مبادئ استرشادية
في مجال مكافحة الإرهاب الإلكتروني

مقدمة

في إطار ما تشهده بلدان العالم المختلفة من أحداث إرهابية مؤسفة، يعتمد مرتكبوها بصفة رئيسية على استغلال تكنولوجيات المعلومات والاتصالات من أجل أغراض التخويف والإرهاب لتحقيق أهداف غير مشروعة؛ وفي إطار سعي العديد من دول العالم في الوقت الحاضر إلى صياغة مشروعات قوانين أو تعديل أخرى قائمة، وكذا إبرام اتفاقيات إقليمية ودولية فيما يتعلق بمكافحة الإرهاب الإلكتروني، تتقدم مصر بمجموعة من المبادئ الاسترشادية المقترحة التي يمكن للدول العربية الاستناد إليها في صياغة ميثاق عربي لمكافحة الإرهاب الإلكتروني.

تستمد مجموعة المبادئ الاسترشادية المقترحة مرجعيتها من دراسة وتحليل الجهود الدولية المتمثلة في الإستراتيجيات الوطنية والأنشطة والاتفاقيات الإقليمية والدولية فيما يتعلق بمكافحة الإرهاب الإلكتروني، والتي تأتي على رأسها اتفاقية بودابست حول الجرائم السيبرانية، وهي إحدى أقدم الاتفاقيات وأشملها من حيث عدد الأعضاء من دول العالم المختلفة، ومن حيث تضمنها القواعد الموضوعية للجرائم، وإجراءات التحقيق، وآليات التعاون الدولي في هذا الشأن، فضلاً عن اهتداء العديد من دول العالم بهذه الاتفاقية في صياغة القوانين الوطنية والتشريعات الخاصة بالجرائم السيبرانية.

كما تستند مجموعة المبادئ الاسترشادية المقترحة إلى اتفاقية الاتحاد الأفريقي الخاصة بالأمن السيبراني لعام ٢٠١٤، والتقرير الخاص بفريق الخبراء الحكوميين، المشكل منذ عام ٢٠٠٩ بقرار من الجمعية العامة للأمم المتحدة، والمعني بالتطورات في ميدان المعلومات السلكية واللاسلكية في سياق الأمن الدولي، فضلاً عن الاسترشاد بإستراتيجيات وقوانين مكافحة الإرهاب الإلكتروني في بعض الدول المتميزة في هذا المجال مثل المملكة المتحدة وفرنسا وغيرها من دول الاتحاد الأوروبي.

أولاً: الإطار العام

ينطلق الإطار العام لمجموعة المبادئ الاسترشادية المقترحة من ضرورة الالتزام بضمان وجود توازن ملائم بين حماية المصالح الوطنية والقومية ومكافحة الإرهاب الإلكتروني وبين احترام حقوق الإنسان الأساسية المنصوص عليها في الإعلان العالمي لحقوق الإنسان الذي تبنته الأمم المتحدة عام ١٩٤٨، والعهد الدولي للأمم المتحدة لعام ١٩٦٦ بشأن الحقوق المدنية والسياسية، والمعاهدات الدولية الأخرى واجبة التنفيذ بشأن حقوق الإنسان. كما يشمل الإطار العام إدراك المفاهيم الدولية ذات الصلة باستخدام تكنولوجيات المعلومات والاتصالات المستمدة من مبدأ سيادة الدول ومن ميثاق الأمم المتحدة، ومنها على سبيل المثال، لا الحصر، ما يلي:

❖ فيما ينعلق بحقوق الإنسان:

- التزام الدول، في سعيها لكفالة الاستخدام الآمن لتكنولوجيات المعلومات والاتصالات، بقراري لجنة حقوق الإنسان (A/HRC/RES/20/8)، (A/HRC/RES/26/13) (تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها)، وقراري الجمعية العامة (١٦٧ ٦٨) . (١٦٦ ٦٩) (الحق في الخصوصية في العصر الرقمي)، لضمان الاحترام الكامل لحقوق الإنسان، بما في ذلك الحق في حرية التعبير، وهو ما ينطوي على التزامات ومسؤوليات خاصة:
- حماية الدول لخصوصية الأفراد وبيانات الشركات بما يتماشى مع قوانينها الوطنية والتزاماتها الدولية:

❖ فيما يتعلق بسيادة الدول:

- السيطرة السيادية للدول على البنية التحتية لتكنولوجيا المعلومات والاتصالات التي تقع داخل إقليمها أو تحت سيطرتها، بما يتفق مع القانون الدولي الساري، والحق في صياغة سياساتها بحرية فيما يتعلق بالأنشطة المتصلة بتكنولوجيا المعلومات والاتصالات داخل إقليمها:
- مراعاة الدول، في استخدام تكنولوجيات المعلومات والاتصالات، لمبادئ القانون الدولي المعترف بها دولياً، بما في ذلك سيادة الدول والمساواة في السيادة وعدم التدخل في الشؤون الداخلية للدول الأخرى. وتنطبق الالتزامات القائمة بموجب القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات:

- عدم استخدام الدول لجهات أخرى لارتكاب أفعال غير مشروعة دوليا بالوكالة عنها، أو السماح باستخدام جهات من غير الدول إقليمها لاستعمال تكنولوجيات المعلومات والاتصالات في ارتكاب أفعال غير مشروعة دولياً؛
- اعتبار الاختراق المتعمد من جانب إحدى الدول للهياكل الأساسية لتكنولوجيا المعلومات والاتصالات الواقعة في إقليم دولة أخرى أو في إطار ولايتها القضائية انتهاكاً للسيادة، حتى وإن لم يصل إلى درجة استخدام القوة أو الهجوم المسلح.

❖ فيما يتعلق بالمسئولية الدولية:

- تنطبق بالكامل المبادئ التي تحكم المسؤولية الدولية للدول على بيئة تكنولوجيا المعلومات والاتصالات، بما في ذلك عدم سماح الدول باستخدام إقليمها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيات المعلومات والاتصالات؛
- عدم قيام الدولة بأنشطة إلكترونية الهدف منها إلحاق الضرر بالبنية التحتية الحيوية المعتمدة علي تكنولوجيا المعلومات والاتصالات في دولة أخري أو إعاقة استخدام وتشغيل البنية التحتية الحيوية بأي شكل آخر، أو دعم هذه الأنشطة عن علم؛
- اتخاذ الدول التدابير المناسبة لحماية البنية التحتية الحرجة والحيوية من التهديدات المتصلة بتكنولوجيا المعلومات والاتصالات وفقاً، في جملة أمور، لقرار الجمعية العامة (١٩٩ ٥٨ /٢٠٠٣) المعنون "إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية البنية التحتية الحيوية للمعلومات"، والالتزامات الدولية الأخرى ذات الصلة:

العامة (١٩٩ ٥٨ /٢٠٠٣) المعنون "إرساء ثقافة عالمية لأمن الفضاء ت"، والالتزامات الدولية الأخرى ذات الصلة:

كنولوجيا المعلومات والاتصالات المستخدمة لأغراض كيدية، والامتناع المعلومات والاتصالات وعن التدخل في سلسلة الإمداد بتكنولوجيا

عدي للطوارئ الحاسوبية، وفرق الاستجابة لحوادث أمن الفضاء طلاع الدول بأنشطة يراد بها منع الفرق الوطنية للتصدي للطوارئ اء الإلكتروني من التصدي للحوادث المتصلة بتكنولوجيا المعلومات وعدم استخدام الدولة لأي من هذه الفرق للقيام بتصرفات كيدية في

والاتصالات وفقاً، في جملة أمور، لقرار الج الحاسوبي وحماية البنية التحتية الحيوية للد

- منع الدول لانتشار الأدوات والتقنيات المتطر عن دس خصائص خفية مضرة في تكنو المعلومات والاتصالات لأغراض كيدية؛
- دعم وتيسير الدول للتعاون فيما بين فرز الإلكتروني، والهيئات المناسبة الأخرى وعد الحاسوبية وفرق الاستجابة لحوادث أمن والاتصالات، وعدم دعم تلك الأنشطة عن مجال تكنولوجيا المعلومات والاتصالات.

❖ فيما يتعلق بالتعاون الدولي:

- تجنب الدول، تماشياً مع التزاماتها بموجب ميثاق الأمم المتحدة، القيام بأعمال تمثل تهديداً للسلام والأمن الدوليين، والتعاون في وضع وتطبيق تدابير لزيادة الاستقرار والأمن في استخدام تكنولوجيات المعلومات والاتصالات، ومنع الممارسات المتعارف على أنها ضارة في مجال تكنولوجيا المعلومات والاتصالات أو التي قد تشكل تهديدا للسلام والأمن الدوليين؛
- اتباع الدول لأفضل سبل التعاون على تبادل المعلومات وتبادل المساعدة ومحاكمة المسئولين عن استخدام تكنولوجيات المعلومات والاتصالات لأغراض إرهابية وإجرامية، وتنفيذ تدابير تعاونية أخرى للتصدي لهذه التهديدات.
- استجابة الدولة لطلبات المساعدة المناسبة التي تقدمها دولة أخرى تكون هياكلها الأساسية الحيوية معرضة لأعمال كيدية تستخدم فيها تكنولوجيا المعلومات والاتصالات، وفي التخفيف من آثار أنشطة استخدام تكنولوجيا المعلومات والاتصالات لأغراض كيدية تستهدف البنية التحتية الحيوية لدولة أخرى انطلاقا من إقليمها، مع مراعاة السيادة على النحو الواجب؛

❖ فيما يتعلق بتسوية المنازعات:

- امتثال الدول، في استخدام تكنولوجيات المعلومات والاتصالات، لالتزاماتها بموجب ميثاق الأمم المتحدة فيما يتعلق بتسوية المنازعات بالوسائل السلمية والامتناع عن التهديد باستعمال القوة أو استعمالها. وإذا ما قررت دولة ما ممارسة حقها الطبيعي في الدفاع عن النفس وفقا للمادة ٥١ من ميثاق الأمم المتحدة، يبلغ مجلس الأمن فوراً بالتدابير المتخذة، ويجب أن تكون هذه التدابير ضرورية ومتناسبة، وفقا للمبادئ القانونية الدولية التي تسترشد بها الدول في تصرفاتها، مثل الإنسانية والضرورة والتناسب والتمييز، وأن تنفذ بطريقة تتماشى مع مقاصد الأمم المتحدة؛

ثانياً: المبادئ الإجرائية

تتمثل المبادئ الإجرائية فيما ينبغي للدول اتخاذه من إجراءات وتدابير في سبيل مكافحة الإرهاب الإلكتروني والقضاء عليه، وتشمل هذه المبادئ ما يلي:

- للسلطات القضائية، في إطار تحقيقات قضائية، أن تلزم مزود خدمات الشبكة، بجمع وتسجيل وتقديم مضمون المعلومات المنقولة بواسطة نظام معلوماتي خلال زمن الإرسال الحقيقي، وبتزويد أجهزة التحقيق بمعلومات حركة البيانات وبيانات التعريف الشخصية حول أصحاب المواقع الإلكترونية التي يستضيفونها، أو أن يساعدها في ذلك. يلتزم مزوّد خدمات الشبكة بالسرية المهنية فيما يخص التعليمات التي ينفّذها في هذا السياق، وكذلك فيما يخص المعلومات..
- إعطاء الصلاحية لمحاكم البلد الذي نشأ منه الإرهاب الإلكتروني ومكان وجود المرتكب (محل وإقامة المجرم)، وإن كانت آثار الفعل قد لحقت بنظام معلوماتي خارج البلد، وذلك نظراً لسهولة السير بالتحقيق وإمكانية توقيف الفاعل.
- صلاحية الأدلة الرقمية لإثبات الإرهاب الإلكتروني وغيرها من الجرائم أمام القضاء. ويعود للمحكمة تقدير قيمة الدليل الرقمي وحجيته في الإثبات، ويجب أن لا يكون قد تعرض لأي تغيير خلال ضبطه وحفظه.
- إلزام مزودي خدمات الشبكة، المتعلّقة بحفظ مضمون المعلومات أو معلومات حركة البيانات وتقديمها إلى القضاء، وتطبيق هذه الالتزامات على أي مزوّد خدمات للشبكة، له على أراضي الدولة مركز إدارة فعلي أو محل إقامة يمارس فيه نشاطاً اقتصادياً راهناً، وذلك بصرف النظر عن جنسيته، وعن مكان تأسيسه، ومقرّه الرئيسي إذا كان شخصاً اعتبارياً، وعن المكان الذي توجد فيه التجهيزات التقنية التي يستخدمها.
- للسلطات القضائية الحق أن تدخل إلى أي نظام معلوماتي أو جزء منه، أو تفتش عليه، وكذلك على البيانات المخزنة فيه أو على أي دعامة إلكترونية. إذا كانت البيانات مخزّنة في نظام معلوماتي آخر موجود على أراضي الدولة، ويمكن الوصول إليها من النظام المعلوماتي الأول المقرر تفتيشه، فيمكن توسيع نطاق التفتيش بسرعة ليشمل النظام المعلوماتي الثاني. وبهذا الخصوص، يمكن ضبط نظام معلوماتي أو جزء منه، أو دعامة إلكترونية، وحفظ نسخة من البيانات المعلوماتية. واتخاذ التدابير لحفظ سلامة البيانات المعلوماتية، ومنع أي مستخدم من الوصول إلى بيانات النظام المعلوماتي.
- للسلطات القضائية أن تلزم أي شخص، على علم ودراية بطرق عمل نظام معلوماتي أو التدابير المطبقة لحماية البيانات المعلوماتية المخزنة، بأن يقدم المعلومات المطلوبة من أجل تمكينها من الوصول إلى البيانات المعلوماتية المخزنة.
- تكون محاكم الدول مختصة إذا وقع الإرهاب الإلكتروني على أراضيها، أو على مركب يرفع علمها، أو على متن طائرة مسجلة وفق قوانينها؛ وإذا وقع الإرهاب الإلكتروني من قبل أحد مواطنيها، وذلك إذا كان معاقباً عليه جزائياً في البلد الذي ارتكبت فيه، أو إذا كان الإرهاب الإلكتروني لا يقع ضمن الاختصاص الإقليمي لأية دولة؛ وإذا وجد فاعل الإرهاب الإلكتروني على أراضيها ولا يمكن استرداده لمحاكمته في دولة أخرى بسبب جنسيته.

ثالثاً: التدابير الوقائية

- نشر الأفكار المضادة للإرهاب على المواقع المختلفة ونشر التوعية في المدارس والجامعات والسجون بمخاطر التشدد بصفة عامة.
- توقيع اتفاقات ثنائية وإقليمية مع مزودي خدمة الإنترنت وشركات الاتصالات العالمية وشركات التواصل الاجتماعي بحيث تتمكن الأخيرة بمقتضاها من إخطار أجهزة الأمن لإلغاء حساب أي مشترك للاشتباه فيه بإرسال رسائل إلكترونية يمكن أن تكون مرتبطة بمخططات إرهابية. وبحيث تلتزم شركات الاتصالات بتسليم معلومات للشرطة حول هوية الأشخاص الذين يستخدمون الحواسيب أو الهواتف الجوالة.
- صياغة قوانين وطنية تمكن السلطات المختصة من غلق المواقع الإرهابية أو تلك التي تحض على العنف والتطرف.
- تبني إجراءات جديدة حول عنوان برتوكول الإنترنت، لتحتفظ الشركات المزودة للخدمة بالبيانات التي تربط بين الأجهزة والمستخدمين لتشمل توقيت المكالمات ومدتها ومكانها، ومتسلمي الرسائل على مواقع التواصل الاجتماعي والبريد الإلكتروني، على أن يتم استصدار أمر قضائي قبل الاطلاع على هذه البيانات.

رابعاً: مبادئ التعاون الدولي

ينبغي للدول أن تنظر في إمكانية وضع تدابير من شأنها تعزيز التعاون الثنائي ودون الإقليمي والإقليمي والمتعدد الأطراف. ويمكن أن تشمل هذه التدابير الاتفاق الطوعي فيما بين الدول. وفيما يلي مجموعة من مبادئ التعاون الإقليمي والدولي:

- تتعاون الدولة مع الدول الأخرى، بناءً على اتفاقيات موقعة معها أو استناداً إلى مبدأ المعاملة بالمثل، في سياق التحقيقات القضائية المتعلقة بالإرهاب الإلكتروني أو لضبط أدلة معلوماتية متعلقة به.
- للسلطات القضائية، بناءً على اتفاق ثنائي أو متعدد الأطراف، أن ترسل إلى سلطات قضائية في دولة أخرى معلومات ناتجة عن تحقيقات قضائية قد تساعدها في مباشرة تحقيقات قضائية خاصة بها. يمكن اشتراط أن تبقى هذه المعلومات سرية أو ألاّ تستعمل إلا وفق شروط معينة.

- للسلطات القضائية أن تأمر بحفظ البيانات المخزنة في نظام معلوماتي. والتي قد تستعمل كدليل في تحقيقات قضائية. ويمكن أن يتم ذلك بموجب طلب مقدم من سلطات قضائية في دولة أخرى، بناء على اتفاق ثنائي أو متعدد الأطراف. على أن تتقدم بطلب لاحق لضبط هذه البيانات ولتسلمها.
- للسلطات القضائية أن تأمر بضبط بيانات محفوظة في نظام معلوماتي من أجل تسليمها إلى سلطات قضائية في دولة أخرى بموجب طلب مساعدة، بناءً على اتفاق ثنائي أو متعدد الأطراف.
- تعزيز آليات التعاون مع الوكالات المعنية لمواجهة الحوادث الأمنية ذات الصلة بتكنولوجيا المعلومات والاتصالات، ووضع آليات تقنية وقانونية ودبلوماسية إضافية للتعامل مع الطلبات المتصلة بالبنية التحتية لتكنولوجيا المعلومات والاتصالات، بما في ذلك النظر في إمكانية تبادل الموظفين في مجالات من قبيل مواجهة الحوادث وإنفاذ القانون، حسب الاقتضاء، وتشجيع عمليات التبادل فيما بين المؤسسات البحثية والمؤسسات الأكاديمية؛
- تعزيز التعاون بسبل منها إنشاء جهات تنسيق لتبادل المعلومات المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات لأغراض إرهابية، ولتقديم المساعدة في التحقيقات؛
- توسيع نطاق الممارسات ودعمها في مجال التعاون فيما بين فرق التصدي للطوارئ الحاسوبية. من قبيل تبادل المعلومات بشأن مكامن الضعف، وأنماط الهجمات، وأفضل الممارسات من أجل التخفيف من آثار الهجمات، بما في ذلك من خلال تنسيق الاستجابات، وتنظيم العمليات، ودعم معالجة الحوادث المتصلة بتكنولوجيا المعلومات والاتصالات، وتعزيز التعاون على الصعيدين الإقليمي والقطاعي؛
- قيام الدول، بطريقة تتماشى مع التزاماتها بالقوانين الوطنية والدولية، بالتعاون مع طلبات المساعدة الواردة من الدول الأخرى بشأن التحقيق في الجرائم المتصلة بتكنولوجيات المعلومات والاتصالات، أو استخدام تلك التكنولوجيات لأغراض إرهابية، أو التخفيف من الآثار الناجمة عن أنشطة استخدامها لأغراض كيدية انطلاقاً من إقليمها.

ملاحظات الهيئة على مسودة مجموعة المبادئ الاسترشادية في مكافحة الارهاب الالكتروني التي أعدتها وزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية

أولاً: ركزت المبادئ على جانب واحد من توصية المكتب التنفيذي لمجلس الوزراء العرب للاتصالات وتقنية المعلومات، حيث تم اختزال المشروع في مكافحة الارهاب الإلكتروني فحسب، دون تناول الموضوع الأصلي للتوصية وهو الآليات المطلوبة للعمل على موضوعات الأمن السيبراني والاستخدام الضار لتطبيقات شبكة الانترنت. وهذا ادى إلى تداخل المبادئ بشكل عام في موضوعات تخص السلطات القضائية وليس السلطات التنفيذية للاتصالات والمعلومات، ومنها على سبيل المثال ما يتعلق بسيادة الدول، أو تسوية النزاعات، أو تبادل المعلومات، أو محاكمة المسؤولين عن استخدام تكنولوجيا المعلومات لأغراض ارهابية، أو طلب المساعدة القانونية .

ثانياً: صدر عن مجلسي وزراء العدل والداخلية العرب بالقاهرة في ٤/٢٢/ ١٩٩٨ الاتفاقية العربية لمكافحة الإرهاب التي دخلت حيز النفاذ في ١٩٩٩/٥/٧م وهي اتفاقية شاملة لم تأت لتعالج نوعاً واحداً من الإرهاب وإنما جاءت بأحكام عامة وضعت أساساً للتعاون لمكافحة الإرهاب بمفهومه العام، ومنها ما يدخل تحته بعض جوانب المشروع محل الدارسة، مثل (وسائل منع الجريمة الإرهابية كالحيلولة دون اتخاذ الدول الأطراف أراضيها مسرحاً لتخطيط او تنظيم او تنفيذ الجرائم الإرهابية او الشروع او الاشتراك فيها بأية صورة من الصور)، وايضاً (التعاون بين الدول كتبادل المعلومات حول وسائل الاتصال والدعاية التي تستخدمها الجماعات الإرهابية)، إضافة إلى (آليات تنفيذ القانون كتسليم المطلوبين ومحاكمتهم وحماية الخبراء).

ثالثاً: صدر عن مجلس وزراء العدل العرب في دورته العاشرة برقم ٤٩٥- د١٩٠ وتاريخ ٢٠٠٣/١٠/٨م، ومجلس وزراء الداخلية العرب برقم ٤١٧- د٢١ في العام ٢٠٠٤م (القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها)، والذي تم التطرق فيه للجماعات الإرهابية التي تتخذ من شبكة الإنترنت وسيلة للقيام بجرائمها، حيث ورد في المادة (٢١) منه (كل من أنشأ او نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها او تمويلها او نشر أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن ....)، كما ورد في المادة (٢٢) من ذات القانون (كل من دخل عمداً وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة او اقتصادها الوطني يعاقب بالسجن ....)، وهذا القانون يغطي مجموعة من المبادئ الواردة في المشروع المقدم من جمهورية مصر العربية.

رابعاً: قد يكون من المناسب أن يتم زيادة تفعيل الجوانب الفنية في المبادئ ودورها في الأمن السيبراني ومكافحة الإرهاب الإلكتروني، وتفعيل الأنظمة المساندة لمكافحة الجريمة الإلكترونية والإرهاب على شبكة الإنترنت، كتطوير أنظمة السجلات الإلكترونية والتوقيع الإلكتروني للأفراد والشركات، وتصنيف واعتماد المنشآت وانظمة التمويل والتجارة، وتطوير القوى العاملة الوطنية المتخصصة في مجال أمن المعلومات ورفع كفاءتها، وتأهيل الموظفين المكلفين بجميع المهام ذات العلاقة، من خلال تطوير مهاراتهم ومعرفتهم في مجال الاتصالات وتقنية المعلومات، وتحديث أساليب البحث والتحري عن الأدلة في مثل هذا النوع من الجرائم، ليتسنى لهم رصد هذه الأنماط السلوكية المستجدة، والذي من شأنه الحفاظ على الأمن وحماية موارد الاتصالات وتقنية المعلومات، والبنى التحية المحلية الخاصة بها.

خامساً: ورد ضمن هذه المبادئ ما يتعلق بالتعاون الدولي بشأن التحقيق في هذه الجرائم وتبادل المعلومات حولها، والأصل في هذا التعاون خضوعه للاتفاقيات الدولية أو الإقليمية أو الثنائية، و قد جرى تنظيم هذه الممارسة في المملكة بموجب قرار مجلس الوزراء الموقر ذي الرقم (٧٨) والتاريخ ١٤٣٣/٠٣/٢١هـ القاضي بتشكيل لجنة دائمة باسم (اللجنة الدائمة لطلبات المساعدة القانونية المتبادلة)، والتي تتكون من الجهات المنصوص عليها في القرار لتنفيذ طلبات المساعدة الواردة من الدول الأجنبية وطلبات المساعدة القانونية الصادرة من المملكة إلى تلك الدول في جميع الجرائم، وجعل اختصاصها الأصيل هو تلقي طلبات المساعدة القانونية وإرسالها، واعتبار اللجنة هي الجهة المخولة الوحيدة بهذه المهمة.

- انتهى-

EMBASSY OF REPUBLIC OF IRAQ
The Permanent Mission
to the League of Arab States
Cairo

سفارة جمهورية العراق
المندوبية الدائمة لدى جامعة الدول العربية
القاهرة

العدد: 248 ف/29/ج/3
التاريخ: 2016/5/11

05696
12 MAY 2016

تهدي مندوبية جمهورية العراق الدائمة لدى جامعة الدول العربية أطيب تحياتها الى الأمانة العامة لجامعة الدول العربية – القطاع الاقتصادي- إدارة تنمية الاتصالات وتقنية المعلومات، وبالاشارة الى مذكرتها المرقمة 5/1746 في 2016/3/24 تتشرف ان توضح لها انه بعد اطلاع الجهات المعنية في جمهورية العراق على المبادئ الاسترشادية المقترحة التي اعدتها وزارة الاتصالات وتقنية المعلومات في جمهورية مصر العربية الشقيقة بينت بان معظم ما جاء فيها يتماشى مع المبادئ الدولية والاساليب المتبعة في مكافحة الجرائم (السبرانية) وتمثل اساساً ذا اعتبار في مكافحة الارهاب الالكتروني، ولكن معظم ما جاء فيها، لاسيما حفظ وتبادل الادلة الالكترونية وفقرة الاتفاقيات المتبادلة مع الشركات المحلية في بند الاجراءات الوقائية لم يتم استكمالها محلياً في الوقت الحالي، لذا فانها تبين ان التزام جمهورية العراق النهائي يكون بعد استكمال القوانين والقدرات المحلية لتحقيق الرؤى الوطنية في الاتفاقية، وكما هو مبين في الملاحظات الآتية:

- ما يتعلق بالمسؤولية الدولية تقترح اعادة صياغة الفقرة الخاصة بـ (دعم وتيسير الدول للتعاون فيما بين فرق التصدي للطوارئ الحاسوبية وفرق الاستجابة لحوادث أمن الفضاء الالكتروني ...) لتكون على الوجه الآتي: (الدعم باتفاق الدول وفق مذكرات تفاهم او اتفاقيات ثنائية أو متعددة).
- ما يتعلق بالتعاون الدولي: اعادة صياغة الفقرة الخاصة بـ (استجابة الدولة لطلبات المساعدة المناسبة التي تقدمها دولة اخرى ..) لتكون: (من خلال مذكرة تفاهم أو اتفاقيات ثنائية او متعددة " جماعية").
- ما يتعلق بالمبادئ الاجرائية:

1- فقرة (للسلطات القضائية في اطار تحقيقات ..) تكون: (وفقاً للقانون الوطني).

2- فقرة (اعطاء الصلاحيات لمحاكم البلد الذي نشأ من الإرهاب الالكتروني ...) لتكون (وفقاً للقانون الوطني).

3- تكون جميع الفقرات المتبقية، من ثانياً (المبادئ الاجرائية) وفقاً للقانون الوطني.

9, Mohamed Mathor St., Zamalek - Cairo
Tel.: (202) 27358087 - (202) 27352633
Fax. (202) 27365075
Website : mofamission.gov.iq Email: caiemb@gov.iq

٩ شارع محمد مظهر - الزمالك - القاهرة
تليفون : ٢٧٣٥٨٠٨٧ (٢٠٢) - ٢٧٣٥٢٦٣٣ (٢٠٢)
فاكس : ٢٧٣٦٥٠٧٥ (٢٠٢)

EMBASSY OF REPUBLIC OF IRAQ
The Permanent Mission
to the League of Arab States
Cairo

سفارة جمهورية العراق
المندوبية الدائمة لدى جامعة الدول العربية
القاهرة

العدد: 2486/29/ج/3
التاريخ: 2016/5/11

- ما يتعلق بالتدابير الوقائية: تعديل فقرة (صياغة القوانين الوطنية ..) لتكون: (صياغة القوانين الوطنية تمكن السلطات المختصة من متابعة النشاط والمحتوى او غلق المواقع الإرهابية ...).

تغتنم المندوبية الدائمة هذه المناسبة لتعرب للامانة العامة الموقرة عن فائق تقديرها واحترامها.

الأمانة العامة لجامعة الدول العربية – القطاع الاقتصادي- إدارة تنمية الاتصالات وتقنية المعلومات،

9. Mohamed Mazhar St., Zamalek - Cairo
Tel.: (202) 27358087 - (202) 27352633
Fax: (202) 27365075

٩ شارع محمد مظهر - الزمالك - القاهرة
تليفون : ٢٧٣٥٨٠٨٧ (٢٠٢) - ٢٧٣٥٢٦٣٣ (٢٠٢)
فاكس : ٢٧٣٦٥٠٧٥ (٢٠٢)

Website : malamission.gov.iq Email: caiemb@gov.iq

مرئيات الوزارة حول مجموعة المبادئ الاسترشادية في مجال مكافحة الإرهاب الإلكتروني

١- من المآخذ الجوهرية على المبادئ الاسترشادية ضرورة امتثال الدول في حالة ممارسة الدول لحقها الطبيعي في الدفاع عن النفس وفقاً للمادة (٥١) من ميثاق الأمم المتحدة ، إلا أن ما قد يؤخذ على هذه المسألة هو أن المادة (٥١) من الميثاق تحدثت عن الاعتداء المسلح وليس قضية الجرائم المعلوماتية (الهادئة) كما يسميها البعض.

٢- نظراً لمرور إجراءات التعاون القضائي بالطرق الدبلوماسية ما يجعلها تتسم بالبطء وكثرة الشكليات، وهو ما يتعارض مع الجرائم المعلوماتية التي تتميز بسرعة عبور وتبادل المعلومات من خلال شبكتها. إلا أن المبادئ لم تعط حلولاً أو آلية للتغلب على البطء في الإجراءات كالاتصال المباشر بين السلطات القضائية في الدولتين . والذي يعد أحد أهم صور التعاون الدولي في المساعدة القضائية. فإعطاء الحق للسلطات القضائية في البلد الذي نشأ منه الإرهاب وكذلك السلطات القضائية في البلد الذي وقعت فيه النتيجة. يعني الأخذ بمبدأ الإقليمية. والذي قد يتعارض مع فكرة الجرائم العابرة للحدود خاصة في ظل غياب التعاون الدولي.

٣- في سياق التعاون مع مزودي الخدمة، ينبغي الإشارة إلى أنه لا تستلزم بعض السياسات الجنائية لوقمع الاتفاقيات ومذكرات التفاهم مع مزودي الخدمة المحليين أو شركات ومؤسسات التواصل الاجتماعي خاصة إن تعلق الأمر بالأمن القومي. إذ يمكن التغلب على هذه المسألة من خلال التنسيق المباشر مع مزود الخدمة المحلي والشركة الأم للتطبيق

٤- إذا كان التعاون الدولي هو السبيل الوحيد لمكافحة الجرائم الإلكترونية. فإن هذا التعاون يقضي التخفيف من الفوارق بين الأنظمة الإجرائية. لأن التباعد بين هذه الأنظمة يجعل المجرمين يبحثون عن الأنظمة القانونية الأكثر تسامحاً.