتهمين والشهود

أيضاُ أن تسمح بالإدلاء بإفادة شفوية أو مسجلة من الشاهد بواسطة تكنولوجيا العرض المرئي أو السمعي فضلاً عن تقديم المستندات أو المحاضر المكتوبة، رهناً بم ا رعاة هذا النظام الأساسي ووفقاً للقواعد الإجرائية وقواعد الإثبات، ويجب ألا تمس هذه التدابير حقوق المتهم أو تتعارض معها". انظر: د. منيرة مسعود السبيعي، ضمانات المتهم أمام المحكمة الجنائية الدولية، رسالة دكتوراة مقدمة إلى جامعة القاهرة ، 2010 ، ص 378.

[1] – عادل يحي، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 27

أو غيرهم من أطراف الخصومة، بحيث يكون لكل منهم دوره في سير جلسات المحاكمة أو التحقيق من خلال مشاركته فيها[1]

وباللجوء إلى استخدام تقنية الـ Video conference في مجال التحقيق الجنائي أصبح في الممكن امتداد النطاق الإقليمي لجلسة التحقيق أو المحاكمة بحيث يشمل عدة أماكن إقليمية داخل الدولة الواحدة أو أماكن إقليمية في دول متعددة، وبحيث تكون سلطة التحقيق في دولة، والمتهم الذي يتم التحقيق معه يكون في دولة أخرى، وقد يكون الشهود في دولة ثالثة[2]

ومن الواضح أن هذه الوسيلة من الممكن أن تلعب دورا كبيرا في التعاون الدولي في مكافحة الجرائم عموماً وجرائم الإرهاب بشكل خاص، إلا أنها تحتاج من الناحية الفنية والتقنية توافر شبكة اتصال مرئي ومسموع على مستوى عالٍ من التطور بين قاعة الجلسة التي تتم فيها إجراءات التحقيق والمكان أو الأماكن التي يتواجد فيها المتهم أو الشهود، بحيث تؤمن الرؤية المتبادلة الواضحة والصوت الواضح دون انقطاع .ومن ثم فإن أي من الدول التي لا تتوفر فيها تلك التقنيات يحق لها رفض استخدام هذا النظام، إلا إذا قامت الدولة الطالبة بوضع هذه التقنية بين يدي الدولة المنفذة[3]

ويمكن التمييز في هذا الصدد بين أربعة نظم مختلفة للتحقيق الجنائي عن بعد conference Video وهي[4]

أولا- نظام الاتصال من نقطة إلى أخرى "punto - punto"

---

[1] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 175

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 175
عادل يحي، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 62

[3] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 197

[4] – انظر في عرض هذه النظم الأربعة مجال التحقيق الجنائي عن بعد: د. عادل يحيى، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 30 ، وما بعدها

يتم بمقتضى هذا النظام الاتصال المباشر، المرئي والمسموع، بين قاعة المحكمة ومكان آخر يتواجد فيه المتهم أو أحد الشهود .ويعد هذا النظام أبسط أنظمة الاتصال المرئي والمسموع وأقلها أثارة للمشكلات التقنية والفنية.

ثانيا – نظام السويتش أو المتحدث النشط " switching ،ou du parleur actif كأن تكون ، Video conferenceحيث تتعدد الأماكن التي يتم بينها الاتصال عبر ال المحكمة في دولة والشهود في دولة والمتهم في دولة ثالثة، ويتطلب هذا النظام أن يتم إعداد هذه الأماكن إعداداً تقنياً جيداً، بحيث يبدو لهذه الأط ا رف وكأنهم في مكان واحد . ولا تظهر شاشة العرض المتواجدة في جميع هذه الأماكن، إلا صورة واحدة هي صورة الشخص الذي يتكلم سواء إلى القاضي أو المتهم أو الشاهد، وفي حالة تكلم أكثر من شخص في نفس الوقت فإن الاتصال المرئي المسموع يتم أوتوماتيكياً مع المكان الذي يوجد فيه الشخص صاحب الصوت الأعلى[1]

ثالثا– نظام الحضور المستمر الثابت أو الموحد Continuous presence "standardبين خمسة أماكن ، Video conferenceويتم الاتصال، وفقًا لهذا النظام، بواسطة ال مختلفة وبعيدة عن بعضها جغ ا رفيًا، والأماكن هي قاعة المحكمة التي تنعقد فيها جلسة المحاكمة، وأربعة أماكن أخرى يتواجد فيها باقي أشخاص الدعوى من شهود ومتهمين وغيرهم .ويوجد في كل مكان شاشة عرض لعرض الصورة إلى هؤلاء الأشخاص، بالإضافة إلى أجهزة دقيقة يتم بواسطتها سماع صوت من يتكلم من المشاركين بهذه الجلسة.

رابعا– نظام الحضور المستمر المتقدم "Continuous presence advanced وفقًا لهذا النظام يتم الاتصال المرئي المسموع الـ Video conference بين القاعة الرئيسية التي تجري فيها إجراءات التحقيق، وبين عدد كبير من الأماكن الأخرى البعيدة

[1] – عادل يحيي، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 31

عنها، حيث يتم تزويد ، video conferenceويعد هذا النظام من أحدث النظم التطبيقية لتقنية ال الأماكن التي تتطلب وجود هذه التقنية، بشاشات عرض لصورة وأجهزة الصوت التي يتكلم من خلالها المشاركين، ويتم تقسيم شاشة عرض الصور الموجودة في كل مكان من هذه الأماكن إلى أربعة أقسام، ويتم تثبيت القسم الأول لعرض بانوراما عامة للقاعة التي تتم فيها المحاكمة، وقسمين آخرين في مكانين من الأماكن المتصلة بهذه القاعة، أما القسم الرابع من شاشة العرض، فتنتقل آلياً بصورة تلقائية إلى صورة الشخص الذي يشارك، ويتكلم بصوت أعلى من غيره من المشاركين في جلسة التحقيق أو المحاكمة.

الفرع الثاني: أهمية تقنية ال Video Conference كوسيلة من وسائل التعاون الدولي في مكافحة الجريمة :

أشرنا إلى أن تقنية ال videoconference تمثل إحدى الوسائل الحديثة للتحقيق الجنائي، والتي اقتضتها ضرورة الاستعانة بالمعطيات التكنولوجية الحديثة، بغية تطوير أداء مرفق العدالة الجنائية ودعم وإضافة وسيلة جديدة إلى وسائل التعاون الدولي في مكافحة الإجراءات، وتتجلى أهمية هذه التقنية فيما يلي[1]

أولا: سرعة الإجراءات وخفض النفقات:

تتجه العديد من التشريعات الجنائية الحديثة، من خلال الاتفاقيات الدولية، إلى تعزيز التعاون الدولي في مكافحة الجرائم، من خلال اتخاذ التدابير التشريعية والعملية لرفع كفاءة أجهزة العدالة الجناية وتطوير أدائها.

ويمثل الاستعانة بالوسائل التكنولوجية الحديثة في ميدان البحث والتحقيق الجنائي إحدى وسيلة video conference أهم هذه التدابير في جميع م ا رحل الدعوى الجنائية، وتعَد

[1] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 179 ، وما بعدها. انظر) أيضًا: عادل يحيي، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 37 ، وما بعدها.

تقنية ال هامة من وسائل التحقيق والمحاكمة الجنائية لما لها من دور كبير في تبسيط وتسريع إجراءات العدالة الجنائية[1]

مع إجراءات Video Conference فإذا قارنا إجراءات التحقيق عن بعد عبر ال الإنابات القضائية مثلا نجد أن الإنابة القضائية تتسم بالبطء والتعقيد، حيث يتم إرسالها عبر الطرق الدبلوماسية في الدولة المطلوب فيها التنفيذ، ومن ثم إلى وزارة العدل فالمحكمة المختصة ومن ثم العودة بذات الطريق حتى تصل إلى الجهة القضائية في الدولة الطالبة، وهذا كله يتصف بطول الإجراءات وزيادة التكاليف[2] وطول هذه الإجراءات قد يؤدي إلى الإفراج عن المهتمين المحبوسين احتياطياً إذا لم يتم محاكمتهم خلال مدة محددة .لذلك فاللجوء إلى التحقيق عن بعد قد يحول دون طول هذه الإجراءات ومن ثم تجنب الإفراج عن المتهمين لانتهاء المدة الواجبة في الحبس الاحتياطي[3] فضلا عن أن نقل المتهمين من أماكن الاحتجاز إلى الأماكن التي تنعقد فيها جلسات التحقيق أو المحاكمة تؤدي إلى زيادة النفقات التي تترب على ذلك.

---

[1]- Sossin, Lorne and Yetnikoff, Zimra, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources (Augus 5, 2007). Windsor Yearbook of Access to Justice, 2007. p257.

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، ص 185 ، وما بعدها.

[3] – إذ تشترط أغلب التشريعات الجنائية الإفراج عن المتهم الموقوف احتياطياً إذا لم تتم محاكمته خلال فترة معينة يحددها المشرع، ومثال ذلك نص المادة (142) من قانون الإجراءات الجنائية المصرية والتي نصت على أنه "ينتهي الحبس الاحتياطي حتماً بمضي خمسة عشر يوماً على حبس المتهم، ومع ذلك يجوز لقاضي التحقيق بعد سماع أقوال النيابة العامة والمتهم أن يصدر أمر بمد الحبس مد أخرى لا يزيد مجموعها على خمسة وأربعين يوماً. على أنه في مواد الجنح يجب الإر وكان الحد الأقصى للعقوبة قانونا لا يتجاوز سنة واحدة ولم يكن عائدا وسبق الحكم عليه بالحبس أكثر من سنة". كما تنص المادة (143) من ذات القانون على أنه " إذا لم ينته التحقيق ورأي القاضي مد الحبس الاحتياطي زيادة على ما هو مقرر في المادة السابقة وجب قبل انقضاء المدة السالفة الذكر إحالة الأوراق إلى محكمة الجنح المستأنفة منعقدة في غرفة المشورة لتصدير أمرها بعد سماع أقوال النيابة العامة والمتهم بمد الحبس مدداً متعاقبة لا تزيد كل منها على خمسة وأربعين يوما إذا اقتضت مصلحة التحقيق ذلك أو الإفراج عن المتهم بكفالة أو بغير كفالة. ومع ذلك يتعين عرض الأمر على النائب العام إذا انقضى على حبس المتهم احتياطيا ثلاثة شهور وذلك لاتخاذ الإجراءات التي يراها كفيلة للانتهاء من التحقيق. وفى جميع الأحوال لا يجوز أن تزيد مدة الحبس الاحتياطي على ستة شهور، ما لم يكن المتهم قد أعلن بإحالته إلى المحكمة المختصة قبل انتهاء هذه المدة، فإذا كانت التهمة

فالتحقيق عن طريق ال videoconference يوفر عناء الإجراءات ويخفف من النفقات، حيث تكفل هذه التقنية حقوق الدفاع المقررة للمتهم، من خلال السماح له برؤية وسماع ومناقشة سلطة التحقيق أو هيئة المحكمة وسائر الخصوم والشهود، بما يحقق قاعدتي شفهية المرافعة والمواجهة بين الخصوم، وتسهم في الوقت نفسه في الحد من نفقات وعناء نقل المتهمين من أماكن احتجازهم إلى أماكن جلسات التحقيق أو المحاكمة.[1] كما أن الدول التي تمتنع عن تسليم مواطنيها للتحقيق أو المحاكمة يمكنها السماح لمواطنيها بالإدلاء بشهاداتهم أو مواجهتهم بالتهم المنسوبة إليهم عن طريق هذه التقنية [2].

ثانيا: تعزيز الوسائل المتبعة في التعاون الدولي لمكافحة الجريمة:

تُعَد وسيلة مستحدثة وإضافية من وسائل video conference تقنية الاتصال المرئي التعاون الدولي في مكافحة الجرائم والمساعدات القضائية المتبادلة بين الدول، ولاسيما في مجال استجواب المتهمين وسماع الشهود عندما يكون ون مقيمين في إقليم دولة غير تلك الدولة التي تقوم بالتحقيق أو المحاكمة .حيث يكفل اللجوء إلى هذه التقنية الوصول إلى حل توافقي للمشكلات الناتجة عن اختلاف النظام الإجرائي للدولتين الطالبة والمطلوبة منها التنفيذ، على اعتبار أنه سوف يكون هناك قانون واحد واجب التطبيق هو قانون الدولة الطالبة، التي تباشر الإجراءات وفقًا لما هو منصوص عليها في قانونها[3]

المنسوبة إليه جناية فلا يجوز أن تزيد مدة الحبس الاحتياطي على ستة شهور إلا بعد الحصول قبل انقضائها على أمر من المحكمة المختصة بمد الحبس مدة لا تزيد على خمسة وأربعين يوما قابلة للتجديد لمدة أو مدد أخرى مماثلة، وإلا وجب الإفراج عن المتهم في جميع الأحوال".

[1] – عادل يحي، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص.53,54.

- Sossin, Lorne and Yetnikoff, Zimra, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources, op. cit. p. 258.

[2] – عمر عيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقًا للمقتضيات التكنولوجية الحديثة، مرجع سابق، ص.287.

[3] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص .181

ثالثا: حماية الشهود والمجني عليهم:

تتجلى أهمية تقنية الحماية video conference باعتباره إحدى الوسائل الفعالة التي تضمن النزاع أو الدعوى القضائية كالشهود والمجني عليهم وأي شخص آخر من الأشخاص المتعاونين مع العدالة، حيث يرى البعض ضرورة استخدام هذه التقنية في سماع الشهود والمتهمين التائبين المتعاونين مع العدالة، لكي يتم الحصول على إفاداتهم المتعلقة بالعصابات الإجرامية المنظمة أو الجماعات الإرهابية المسلحة حول مخططاتهم الإجرامية المستقبلية وغيرها من المعلومات التي تفيد العدالة الجنائية في القبض عليهم . فتستخدم هذه التقنية لعدم كشف هذه الجماعات الإجرامية لأماكن تواجد الشهود وتحركاتهم وذلك حماية لهم من الانتقام الذي قد يتعرضون له .كما تتجه بعض التشريعات الجنائية الحديثة إلى استخدامها في مجال التحقيق والمحاكمات الجنائية الخاصة بالأحداث القاصرين وذلك لتلافي الآثار النفسية الضارة التي تصاحب حضور القاصر بشخصه لجلسات المحاكمة وأمام الجميع، وهو ما تقوم به كل من كندا وأستراليا ونيوزيلندا[1].

لكننا يجب أن نشير هنا إلى أنه وعلى الرغم من المزايا العديدة التي تقدمها هذه التقنية في ميدان التحقيق والمحاكمة، فإن بعض الفقه يرى أنها لا تخلو من أوجه القصور. فمن ناحية أولى قد لا توفر هذه التقنية مستوى عالًيا من الواقعية والجدية في مجال

[1] – عادل يحيي، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 59.

ونشير هنا إلى أن النظام الأساسي للمحكمة الجنائية الدولية قد سمح أن يتم إجراء التحقيق أو سماع الشهود بوسائل غير المواجهة المباشرة وجهاً لوجه في اشارة الى امكانية استخدام تقنية ال video conference وذلك حرصاً على سلامة الشهود أو المتهمين، حيث نصت المادة (68) فقرة 2:" استثناء من مبدأ علنية الجلسات المنصوص عليه في المادة 67 لدوائر المحكمة أن تقوم– حماية للمجني عليهم والشهود أو المتهم–بإجراء أي جزء من المحاكمة في جلسات سرية أو بالسماح بتقديم الأدلة بوسائل إلكترونية أو بوسائل خاصة أخرى، وتنفذ هذه التدابير بشكل خاص في حالة ضحية العنف الجنسي أو الطفل الذي يكون مجنياً عليه أو شاهداً. مالم تأمر المحكمة بغير ذلك، مع مراعاة كافة الظروف لاسيما آراء المجني عليه أو الشاهد". انظر. د: منيرة مسعود السبيعي، ضمانات المتهم أمام المحكمة الجنائية الدولية، مرجع سابق، ص 378.

التحقيق، فمن أهم الأمور التي يمكن أن يستفيد منها القاضي لكشف الحقيقة، هي تقييم لغة الجسد وطريقة التعبير لدى الشاهد أو المتهم، فلا يستطيع القاضي أن يستنبط ردة فعل المستوجب على سؤال معين قد يكون محرجا بالنسبة له حيث إن استخدام هذه التقنية تمنح المتهم فاصلاً زمنيا حتى يستوعب السؤال ويقدم الإجابة عليها. وعلاوة على ذلك فهي لا تسمح لأطراف المحاكمة بالقيام بمداخلات متكررة بشكل مريح وسلس كما هو الحال في الجلسات العادية، مما يقوض النزاهة في الإجراءات و ، يشكك في دستوريتها في بعض الحالات التي لا تتوفر فيها كامل الاحتياجات المتعلقة بسير الدعاوي.[1]

المطلب الثاني : قواعد التحقيق عن بعد عبر الـ video conference في البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية :

سعت الدول الأرورربية من خلال التوقيع على البروتوكول الإضافي الثانية للإتفاقية الأوروبية للمساعدة المتبادلة في المسائل الجنائية والذي تم التوقيع عليه في ستراسبورغ في:2001/11/08 و دخل حيز النفاذ في 2004/02/01[2] الى توسيع نطاق آليات و وسائل التعاون القضائي فيما بينها، بغية الإستفادة من الإمكانيات والوسائل التكنولوجية الحديثة في التحقيق والبحث الجنائي، بحيث تكفل سرعة أكبر و مرونة أعلى وفاعلية أشد لهذا التعاون ، وبما يتعارض مع حقوق الإنسان وسيادة القانون وبهدف ضمان مواجهة قانونية وقضائية فعالة وسريعة للجرائم الخطيرة التي باتت تهدد الدول الأوروبية[3]

[1] - Sossin, Lorne and Yetnikoff, Zimra, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources, op. cit. pp 259 - 262. - Tokson, Matthew J. , Virtual Confrontation: Is Videoconference Testimony by an Unavailable Witness Constitutional?. Op. cit , p1612 - 1613.

[2] - Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. Strasbourg, 8. XI. 2001

[3] -- White, Simone, European Constitution: What is New in the Area of Judicial Cooperation in Criminal Matters and Police Cooperation. Op, cit. p1 - 2.

وبالفعل فقد تم تبني الإنجازات التكنولوجية في هذه الإتفاقية تلبية لإحتياجات المساعدة القضائية في المسائل الجنائية و أهم هذه المظاهر تجلى في اللجوء الى تقنية الإتصال المرئي والمسموع الـ **VIDEOCONFERENCE.**

وقد تضمنت المادتان التاسعة والعاشرة من البروتوكول الإضافي الثاني للإتفاقية بيانا تفصيليا لكيفية إستخدام هذه التقنية،بحيث جاءت بحلول تفصيلية للعديد من المشكلات العملية والقانونية التي قد تعترض إستخدامها في مجال التحقيق الجنائي، مراعية تحقيق التوازن بين كفالة فعاليتها في المساعدة والتعاون القضائي بين الدول الأوروبية من جهة وبين حماية الحريات والحقوق التي تمنحها القوانين الوطنية والدولية للأفراد[1].

وفي ضوء ما تقدم سوف نبين من خلال هذا البروتوكول شروط تطبيق هذه التقنية و كذلك الإجراءات المتبعة في تطبيقها . كما تعرض لأهم تطبيقاتها في مكافحة جرائم الإرهاب وذلك قي ثلاثة فروع منفصلة.

الفرع الأول: شروط تطبيق تقنية الـ VIDEOCONFERENCE في البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية .

الفرع الثاني:إجراءات تطبية تقنية الـ VIDEOCONFERENCE كوسيلة للتحقيق الجنائي في البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية في المسائل الجنائية.

الفرع الثالث: تطبيق تقنية التحقيق الجنائي عن بعد VIDEOCONFERENCE في جرائم الإرهاب.

[1]- White, Simone, European Constitution: What is New in the Area of Judicial Cooperation in Criminal Matters and Police Cooperation. Op, cit. p4.

الفرع الأول: شروط تطبيق تقنيةVIDEOCONFERENCE في البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية :

فرضت المادة التاسعة من البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية شروطا معينة يتوجب التقيد بها عند إستخدام تقنية الـ VIDEOCONFERENCE في التحقيق الجنائي الدولي، حيث إستلزمت عدم تعارض إستخدامها مع المبادىء الأساسية لقانون الدولة المنفذة، كما يتوجب توفير الإمكانيات الفنية التي تمكنها من إستخدام هذه التقنية، وحصر إستخدامها في مجال سماع الشهود والخبراء.

أولا:عدم تعارض إستخدام تقنيةVIDEOCONFERENCE مع قانون الدولة المطلوب منها التنفيذ :

إشترطت الفقرة الثانية من المادة التاسعة من البروتوكول ألا ينطوي إستخدام هذه التقنية على تعارض مع المبادئ الأساسية للقانون في الدولة المنفذة[1] ومن ثم فإن للدولة رفض هذا الإستخدام إذا قدرت أنه يؤدي إلى إهدار المبادىء الأساسية لقانونها[2].

فإستخدام هذه التقنية في سماع شاهد أو خبير أو إستجواب متهم يتواجد في إقليم الدولة المنفذة، هو في الأصل مباشرة لإختصاص قضائي يدخل في إختصاص تلك الدولة، ومن ثم فإن مباشرة دولة أخرى لهذا الإختصاص عن طريق التحقيق الجنائي عن بعد بواسطة الـ VIDEOCONFERENCE يستوجب موافقة الدولة المنفذة

[1] - Article 9 - 2: The requested Party shall agree to the hearing by video conference provided that the use of the video conference is not contrary to fundamental principles of its law and on condition that it has the technical means to carry out the hearing. If the requested Party has no access to the technical means for video conferencing, such means may be made available to it by the requesting Party by mutual agreement

للاطلاع على مضمون الاتفاقية انظر هذا الرابط من موقع مجلس أوروبا على الإنترنت:

http:/ / conventions. coe. int/ Treaty/ en/ Treaties/ Word/ 182. doc

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 196.

التي يتواجد الشخص المطلوب منه الإدلاء بأقواله على أرضها ، ولهذه الدولة أن تقدر مدى تعارض هذا الإجراء مع المبادىء الأساسية لقانونها[1]

ثانيا: توافر الوسائل والامكانيات التي تمكن الدولة المنفذة من استخدام هذه التقنية:

تشترط الفقرة الثانية من المادة التاسعة من البروتوكول الاضافي الثاني للاتفاقية الاوروبية الجديدة للمساعدة القضائية، لاستخدام تقنية الـ VIDEOCONFERENCE في مجال التحقيق الجنائي عن بعد، ان تتوافر لدى الدولة المطلوب منها التنفيذ الامكانيات والوسائل الفنية التي تمكنها من ذلك[2]، وفي حال عجزها عن توفير ذلك هذه الامكانيات والوسائل، يمكن لها ان ترفض استخدام هذه التقنية3، اذ قد يكون استخدامها – في مجال التحقيق الجنائي – مكلفا في بعض الاحيان بالنسبة للدولة المطلوب منها التنفيذ ، من حيث توفير المعدات اللازمة لذلك مما ينطوي عليه نفقات مالية باهظة[4].

لذلك فقد اجازت الاتفاقية للدولة الطالبة – في حال عجز الدولة المطلوب من توفير الامكانيات الفنية والتقنية اللازمة لاستخدام هذه الوسيلة – أن تعرض عليها المساعدة في توفير ما يلزم من معدات او خبرات لاستخدام هذه التقنية ، سواء على سبيل الإعارة أو الهبة [5]

---

[1] – عادل يحيى، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 97.

[2]Art 9 - 2 "….. and on condition that it has the technical means to carry out the hearing. If the requested Party has no access to the technical means for video conferencing, such means may be made available to it by the requesting Party by mutual agreement"–

[3] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 197.

عمر عيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقًا للمقتضيات التكنولوجية الحديثة، مرجع سابق، ص 294.

[4] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 197–198.

[5] – نفس المرجع، ص 197.

– عادل يحيى، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 98.

ثالثا : حصر استخدام هذه التقنية في مجال سماع الشهود و الخبراء:

يقتصر استخدام تقنية الـ VIDEOCONFERENCE وفقا للمادة العاشرة من الاتفاقية الاوروبية الجديدة للمساعدة القضائية، في مجال سماع الشهود وإفادات الخبراء حيث يمكن للسلطات القضائية لإحدى الدول المتعاقدة طلب سماع شخص متواجد على اقليم دولة متعاقدة أخرى – بصفته شاهدا او خبيرا – عبر هذه التقنية متى ثبت استحالة او عدم ملائمة مثول هذا الشخص بنفسه أمامها[1]. ويبدو أن واضعي هذه الاتفاقية أرادوا من خلال هذا الشرط أن يحصروا استخدام هذه التقنية في الاجراءات التي لا تثير الكثير من المشكلات القانونية[2].

كما يتبين أيضا من نص الفقرة الأولى من المادة العاشرة، أن اللجوء لتقنية VIDEOCONFERENCE في التحقيق الجنائي يتم بصورة إحتياطية وليس أصلية فنص هذه المادة يحظر إستخدامها إلا في الحالات التي يثبت فيها عدم ملائمة إنتقال الشاهد أو الخبير الى الدولة الطالبة للمثول أمام سلطاتها القضائية.

ومفاد ذلك أنه يجوز، وفقا لهذه الإتفاقية، إنتقال الشهود أو الخبراء الى الدولة الطالبة، متى إقتضى ذلك، وضمن الشروط التي وضعتها المادة(12) من الإتفاقية الأوروبية للمساعدة القضائية الموقعة سنة 1959، حيث تنص هذه المادة على عدم جواز ملاحقة الأشخاص أو إحتجازهم أو فرض أي قيود أخرى على حريتهم الشخصية

[1]Article 9 - 1: If a person is in one Party's territory and has to be heard as a witness or expert by the judicial authorities of another Party, the latter may, where it is not desirable or possible for the person to be heard to appear in its territory inperson, request that the hearing take place by video conference, as provided for in paragraphs 2 to 7.

[2] –عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية ، مرجع سابق، ص 197.

عمر عيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقًا للمقتضيات التكنولوجية الحديثة، مرجع سابق، ص 294.

في إقليم الطرف الطالب، وذلك بالنسبة للأفعال أو أحكام الإدانة السابقة لمغادرته إقليم الدولة متلقية الطلب[1].

ومن ثم فإن التحقيق عن بعد عبرال VIDEOCONFERENCE هو وسيلة إحتياطية يمكن اللجوء إليها بعد تعذراللجوء الى إستدعاء الشخص المطلوب أوإرسال إنابة قضائية للسلطة القضائية في الدولة المطلوب منها لسماع الشهادة نيابة عنها، و من ثم إرسال نتائج ألإنابة مرة أخرى للدولة الطالبة ، فعند إستنفاذ هاتين الوسيلتين وعدم إمكان إستخدامهما في التحقيق، يجوز للسلطات القضائية أن تطالب القيام بهذا التحقيق عبر ال VIDEOCONFERENCE[2].

الفرع الثاني: إجراءات تطبيق تقنية الـ VIDEOCONFERENCE كوسيلة للتحقيق الجنائي في البروتوكول ألإضافي الثاني للإتفاقية ألأروبية للمساعدة القضائية في المسائل الجنائية :

[1] - European Convention on Mutual Assistance in Criminal Matters Strasbourg, 20. IV. 1959. Article 12 - 1. A witness or expert, whatever his nationality, appearing on a summons before the judicial authorities of the requesting Party shall not be prosecuted or detained or subjected to any other restriction of his personal liberty in the territory of that Party in respect of acts or convictions anterior to his departure from the territory of the requested Party.
A person, whatever his nationality, summoned before the judicial authorities of the requesting Party to answer for acts forming the subject of proceedings against him, shall not be prosecuted or detained or subjected to any other restriction of his personal liberty for acts or convictions anterior to his departure from the territory of the requested Party and not specified in the summons.
The immunity provided for in this article shall cease when the witness or expert or prosecuted person, having had for a period of fifteen consecutive days from the date when his presence is no longer required by the judicial authorities an opportunity of leaving, has nevertheless remained in the territory, or having left it, has returned.
http:/ / conventions. coe. int/ Treaty/ en/ Treaties/ Word/ 030. doc

[2] –عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص194

نصت الإتفاقية على إجراءات معينة يتوجب على الدول ألأطراف الألتزام بها لتطبيق هذه التقنية الحديثة في مجال التحقيق الجنائي عن بعد، سواء من قبل الدولة الطالبة ، او من قبل الدولة المطلوب منها التنفيذ، ذا ما سنبينه على النحو التالي:

أولا : إجراءات السلطة القضائية في الدولة الطالبة:

يتوجب على السلطات القضائية في الدولة الطالبة ان تلتزم، في حال رغبت ، في مباشرة إجراء تحقيق جنائي عبر الـVIDEOCONFERENCE، أن تقدم الطلب على إسم السلطة مقدمة الطلب وكذلك موضوعه و سببه، وتحديد هوية الشخص المطلوب التحقيق معه أو إستجوابه وجنسيته، والتهمة الموجهة له، مع عرض مختصر للوقائع، وعند ألإقتضاء يتعين ذكر إسم وعنوان الجهة الموجه إليها الطلب[1]، كما أوجبت الفقرة الثالثة من المادة التاسعة على الدولة الطالبة أن تبين في الطلب السبب الذي إستندت إليه في إعتبار أن إنتقال الشهود أوالخبراء إليها مستحيل أو غير مرغوب فيه، وإسم السلطة القضائية ومن ألأشخاص الذين سيتم إجراء جلسة الـ VIDEOCONFERENCE معهم[2].

[1] – انظر الفقرة الأولى من المادة 14 من الاتفاقية الأوروبية للمساعدة القضائية الموقعة عام195

Article 14 - 1. Requests for mutual assistance shall indicate as follows:
a. the authority making the request,
b. the object of and the reason for the request,
c. where possible, the identity and the nationality of the person concerned.
d. where necessary, the name and address of the person to be served.
2- Letters rogatory referred to in Articles 3, 4 and 5 shall, in addition, state the offence and contain a summary of the facts

[2] Article 9 - 3. Requests for a hearing by video conference shall contain, in addition to the information referred to in Article 14 of the Convention, the reason why it is not desirable or possible for the witness or expert to attend in person, the name of the judicial authority and of the persons who will be conducting the hearing.

وبعد إتمام ألإجراءات المتعلقة بالطلب المقدم، تباشر السلطات القضائية في الدولة الطالبة إجراءات التحقيق الجنائي، سواء بنفسها أو تحت إشرافها، و التي تتمثل في سماع الشهود أو إفادات الخبراء أو إستجواب المتهم، وذلك وفقا لقانونها الوطني[1].

وتقع جميع النفقات المالية اللازمة لوضع هذه التقنية موضع التطبيق الفعلي على عاتق الدولة الطالبة، حيث تتحمل هذه الدولة النفقات المالية، وكذلك أجور المترجمين والتعويضات التي يتم دفعها للشهود والخبراء ومصاريف إنتقالهم داخل الدولة المنفذة ، فإذا ما تحملت هذه ألأخيرة أي جزء من النفقات، كان لها الرجوع الى الدولة لتعويضها بكل ما تكبدته من مصاريف[2].

ثانيا : إجراءات السلطة القضائية في الدولة المطلوب منها التنفيذ:

تلتزم السلطة القضائية التي يرفع إليها طلب تنفيذ إجراء الـ 67 ، بإخطار الشاهد أو الخبير أو المتهم بهذا الطلب، وذلك بهدف تنفيذه في الموعد المحدد، ويتم هذا ألإخطار وفقا للإجراء أو الشكل الذي نص عليه قانون الدولة المطلوب منها التنفيذ ، وليس قانون الدولة الطالبة[3].

ويتعين حضور ممثل الدولة المنفذة في المكان الذي يتواجد فيه الشخص الذي يتم سماعه أو إستجوابه بواسطة السلطات القضائية للدولة الطالبة ، وكذلك إحضار مترجم متى دعت الحاجة، حيث يقتصر دور ممثل السلطة القضائية للدولة المنفذة على التأكد من شخصية الشاهد أو الخبير أو المتهم، وضمان إحترام المبادئ الأساسية لقانون الدولة

[1] - With reference to hearing by video conference, the following rules shall apply: = c) the hearing shall be conducted directly by, or under the direction of, the judicial authority of the requesting Party in accordance with its own laws;

[2] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص.204 .

[3] -Article 4. The judicial authority of the requested Party shall summon the person concerned to appear in accordance with the forms laid down by its law.

المنفذة وبالتالي لا يحق له توجيه الأسئلة أو الإستجواب أو إبداء الملاحظات[1]. و في حال إتضح له عدم إحترام المبادئ الأساسية للقانون ، كان له إتخاذ الإجراءات اللازمة حتى يتم توافق إجراءات التحقيق مع تلك المبادئ.[2]

كما تلتزم السلطة القضائية في الدولة المنفذة، عقب الإنتهاء من سماع شهادة الشاهد أو إفادة الخبير أو إستجواب المتهم المتهم من قبل السلطة القضائية للدولة الطالبة، إعداد محضر يتضمن تاريخ ومكان إنعقاد الجلسة، وهوية الشخص الذي يتم سماع اقواله ، وهويات بقية الأشخاص الذين شاركوا في الجلسة، والظروف التقنية التي تم فيها إتخاذ الإجراء ، و يتم إحالة هذا المحضر الى السلطة القضائية في الدولة الطالبة.[3]

الفرع الثالث: تطبيق تقنية التحقيق الجنائي عن بعد VIDEOCONFERENCE **في مكافحة جرائم الإرهاب**

لم تستخدم تقنية الـVIDEOCONFERENCE بشكل واسع فيما يتعلق بالتعاون القضائي في مكافحة جرائم الإرهاب، و لعل حادثة إغتيال الوزير البلجيكي Andre

[1] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص.201

– عادل يحيى، التحقيق والمحاكمة الجنائية عن بعد، مرجع سابق، ص 104.

[2] – انظر نص الفقرة الخامسة أ من البروتوكول الإضافي الثاني للاتفاقية الدولية الجديدة للمساعدة القضائية في المواد الجنائية:

Article 5 - a) "judicial authority of the requested Party shall be present during the hearing, where necessary assisted by an interpreter, and shall also be responsible for ensuring both the identification of the person to be heard and respect for the fundamental principles of the law of the requested Party. If the judicial authority of the requested Party is of the view that during the hearing the fundamental principles of the law of the requested Party are being =infringed, it shall immediately take the necessary measures to ensure that the hearing continues in accordance with the said principles".

3 - Article 6. Without prejudice to any measures agreed for the protection of persons, the judicial authority of the requested Party shall on the conclusion of the hearing draw up minutes indicating the date and place of the hearing, the identity of the person heard, the identities and functions of all other persons in the requested Party participating in the hearing, any oaths taken and the technical conditions under which the hearing took place. The document shall be forwarded by the competent authority of the requested Party to the competent authority of the requesting Party.

Cools هي أشهرالحوادث الإرهابية التي استخدمت فيها هذه التقنية للتحقيق و المواجهة مع المتهمين.

فمن المعروف أن الإعتداء على الأشخاص المتمتعين بحماية دولية ، حسب إتفاقية منع ومعاقبة الجرائم الموجهة ضد الأشخاص المحميين دوليا الموقعة في نيويورك عام 1973، تمثل إحدى صورالإرهاب التي جرمتها الإتفاقية، وقضت بأن تجرم كل دولة طرف الإعتداء على شخص يتمتع بحماية دولية، بالقتل عمدا، أو الإختطاف، أو الهجوم على شخصه أوالمس بحريته، أو إرتكاب هجمات خطرة على أماكن عمله الرسمية، أو مراسلاته الخاصة، أو وسائل تنقله، أو التهديد بالقيام بتلك الهجمات أو محاولة القيام بها وبأن تجعل تلك الأفعال مستوجبة " لعقوبات مناسبة تأخذ في الإعتبار طبيعتها الخطرة وإعتبار من يهدد بتلك الهجمات أو يحاول القيام بها شريكا في تلك الإعتداءات[1]

وإستنادا إلى ما سبق فإن حادثة إغتيال رئيس الحزب الإشتراكي الوزير البلجيكي اندريه كواز"Andre Cools" عام 1991، تمثل جريمة إرهابية حسب هذه الإتفاقية، التي ألزمت فيها المادة 8 منها الدول الموقعة على إعتبار هذا النوع من الجرائم، جرائم تستوجب التسليم، لكن مع مراعاة الأحكام الإجرائية والشروط الأخرى المنصوص عليها في قانون الدولة التي يقدم إليها الطلب.

وقد توصلت سلطات التحقيق البلجيكية الى أن بعض المتهمين في هذه القضية هم من الرعايا التونسيين الذين غادروا البلاد وقبض عليهم في تونس، وإعترفوا بإرتكاب الجريمة ولما كان الدستور التونسي يحظر تسليم المواطنين، فقد كان من المستحيل على السلطات التونسية أن تستجيب لطلب السلطات البلجيكية، فلم يتم تسليمهم إليها، ونظرا

[1] – المادة الثانية من اتفاقية الجرائم المرتكبة ضد الأشخاص المتمتعين بحماية دولية، الموقعة في نيويورك عام 1973.

لوجود بعض المشتبه فيه مشاركتهم هذه الجريمة في بلجيكا، فقد أرادت السلطات القضائية البلجيكية إجراء مواجهة بين المتهمين التونسيين وهؤلاء المشتبه فيهم، ولم يكن أمامهم، سوى اللجوء إلى تقنية التحقيق عن بعد عبر الـVIDEOCONFERENCE لإجراء هذه المواجهة، وبالفعل تم ذلك بين المتهمين رغم إختلاف أماكن تواجدهم[1]

وهذا إن دل، فإنما يدل على انه يمكن أن تكون هذه الوسلية الحديثة إحدى الوسائل الفعالة والبديلة للوسائل التقليدية كالإنابات القضائية، أو طلب إستجواب الشاهد أو المتهم في البلد الطالبة له، والذي غالبا ما يواجه بالرفض نظرا لإعتبارات السيادة، فتسهم هذه الوسيلة بشكل كبير في التعاون القضائي بين الدول في مجال كشف الجرائم ألإرهابية ومعاقبة مرتكبيها .

[1] – عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، مرجع سابق، ص 183-184.

خلاصة الفصل الثاني:

يقصد بالإنابة الدولية القضائية طلب اتخاذ اجراء قضائي من اجراءات الدعوى الجنائية تتقدم به الدولة الطالبة الى الدولة المطلوب اليها للفصل في مسألة معروضة على السلطة القضائية في الدولة الطلبة يتعذر عليها القيام به بنفسها، والإنابة القضائية تسهل اذا الاجراءات الجنائية بي الدول بما يكفل اجراء التحقيقات الازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة الإقليمية التي تمنع الدول الاجنبية من ممارسة بعض الأعمال القضائية داخل اقاليم الدول الاخرى , مثال ذلك إجراء التفتيش والضبط والمعاينة ولزيادة تسهيل المساعدة القضائية في المسائل الجنائية عموما إرتئ المجتمع الدولي استحداث آليات تسهل عمليت التعاون الدولي في التحقيق والمحاكمة وابرز الوسائل أو التقنيات المستحدثة نجد ما يعرف بإسم الـ video conference والتي تمثل إحدى وسائل الاتصالات المرئية الحديثة من خلال الانترنت حيث يتم نقل الصوت والصورة لمجموعة من الأشخاص المجتمعين في مكان ما إلى مجموعة أخرى من الأشخاص المجتمعين في أي مكان آخر من العالم، أهم متطلبات هذه التقنية هي وجود انترنت ذات سرعات عالية، وميكروفونات وسماعات ذات جودة معقولة وكذلك كاميرات الويب أو webcam يستطيع المشتركون في التحقيق والمحاكمة سماع ورؤية الطرف الآخر في نفس الوقت كما لوكان الاجتماع في نفس الحجرة وليس في مكانين متباعدين حول العالم.

خاتمة

في الأخير نخلص إلى ضرورة أن يكون هناك تعاون دولي يتفق مع طبيعة الجرائم الإلكترونية والتي تتميز بطابع خاص الأمر الذي يقتضي أن تكون هناك إجراءات تحقيقية سريعة وضرورة أن يسمح هذا التعاون الدولي بسهولة الاتصال المباشر بين أجهزة الشرطة في الدول المختلفة وبين جهات التحقيق وذلك عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالانترنت والحاسوب وتعميمها فالدولة بمفردها لا تستطيع القضاء على هذه الجرائم لأنها عابرة للحدود لذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل في ما بينها لضبط المجرمين ومكافحة هذه الجرائم .

وبعد أن انتهينا من دراستنا هذه خلصنا إلى **النتائج والتوصيات** التالية:

- كان للتطور التكنولوجي الهائل والتقدم العلمي الكبير في وسائل الاتصالات والمواصلات الدور الكبير في زيادة حدة الجريمة الإلكترونية.
- للتعاون الدولي أهمية كبيرة في ميدان مكافحة المجرمين وهو ما بات حاجة ملحة في ميدان مكافحة الجرائم الإلكترونية، لذلك يتوجب على جميع الدول أن تقوم بتفعيل هذا التعاون من خلال تطوير تشريعاتها الجنائية، بما يحقق التكامل بين هذه التشريعات من جهة وبينها وبين القواعد الدولية من جهة أخرى.
- تحقيق التوازن بين إجراءات مكافحة الجريمة الإلكترونية وحماية حقوق الإنسان أمر ضروري للحفاظ على نزاهة هذا التعاون، وهذا الأمر يحتم على الدول عدم التذرع بمكافحة الجريمة الإلكترونية لانتهاك هذه الحقوق.
- تتنوع وتتعدد الأسباب والدوافع التي تدفع فردا أو جماعة ما على ارتكاب جريمة إلكترونية، إلا أن الأسباب والدوافع السياسية الداخلية والدولية هي الأكثر شيوعيا مع عدم إغفال الدور الكبير للدوافع الاقتصادية والاجتماعية وحتى الشخصية . لذلك يتوجب على المجتمع الدولي دراسة هذه الأسباب بشكل جدي بحثاً عن

وضع حلول وقائية وعلاجية فعالة، تراعي الخصوصية الاجتماعية والثقافية والحضارية للدول المختلفة.

- أثبتت الوقائع والممارسات الدولية إمكانية تحمل الفرد للمسئولية الجنائية الدولية لكن إلى الآن لم يتم الاتفاق حول إمكانية تحميل الدولة تلك المسئولية، وإن كانت بعض الوقائع والممارسات أثبتت إمكانية توقيع بعض الجزاءات الاقتصادية وقطع العلاقات الدبلوماسية وغيرها من الجزاءات التي من الممكن أن تُفرض على الدولة .لذلك يجب أن تتحمل المسئولية الجنائية عن الجرائم المرتكبة باسمها أو لحسابها، فالدول أغلبها وقعت على المعاهدات والاتفاقيات المتعلقة بمكافحة الجرائم الإلكترونة، ومن ثم فهي تتحمل مسئولية مخالفتها لأحكام تلك المعاهدات.
- تمثل الجريمة الإلكترونية إحدى الجرائم الدولية، عندما يدخل فيها عنصر دولي متمثل في جنسية الجاني أو الضحية أو مكان ارتكاب الجريمة أو عندما تقع على مصلحة يحميها القانون الدولي، وفي هذه الحالة فإنه يخضع للقواعد التي وضعها القانون الجنائي الدولي.
- كان للقانون الجنائي الدولي، رغم حداثته وعدم اكتمال قواعده، الدور الكبير في تقنين أهم أساليب الجريمة الإلكترونية، وذلك من خلال إبرام الاتفاقيات الدولية المتعلقة بها.
- يبقى للوسائل التقليدية للتعاون الدولي في مكافحة الجرائم الإلكترونية سواء فيما يتعلق بالإنابات القضائية الدولية أو غيرها –فاعليتها وأهميتها الكبيرة في ميدان مكافحة الجرائم الإلكترونية.
- إذ تكتسب المساعدة القضائية في هذا الوقت أهمية كبيرة نظرا لسهولة انتقال وهروب المجرمين من بلد إلى بلد ومن مكان إلى مكان،ناهيك على أن هذه

الجرائم عابرة للحدود حيث يعطي هذا النظام للدولة فرصة لإثبات هيبتها في القصاص ممن انتهك حرمة قوانينها ولاذ بالفرار إلى الخارج.

- كما أن للإنابة القضائية الدولية في المسائل الجنائية أهمية بالغة في التعاون بين السلطات القضائية للدول المختلفة مما يوفر في الإجراءات ويقتصد في النفقات.
- تتجه تشريعات مكافحة الجرائم الإلكترونية اليوم إلى ضرورة الاعتراف بآثار الأحكام الجنائية الأجنبية المتعلقة بالجرائم الإلكترونية ، وهذا الأمر يحتم على الدول المزيد من التنسيق بينها لتوحيد السياسة التشريعية المتعلقة بمكافحة الجرائم الإلكترونية، بغية تأسيس المزيد من الثقة التي تؤدي إلى تأكيد حجية هذه الأحكام مما يجعلها صادرة كما لو كانت من المحاكم الوطنية.
- أثبتت تقنية التحقيق والمحاكمة الجنائية عن بعد Videoconference أنها إحدى الوسائل الفعالة والبديلة للوسائل التقليدية التي كثيرا ما تواجه بالرفض وعدم القبول نظرا لإعتبارات السيادة التي تتذرع فيها الدول للتنصل من هذا التعاون، كما أن هذه الوسيلة الجديدة تسهم في سرعة الإجراءات وخفض النفقات وحماية الشهود والمجني عليهم، على الرغم مما قد يعيبها في أنها قد لا توفر الواقعية والجدية اللازمة في ميدان التحقيق والمحاكمة .لذلك يجب، بعد معالجة أوجه القصور التي تعتريها، تعميم التجربة الأوروبية في هذا المجال إلى جميع دول العالم لما تحمله هذه التقنية من فوائد جمة لما يتعلق بالتعاون بين السلطات القضائية للدول المختلفة.
- مكافحة الجرائم الإلكترونية بات جزءا لا يتجزأ من المنظومة المتكاملة للتعاون الدولي في مكافحة الجرائم الإلكترونية، فعلى الرغم من أن تتبع آثار الجريمة الإلكترونية لن يوقف كل نشاطاتها، فإنه يمكن أن يعطل ويدمر بعض هذه

الأنشطة، وعلى الأقل فإن تعقب المعاملات الإلكترونية سوف يجعل من الصعب عليهم القيام بهذه العمليات مجددا.

- لعبت وتلعب المنظمات والهيئات الدولية والإقليمية دورا مهما في الجهود المبذولة لمكافحة الجرائم الإلكترونية وكان أبرز ما أثمرت عليه هو اتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية.
- يعيب الجهود التي تضلع بها الأمم المتحدة وهيئاتها المتخصصة بأن جميع قراراتها موجهة إلى دول معينة تلتزم بها تلك الدول فقط، فالمشرع هنا هو الدول الكبرى ذات النفوذ والسيادة، والمطلوب منه التنفيذ هي الدول المستضعفة، إذ تصدر هذه القرارات وفق مصالح مبيتة تعكس رغبة الدول الكبرى في سيطرتها على مقدرات الأمم والشعوب.
- لم تقتصر الجهود الدولية لمكافحة الجريمة الإلكترونية على منظمة الأمم المتحدة والهيئات التابعة لها بل كان للمنظمات الإقليمية الدور الكبير في التعاون الدولي، ففي المنطقة العربية كان لجامعة الدول العربية الدور الأبرز في التصدي لهذه الجرائم وتعزيز العمل العربي المشترك للحد منها، فأثمرت جهود المجالس التابعة لها عن ولادة الاتفاقية العربية بشأن مكافحة الجريمة الإلكترونية .
- على الرغم من الجهود المبذولة والتي تبذل من قبل التشريعات الوطنية والهيئات الدولية والإقليمية للتصدي للجريمة الإلكترونية، إلا أن تلك الجهود اصطدمت بالعديد من العقبات والمشاكل التي وضعت العراقيل أمام سير العدالة الجنائية . فالقصور في المجال التشريعي الدولي وعدم الوصول إلى تعريف متفق عليه للجريمة الإلكترونية

الملخص العام:

كان للتطور العلمي والتكنولوجي الكبير الحاصل في عصرنا الراهن أثره الواضح في كافة مرافق الحياة المعاصرة، الأمر الذي أدى إلى استفادة الجماعات الإجرامية من المعطيات التكنولوجية الحديثة في تأمين أنشطتها الإجرامية لذا كان لازما على القواعد الجزائية أن تخرج في طابعها التقليدي المفرط الذي يميل إلى الثبات والاستقرار، والذي أدى إلى قصور تلك القواعد عن ملاحقة التطور العلمي الحاصل، مما جعل بعض التشريعات الجزائية تحاول إعادة النظر في المبادئ القانونية المستقرة، واستحدثت قواعد ووسائل جديدة تواجه هذه المشكلات بهدف استثمار هذا التطور في خدمة العدالة الجزائية لدعم عملية المساعدة القضائية في المسائل الجنائية لمكافحة الجرائم الإلكترونية وتعد تقنية التحقيق والمحاكمة الجزائية عن بعد عبر وسيلة الVideoconference من أهم ثمار تلك الجهود، إذ تعتبر هذه الوسيلة خروجا عن الطابع التقليدي المفرط في ميدان التحقيق والمحاكمة الذي اتسم به مرفق العدالة الجزائية، إلى طابع أكثر ليونة وأوفر جهدا وأقل وقتا، حيث يترتب على تطبيقها امتداد النطاق الجغرافي لجلسات التحقيق أو المحاكمة الجزائية إلى أكثر من دولة، والتي يتحقق بموجبها مبدأ المواجهة بين أطراف الدعوى، دون حاجة إلى وجودهم الفعلي في مكان واحد، لهذا يطلق البعض على هذه الوسيلة تعبير "الجلسات التكنولوجية أو الإلكترونية أما الوسيلة الثانية فجاءت نتيجة حتمية لما أفرزه استفادة الإرهابيين من التكنولوجيا الحديثة ونظام البنوك والمصارف التي تيسر لهم انتقال الأموال المستخدمة لتسهيل تنفيذ عملياتهم من دولة إلى دولة، فكان لابد من وضع حد لتسهيل مهمة التحقيق معهم. الأمر الذي حملنا على دراسة "**المساعدة القضائية المتبادلة لمكافحة الجرائم الإلكترونية**" فنهجنا تقسيم عملنا إلى فصلين حيث حملنا الفصل الأول عنوان "**أحكام المساعدة القضائية المتبادلة لمكافحة الجرائم**

الإلكترونية" في حين حملنا الفصل الثاني عنوان **الجانب الموضوعي للإنابة القضائية والوسائل المستحدثة للتعاون الدولي في مكافحة الجريمة الإلكترونية.**

قائمة المصادر والمراجع

الإتفاقيات الدولية:

- اتفاقية الرياض للتعاون القضائي بين الدول العربية الوقعة بالرياض بتاريخ 23 جمادى الثاني عام 1403 الموافق ل 6 أبريل سنة 1983.المنشورة بالجريدة الرسمية الجزائرية عدد 11 بتاريخ 18 ذو القعدة عام 1421 هـ الموافق ل 12 فبراير سنة 2001 م .
- إتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية رقم 158 بتاريخ 2001/11/23. المنشورة على الموقع الإلكتروني:

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f8069

- الإتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة بتاريخ 1998/04/22 , الصادرة عن مجلسي وزراء الداخلية والعدل المنشورة على الموقع الإلكتروني :
  - http://www.madcour.com/LawsDocuments/LDOC-44-635278203054882024.pdf

الإتفاقيات باللغة الإنجليزية:

- the council of europe’s cyber –crmé convention and the need for International Regime to fight cyber crime-information- systems security- nov/ des 2002-vol 11 issue 55.
- European Convention on Mutual Assistance in Criminal Matters Strasbourg, 20. IV. 1959

القوانين والأوامر:

القوانين:

- قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950 منشور على الموقع الإلكتروني :

http://www.elawyerassistance.com/LegislationsPDF/Egypt/ProceduralLawInCriminalProceedingsAr.pdf

- قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة.

الأوامر :

- الأمر 66- 156 المؤرخ في 8 يونيو 1966 المتضمن لقانون العقوبات والمتمم لأمر رقم15- 19 المؤرخ في 30 ديسمبر 2015.

المذكرات التفسيرية :

- المذكرة التفسيرية لإتفاقية بودابست 7 نوفمبر 2001 باللغة الفرنسية.

Convention sur la cybercriminalité « STEno-185, Rapportexplicatif adopté le 8 novembre 2001, pp 80-83.

- المذكرة التفسيرية إتفاقية بودابست ستراسبورج 14 فبراير 2001 باللغة الأنجليزية.

Draft explantary memorandum to the draft convention on Cybercrime », Strasbourg 14 February 2001.

المسودات:

Counil of europe draft Convention on Cyber-Crime, October 2, 2000.

Counil of europe draft Convention on Cyber-Crime, November 26, 2000.

Counil of europe draft Convention on Cyber-Crime, Décembre 25, 2000.

الكتب باللغة العربية :

- إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة ، ط1 , 2007.
- الجوانب الموضوعية الإجرائية لجرائم المعلوماتية، د ط، دار النهضة العربية القاهرة، 2003.
- المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحرين على ضوء إتفاقية بودابست، ط2، دار النهضة العربية، القاهرة، 2013.
- جرائم المعلومات عابرة الحدود، ط1، دار النهضة العربية، القاهرة، 2007.
- د .إدوارد عيد، الإنابات والإعلانات القضائية، وفقاً للقانون الدولي الخاص واتفاقية الدول العربية في عام 1953 ، معهد البحوث والدراسات العربية، 1969.
- د. جميل عبد الباقي، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001 .
- د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992.
- د. جميل عبد الباقي الصغير، الجوانب إجرائية المتعقة بالأنترنت، ط 1، دار النهضة العربية القاهرة، 2001.
- د. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية عنوان 84 شارع زكرياء غنيم الإبراهيمية الإسكندرية، 2008.

- د. زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى عين مليلة، الجزائر، د ط، 2011 .
- د. طوبي ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، دار صادر للمنشورات بيروت، ط1، 2007.
- د. عادل يحيى، التحقيق والمحاكمة الجنائية عن بعد، دار النهضة العربية الطبعة الأولى، 2006.
- د. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية. 2006
- د .عكاشة محمد عبد العال، الإنابات القضائية في العلاقات الخاصة الدولية، دار المطبوعات الجامعية، الإسكندرية، 1994.
- د. علي حسن الطوالبة، التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية، دار العوم، بغداد، 2010.
- د. عماد طارق البشري، فكرة النظام العام في النظرية والتطبيق، المكتب الإسلامي للطباعة والنشر، 2005.
- د .عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دار النهضة العربية الطبعة الأولى، 2001.
- د. عمر سالم، المراقبة الإلكترونية، طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية 2000.
- د. محمد زكي أبو عامر وعلي عبد القادر القهوجي: قانون العقوبات القسم الخاص، دار النهضة العربية القاهرة، سنة 1993 .
- د. محمد فاضل، التعاون الدولي في مكافحة جرائم الأنترنت، ط1، دار الهدى البحرين، د س نشر.

- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، 2000 .
- د. هشام محمد فريد ، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة ، أسيوط ، ط1 ، 1994 .
- د. هلال عبد الله أحمد :
- د. هلالي عبد الله أحمد،إتفاقية بودابست مكافحة جرائم امعلومات معلقا، ط1، دار النهضة العربية، القاهرة، 2010.
- د.عزت مصطفي الدس وقي، شرح قانون الأحكام العسكرية، الكتاب الأول، قانون العقوبات، الطبعة الأولي، دار النهضة العربية، القاهرة، 1991 .

الكتب بالغة الإنجليزية:

- DUSSAIX (R.) , Qvelques problemes a l' application pratique du point de vue judiciaire de la convention Eouropeene relatifs d' entvaide judiciaire en matiere penal, in (problemes relatifs a l' application pratique de la convention europeene d' entraide judiciaire en matiere penal) Conseil de Eurpe, 1971 .
- HUET (A) , et KORING - JOULIN Renee, droit penal international, 1993 .
- Kelly Gable , Securing the Internet Against Cyber terrorism and Using Universal Jurisdiction as a Deterrent, Drexel university Earle Mack school of law, ,August 14, 2009, Working Paper Series.
- Pengelley, Pamela D. , A Compelling Situation: Enforcing American Letters Rogatory in Ontario. Canadian Bar Review, 2006.
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. Strasbourg, 8. XI. 2001
- Sossin, Lorne and Yetnikoff, Zimra, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources (Augus 5, 2007). Windsor Yearbook of Access to Justice, 2007.
- Sossin, Lorne and Yetnikoff, Zimra, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources, op. cit.
- Sossin, Lorne and Yetnikoff, Zimra, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources, op. cit.

- Tokson, Matthew J. , Virtual Confrontation: Is Videoconference Testimony by an Unavailable Witness Constitutional? (June 11, 2007). University of Chicago Law Review, Vol. 74, No. 4, 2007.
- Tokson, Matthew J. , Virtual Confrontation: Is Videoconference Testimony by an Unavailable Witness Constitutional?. Op. cit.
- White, Simone, European Constitution: What is New in the Area of Judicial Cooperation in Criminal Matters and Police Cooperation. Op, cit.
- White, Simone, European Constitution: What is New in the Area of Judicial Cooperation in Criminal Matters and Police Cooperation. Op, cit.

الرسائل العلمية :

– د. حازم مختار الحاروني، نطاق تطبيق القاضي الجنائي للقانون الأجنبي، رسالة دكتوراه، جامعة القاهرة، 1987.

– د. عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقاً لمعطيات التكنولوجيا المعاصرة، رسالة دكتوراه جامعة القاهرة، ص 2010.

– د. منيرة مسعود السبيعي، ضمانات المتهم أمام المحكمة الجنائية الدولية، رسالة دكتوراه مقدمة إلى جامعة القاهرة ،2010 .

– أ. سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة 2012 ـ 2013 .

– أ. معتوق عبد اللطيف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير في العلوم الجنائية 2011.

المداخلات:

- د. المقدم عز الدين عز الدين ،مداخلة بعنوان الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ملتقى حول الجرائم المعلوماتية 2015/11/01 في بسكرة.
- د. نشنـاش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، ملتقى حول الجرائم المعلوماتية، جامعة بسكرة 2015-2016.

المجلات :

- أ. حمد السمدان، النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوقي، الكويت، العدد 32, 1987 .
- د. لطفي جمعه ، دور الشرطة في حفظ السكينة والنظام، مجلة الأمن العام المصرية، العدد 24 , 2006.
- مجلة جامعة بابل ، العلوم الإنسانية ، المجلد ، 14العدد 6، 2007 .

المواقع الإلكترونية :

- Site Council of Europe : https://www.coe.int/en/web/portal/home
- موقع مذكور:

http://www.madcour.com

الفهرس

المحتوى	الصفحة
شكر وعرفان	/
المقدمة	1-
الفصل الأول: أحكام المساعدة القضائية المتبادلة لمكافحة الجرائم الإلكترونية	
تمهيد	07
المبحث الأول: مفهوم الجريمة الإلكترونية والأحكام والمبادىء العامة التي تحكم المساعدة القضائية المتبادلة لمكافحتها	09
المطلب الأول: مفهوم الجريمة الإلكترونية في التشريع الجزائري.	10
الفرع الأول : تعريف المشرع الجزائري للجريمة الإلكترونية	10
أولا : التعريف الفقهي	10
ثانيا: التعريف الأكاديمي	11
ثالثا: التعريف القانوني	11
الفرع الثاني: الطبيعة القانونية الخاصة للجريمة الإلكترونية	14
أولا: الطبيعة القانونية الخاصة للجريمة الإلكترونية	14
ثانيا:خصائص الجريمة الإلكترونية	17
الفرع الثالث : إتساع نطاق الجريمة الإلكترونية	20
أولا : الجرائم المرتكبة من طرف الشخص الطبيعي	20
ثانيا : جرائم الشخص المعنوي القانوني	22
المطلب الثاني : أحكام و مبادىء المساعدة القضائية المتبادلة	24
الفرع الاول: الاحكام العامة التي تحكم المساعدة القضائية المتبادلة	30
أولا : نص المادة 25: المساعدة القضائية المتبادلة	30
ثانيا : التعليقات	31
الفرع الثاني: الأحكام المتعلقة بالمعلومات التلقائية	36

أولا : نص المادة 26: المعلومات التلقائية	36
ثانيا: التعليقات	37
المبحث الثاني: الأحكام الإجرائية للمساعدة القضائية المتبادلة لمكافحة الجرائم الإلكترونية	39
المطلب الأول: إجراءات طلب المساعدة القضائية المتبادلة:	40
الفرع الأول: الإجراءات المتعلقة بطلبات المساعدة القضائية بين الأطراف في ظل غياب اتفاقية دولية مطبقة	40
أولا: نص المادة 27: المتعلقة بإجراءات طلبات المساعدة القضائية بين الأطراف في ظل غياب اتفاقية دولية مطبقة	41
ثانيا: التعليقات	43
الفرع الثاني : سرية المعلومات و تحديد أوجه إستخدامها	51
أولا : نص المادة 28: المتعلقة بالسرية وتحديد الاستخدام	51
ثانيا: التعليقات	52
المطلب الثاني: مجالات المساعدة المتبادلة لمواجهة جرائم المعلوماتية	55
الفرع الأول: المساعدة المتبادلة في مجال الإجراءات الوقتية العاجلة	55
أولا: التحفظ المعجل على البيانات المخزنة في الحاسوب	55
ثانيا : الكشف المعجل على حركة البيانات محل التحفظ	62
الفرع الثاني : المساعدة القضائية المتبادلة في مجال سلطات التحقيق	64
أولا : المساعدة المتبادلة استنادا إلى الدخول على البيانات المخزنة في الحاسوب	64
ثانيا: الدخول العابر للحدود إلى البيانات المخزنة في الحاسوب بالرضا أو عندما تكون معروضة للجمهور:	66
ثالثا: المساعدة المتبادلة استنادا إلى تجميع حركة البيانات في الزمن الفعلي	68
رابعا: المساعدة المتبادلة استنادا إلى مراقبة محتوى البيانات	70
خلاصة الفصل الأول	72

الفصل الثاني: الجانب الموضوعي للإنابة القضائية و الوسائل المستحدثة للتعاون الدولي في مكافحة الجريمة الإلكترونية "	
تمهيد	74
المبحث الأول: الإطار الموضوعي للإنابة القضائية	75
المطلب الأول: الإطار المفاهيمي للإنابة القضائية الدولية في المسائل الجنائية	76
الفرع الأول: تعريف الإنابة القضائية الدولية وأساسها القانوني	76
أولا : تعريف الإنابة القضائية الدولية في المسائل الجنائية:	76
ثانيا: الأساس القانوني للإنابة القضائية الدولية:	79
الفرع الثاني : شروط تطبيق الإنابة القضائية الدولية في المسائل الجنائية :	80
أولا: شروط الاختصاص:	80
ثانيا: عدم تعارض تنفيذ الإنابة مع النظام العام:	81
ثالثا: مراعاة الشروط الشكلية:	83
رابعا: ألا تكون الجريمة موضوع الإنابة من الجرائم المستبعدة من نطاق الإنابات القضائية الدولية	87
المطلب الثاني: دور الإنابات القضائية الدولية في التعاون الدولي لمكافحة الجرائم الإلكترونية	88
الفرع الأول: المسائل التي تتناولها الإنابة:	89
الفرع الثاني: حالات رفض الإنابة:	90
الفرع الثالث: إجراءات تنفيذ الإنابة:	91
الفرع الرابع: الأثر القانوني للإجراءات المنفذ بطريق الإنابة:	91
المبحث الثاني: الوسائل المستحدثة للتعاون الدولي لمكافحة الجريمة الإلكترونية	92
المطلب الأول :ماهية تقنية الـ Video conference وأهميتها	95
الفرع الأول :تعريف التحقيق الجنائي عن بعد Video conference	95

أولا: نظام الاتصال من نقطة إلى أخرى "punto – punto"	96
ثانيا: نظام السويتش أو المتحدث النشط " ou du parleur actif switching	96
ثالثا: نظام الحضور المستمر الثابت أو الموحد Continuous presence	97
رابعا: نظام الحضور المستمر المتقدم Continuous presence advanced"	97
الفرع الثاني: أهمية تقنية الـ Video Conference كوسيلة من وسائل التعاون الدولي في مكافحة الجريمة	98
أولا: سرعة الإجراءات وخفض النفقات	98
ثانيا: تعزيز الوسائل المتبعة في التعاون الدولي لمكافحة الجريمة:	100
ثالثا: حماية الشهود والمجني عليهم:	100
المطلب الثاني: قواعد التحقيق عن بعد عبر الـ video conference في البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية	102
الفرع الأول: شروط تطبيق تقنيةVIDEOCONFERENCE في البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية	103
أولا:عدم تعارض إستخدام تقنيةVIDEOCONFERENCE مع قانون الدولة المطلوب منها التنفيذ	104
ثانيا: توافر الوسائل والامكانيات التي تمكن الدولة المنفذة من استخدام هذه التقنية	105
ثالثا: حصر استخدام هذه التقنية في مجال سماع الشهود والخبراء	105
الفرع الثاني: إجراءات تطبيق تقنية الـ VIDEOCONFERENCE كوسيلة للتحقيق الجنائي في البروتوكول ألإضافي الثاني للإتفاقية ألأروبية للمساعدة القضائية في المسائل الجنائية	107
أولا : إجراءات السلطة القضائية في الدولة الطالبة	108

ثانيا : إجراءات السلطة القضائية في الدولة المطلوب منها التنفيذ:	109
الفرع الثالث: تطبيق تقنية التحقيق الجنائي عن بعد VIDEOCONFERENCE في مكافحة جرائم الإرهاب	110
خلاصة الفصل الثاني	113
الخاتمة	118-115
قائمة المصادر والمراجع	120-119