الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة يحيى فارس بالمدية

كليـــة الحقــوق

قسم الحقوق

نــدوة علميــة حــول الأمــن الإلكتــرونــي

يوم 03 مـــــاي 2016

اللقب: حرز الله.

الاسم: كريم.

الوظيفة: أستاذ مؤقت بكلية الحقوق والعلوم السياسية بجامعة البليدة 02.

الرتبة العلمية: دكتور في تخصص القانون الخاص.

الهاتف: 05.40.00.35.45.

البريد الإلكتروني: harzallah34@hotmail.fr.

عنوان المداخلة: التعاون الدولي في مجال مكافحة الجريمة الالكترونية.

مقدمــة

ظهرت في الآونة الأخيرة تقنيات علمية، هذه التقنيات الغرض منها هو تلبية حاجة الإنسان في أسرع وقت ممكن، ومحاولة تقريب المسافات بينه وبين الآخرين، فالعالم يعيش عصر ثورة المعلومات تلك الثورة التي تؤثر في حياة البشر جميعاً، وستكون المكاسب والفوائد وكذا المشكلات والمخاطر المترتبة على هذه الثورة الوشيكة في مجال المعلومات كبيرة.

وقد كرست الأعمال القانونية الدولية حق الاتصال والحصول على المعلومات وتداولها، وأكدت على أهمية ضمان ممارسته.

فقد نص القرار 59 الصادر عن الأمم المتحدة في 14 ديسمبر 1946 على أن "حرية الاستعلام هي حق أساسي للإنسان، وهي حجر الزواية لكل الحريات التي كرست الأمم المتحدة نفسها للدفاع عنها، وحرية الاستعلام تشمل جمع ونقل ونشر المعلومات في كل مكان دون عقبات".[1]

كما نصت المادة 19 من الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 10 ديسمبر 1948 على أن "لكل فرد الحق في حرية الرأي والتعبير ويشمل هذا الحق حرية اعتناق الآراء دون تدخل واستقاء وتلقي وإذاعة الأنباء والأفكار دون تقيد بالحدود الجغرافية وبأية وسيلة كانت".[2]

وأخيراً نصت المادة 19 من العهد الدولي للحقوق المدنية والسياسية الصادر عن الأمم المتحدة في 16 ديسمبر 1966 على أن "2- لكل فرد الحق في حرية التعبير وهذا الحق يشمل حرية البحث عن المعلومات أو الأفكار من أي نوع واستلامها ونقلها بغض النظر عن الحدود، وذلك إما شفاهة أو كتابة أو طباعة، وسواء كان ذلك في قالب فني أو بأية وسيلة أخرى يختارها".[3]

وتنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في

حركة المعلومات بأنه بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الإجرامي في دولة أخرى.

وتستلزم مثل هذه الجرائم وجود تعاون دولي فعال والذي يعتبر ضرورياً من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول وينشأ حتماً عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقنية نظم المعلومات ما يعرف بالمعلومات المختبئة والذي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات.

وفي مجال الإجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاماً من أجل التسيير دون عقبة لطلب المساعدة القانونية الوطنية، أنه قد تلتمس إحدى الدول المساعدة القضائية من دول أخرى بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون طبقاً لقوانينها الخاصة.

المبحث الأول: التدابير الواجب مباشرتها على المستوى الوطني.

يمكن تقسيم هذه التدابير إلى نوعين إحداهما تدابير موضوعية والأخرى إجرائية، وسنخصص لكل منهما مطلباً مستقلاً وذلك على النحو التالي: [4]

المطلب الأول: التدابير الموضوعية.

ينبغي على الدول أن تتبع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من مخاطر الجريمة المعلوماتية وذلك من خلال تبني التشريعات الملائمة لمواجهة الخطورة المتمثلة في إمكان استخدام شبكات الكمبيوتر والمعلومات الإلكترونية في ارتكاب أفعال إجرامية مع إمكانية تخزين ونقل الدليل المتعلق بمثل هذه الأفعال عبر تلك الشبكات.

لذا من الأهمية بمكان مباشرة التدابير الآتية:

أولاً: يجب على كافة الدول أن تتبنى التدابير التشريعية وغيرها من التدابير اللازمة لإدراك عملية الدخول غير المشروع إلى سائر أو جزء من أجزاء نظام الكمبيوتر كجريمة جنائية وفقاً لأحكام قوانينها الوطنية إذا ما ارتكبت هذه الأفعال بصورة عمدية ويجوز لأي دولة أن تحدد من

بين متطلبات ارتكاب الجريمة أن تكون ارتكابها من خلال اختراق تدابير الأمن أو بيئة الحصول على بيانات الكمبيوتر.

ثانياً: ينبغي على أن تتبنى التدابير التشريعية وغيرها من التدابير اللازمة لإدراك أعمال الاعتراض دون حق والتي تتم بأساليب فنية كعمليات نقل الكمبيوتر إلى أو من خلال حاسب آلي آخر وكذا الإشارات الإلكترومغناطيسية الصادرة من أحد نظم المعلومات والتي تحمل مثل تلك البيانات واعتبارها جريمة جنائية لأحكام قوانينها الوطنية إذا ما ارتكبت بصورة عمدية.

ثالثاً: يجب على الدول أن تتبنى التدابير التشريعية التشريعية اللازمة لإدراك أعمال الإضرار أو المحو أو الإتلاف أو التعديل أو الإعاقة التي تستهدف بيانات الحاسب الآلي بدون وجه حق واعتبارها جريمة إذا ما ارتكبت بصورة عمدية. (5)

رابعاً: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراج أعمال الإعاقة الخطرة دون وجه حق بوظائف نظام الكمبيوتر من خلال إدخال أو نقل أو الإضرار أو محو أو إتلاف أو تعديل أو إعاقة بيانات الكمبيوتر وإدراكها باعتبارها جريمة جنائية إذا ارتكبت بصفة عمدية.

خامساً: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإمكانية مساءلة الأشخاص المعنوية جنائياً عن الجرائم الناشئة عن نظم المعلومات وذلك في الأحوال التي يؤدي فيها قصور الإشراف أو الرقابة من قبل الشخص الطبيعية إلى تسهيل ارتكابها.

المطلب الثاني: التدابير الإجرائية.

وتتمثل هذه التدابير على النحو التالي:

أولاً: يجب على الدول أن تتخذ التدابير التشريعية التي تخولها سلطة تفتيش:

أ- أحد أنظمة الكمبيوتر أو جزء منه وبيانات الكمبيوتر المختزنة به.

ب- أحد الوسائط التي قد تكون بيانات الكمبيوتر مختزنة به، وذلك في أراضيها أو في أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق.

ثانياً: يجب على الدول ن تتخذ التدابير التشريعية اللازمة لتخويل سلطاتها المعنية في إصدار الأمر لأي شخص سواء كان متواجداً في إقليمها في أي مكان آخر عليه سلطاتها السيادية لكي يقدم أي بيانات محددة واقعة تحت سيطرته ومخزنة في أحد أنظمة الكمبيوتر أو أحد الوسائط المستخدمة في تخزين البيانات وذلك بالصورة التي تطلبها تلك السلطات لأغراض التحقيق. (6)

ثالثاً: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد نظم الكمبيوتر وذلك لأغراض التحقيقات وذلك إذا تبين أنها معرضة بصفة خاصة للفقد والتعديل.

رابعاً: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإجبار الشخص الذي تتخذ حياله إجراءات الحفظ المشار إليها سلفاً على الاحتفاظ بسرية الإجراءات لمدة محددة من الزمن وفقاً للإطار الذي يسمح به القانون الوضعي.

خامساً: يجب على الدول أن تتخذ التدابير التشريعية اللازمة التي تكفل حفظ السريع لتلك البيانات الخاصة بعملية النقل وبغض النظر إذا كان مقدم الخدمة واحدة أو أكثر ممن شاركوا في عملية نقل هذا الاتصال.

سادساً: يجب على الدول أن تتخذ التدابير التشريعية اللازمة لمد اختصاصها القضائي على أي من الجرائم المشار إليها إذا ما ارتكبت

أ- بصورة كلية أو جزئية على أراضيها أو على متن باخرة أو طائرة أو قمر صناعي يحمل علمها أو مسجل لديها.

ب-من قبل أحد مواطنيها إذا كانت الجريمة من الجرائم المعاقب عليها وفقاً لأحكام القانون الجنائي الساري في محل ارتكابه أو إذا كانت الجريمة قد ارتكبت خارج الاختصاص الإقليمي لأي دولة. (7)

المبحث الثاني: التدابير الواجب مباشرتها على المستوى الدولي.

ويمكن تقسيم هذه التدبير إلى نوعين، الأولى تتعلق بالتسليم والثاني يتعلق بالمعونة المتبادلة.

المطلب الأول: تسليم المجرم المعلوماتي.

يجب على الدول أن تتعاون بعضها مع بعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب تسليم مرتكبيها وذلك وفقاً لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها:

أولاً: أن يكون الدخول إلى النظام أو البيانات قد تم بدون وجه حق وبنية الاخلال بسرية البيانات أو إعاقة نظام الكمبيوتر.

ثانياً: أن تبرم الدول فيما بينها اتفاقية تسليم مرتكبي الجرائم المعلوماتية.

ثالثاً: إذا ما رفض طلب التسليم الصادر في شأن مرتكبي إحدى الجرائم المعلوماتية بناء على جنسية الشخص المراد تسليمه نظراً لأن طرف المدعي يعتبر أنه يختص قضائياً بالجرمية محل الإدعاء، يقوم الطرف المدعي عليه بتقديم القضية إلى سلطاته بغرض السير في الدعوى الجنائية وعلى أن يبلغ الطرف المدعي بالنتائج المترتبة عليه. (8)

المطلب الثاني: المعونة المتبادلة

وتتمثل المعونة المتبادلة في الإجراءات التالية:

أولاً: يجب على الدول أن تقدم لبعضها البعض المعونة المتبادل وذلك بأكبر قدر ممكن لأغراض التحقيق والإجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي.

ثانياً: يجب على الدول أن تقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الالكتروني، بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصادقة.

ثالثاً: تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة.

رابعاً: في الأحوال التي يسمح فيها للطرف المدعي عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة، يعتبر هذا الشرط محل اعتبار وبغض النظر عما إذا كانت قوانين هذه الدولة تضع الجريمة في نطاق ذات تصنيف آخر.

خامساً: تحدد كل دولة سلطة مركزية تنهض بالمسؤولين إرسال طلبات المعونة المتابدلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

سادساً: تنفذ طلبات المعونة المتبادلة وفقاً للإجراءات التي تحددها الطرف المدعي فما عدى الأحوال التي لا تتصل فيها تلك الإجراءات مع أحكام القانون السائد بالدولة المعدي عليه.

سابعاً: يجوز للدولة المدعي عليه أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام بما ورد بالطلب قد يخل بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

ثامناً: يجوز للدولة المدعي عليها تأجيل التصرف في الطلب إذا كان هذا التصرف سيخل بالتحقيقات أو إجراءات الإدعاء أو الإجراءات الجنائية التي تباشر بمعرفة السلطات المعنية.

تاسعاً: يجب على الدول المدعي عليه أن تخطر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة فإذا ما رفض الطلب أو تم تأجيله يجب تقديم الأسباب إلى الرفض أو التأجيل.

عاشراً: يجوز للدولة المدعية أن تطلب من الدولة المدعي عليه أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب، فإذا لم يكن بمقدور الدولة المدعية عليها الوفاء بمتطلبات سرية الطلب فيجب عليها إخطار الدولة المدعية بذلك وعلى الأخيرة في هذه الحالة تحديد ما إذا كان سينفذ الطلب من عدمه. (9)

الحادي عشر: يجوز في حالة الاستعجال إرسال طلبات المعونة المتبادلة مباشرة إلى السلطات القضائية بما فيها النيابة العامة لدى الدولة المدعية عليها وفي مثل الحالة يجب إرسال نسخة بنفس الطلب إلى السلطة المركزية القائمة لدى الدولة المدعي عليها. (10)

وفي الأخير نقول أنه ما من دولة يمكنها بنجاح مجابهة هذا التحدي في مواجهة هذه الأنماط المستحدثة من الجرائم ومنها الجرائم الناشئة عن استخدام شبكة الإنترنت بمفردها، ولا مفر من مواصلة أجهزة تطبيق القانون في أنحاء العالم وتطوير القدرة على التعاون الدولي في المجال المعلومات، ولا مفر للدول المتقدمة من مساعدة الدول النامية لتعزيز مؤسساتها المتخصصة بالتحري والتحقيق والمحاكمة، من خلال توفير الوسائل والإمكانيات وسائر أنواع المعونة التقنية.

التهميـش:

1- القرار 59 الصادر عن الأمم المتحدة في 1946/12/14.
2- المادة 19 من الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 1948/12/10.
3- المادة 19 من العهد الدولي للحقوق المدنية والسياسة الصادر عن الأمم المتحدة في 1966/12/16.
4- أ. محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة المعلوماتية والإنترنت، الطبعة الأولى، القاهرة، 2012، ص 386.
5- المرجع نفسه، ص 386.
6- أ. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، الطبعة الأولى، الإسكندرية، 2011، ص 419.
7- أ. محمد صادق إسماعيل، المرجع السابق، ص 389.
8- أ. أمير فرج يوسف، المرجع السابق، ص 445.
9- الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، بحث فقهي مقارن، دار الفكر الجامعي، الإسكندرية، مصر، الطبعة الأولى، 2011، ص 83.
10- أ. محمد صادق إسماعيل، المرجع السابق، ص 392.

المراجـــع:

1- أ. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، الطبعة الأولى، الإسكندرية، 2011.
2- الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، بحث فقهي مقارن، دار الفكر الجامعي، الإسكندرية، مصر، الطبعة الأولى، 2011.

3- أ. محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة المعلوماتية والإنترنت، الطبعة الأولى، القاهرة، 2012.

4- القرار 59 الصادر عن الأمم المتحدة في 1946/12/14.

5- الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 1948/12/10.

6- العهد الدولي للحقوق المدنية والسياسة الصادر عن الأمم المتحدة في 1966/12/16.