AALCO/54/BEIJING/2015/SD/S1
للاستخدام الرسمي فقط

المنظمة الاستشارية القانونية الآسيوية الأفريقية

القانون الدولي في الفضاء الإلكتروني

تم إعدادها من قبل:
أمانة آلكو
29 سي، ريزال مارج،
دبلوماتيك انكليف، تشاناكيابوري،
نيودلهي – 110021
الهند

القانون الدولي في الفضاء الإلكتروني

جدول المحتويات

القانون الدولي في الفضاء الإلكتروني

أولاً. مقدمة

أ.تمهيد

1. مع حلول عصر المعلومات، أصبح الفضاء الإلكتروني مجالاً جديداً للتفاعل البشري وجزءاً لا يتجزأ من التحليل الدولي المعاصر. يتكون الطابع الهجين التكنولوجي من بنية افتراضية عبر الحدود الوطنية، مع معلومات متجولة من خلال كابلات تحت البحر وبين الأجهزة الفعلية الموجودة داخل وخارج أراضي الدول القومية. في الوقت الحاضر ثلث سكان العالم لديهم إذن بالدخول إلى الإنترنت. حوّل وجود الإنترنت في كل مكان الطريقة التي نتواصل بها والبحث عن المعلومات وبدّل بشكل يتعذر إلغاؤه الطريقة التي نقوم بها بأعمالنا اليومية. كما جاء بفرصٍ غير مسبوقة للترقية الإنسانية. وتشير التقديرات إلى أن الإنترنت يمثل أكثر من 20 في المئة من نمو الناتج المحلي الإجمالي للإقتصادات الكبرى في العالم خلال الفترة بين عامي 2008-12. لا حاجة لتفصيل الفوائد التي تمتد لما هو أبعد من النمو الإقتصادي- كتحسين فرص الحصول على التعليم، الحد من الفقر، وزيادة فرص الحصول على المعلومات وهلم جرا.

2. وخلافاً للمجالات الإستراتيجية الأخرى- أرض، بحر، هواء وفضاء- الفضاء الإلكتروني هو إفتراضي، وبالتالي يمكن تغيير هيكله كثيراً. هذه الميزة الفريدة للفضاء الإلكتروني تشكل تحدياً كبيراً لأية محاولات لتنظيمهم داخل الحدود الإقليمية للدول القومية. في الواقع، هناك خلاف كبير سواء إلى أي درجة يمكن السيطرة على الفضاء الإلكتروني بشكل عام وحول ما إذا كانت القيادة هي أمر ممكن، ليس فقط من قبل الدول ولكن من أي جهة منظمة بشكل تسلسلي. ويناقش العديد بأن عدم التحفظ، الحد اللأدنى والتخطيط الغير مركزي للفضاء الإلكتروني، يحكم من قبل شبكة من الجهات بما في ذلك الشركات الخاصة والهيئات غير الحكومية بشكل أساسي التي تقوض القيادة من قبل الدول وتحد من نقاط السيطرة. يجادل آخرون، بأن قيادة الدولة هي ممكنة ويتزايد تنظيم الفضاء الإلكتروني من خلال سلطة الدولة كما تظهر العديد من الأمثلة. وكثيراً ما تم تأطير نظام إدارة الإنترنت الحالي "لنموذج صاحب المصلحة المتعددة'، الذي يتكون من الحكومات والشركات الخاصة والمنظمات غير الحكومية دون وجود التسلسل الهرمي المتأصل بين الثلاثة.[1] وأُتفق أيضاً على نموذج صاحب المصلحة المتعددة بأنه 'افتتاح للدولة بالإعتماد على المنظمات العالمية للمشاركة من قبل "أصحاب المصلحة" بالإضافة إلى الحكومات.

3. على أية حال، في تدريب نموذج صاحب المصلحة المتعدد النموذجي المثالي يبرز الشذوذ في قيادة الحكومة الأمريكية التاريخية والعلاقة التعاقدية المستمرة بين قسمها التجاري ومؤسسة الإنترنت المخصصة للأسماء والأرقام (ICANN). وكانت بعض الدول الأعضاء لآلكو مدركة لهذه الحقيقة والتي كانت تتناقش لإنشاء نموذج مركزي للأمم المتحدة لإدارة الإنترنت مع الإتحاد الدولي للاتصالات (ITU) في مركزها. ويبدو أن هذا احتمال بعيد، كما هو

[1] ميلتون مولر ل.، الشبكات والدول: السياسات العالمية لحوكمة الإنترنت 7 (2010).

واضح من نتيجة مؤتمر المندوبين المفوضين لعام 2014 للإتحاد الدولي للإتصالات الذي اختتم مؤخراً، حيث ساد موقف الدول المتقدمة.[2]

4. ومع ذلك، من وجهة نظر سيادة القانون الدولي، الحداثة لما يسمى بـ "النطاق الخامس" لا تمنعه من القواعد والمبادئ التقليدية للقانون الدولي. المبدأ الأساسي للقانون الدولي، أي أن سيادة الدولة ليست استثناء، وترتبط ارتباطاً وثيقاً مع إدارة الإنترنت. وعلى الرغم من امتلاك الفضاء الإلكتروني العديد من ميزات "التداولات العالمية"، فإن مزاولة الدولة تعطي أدلة وافرة لتمرين الدول لسلطتها القضائية لتنظيم سلوك مواطنيها في الفضاء الإلكتروني. في الآونة الأخيرة، ثبتت ممارسة السيادة في العديد من المحافل الدولية بشكلٍ جيد. ومع ذلك، هذا يستلزم مساوات الإلتزامات للإحترام ودعم الحريات الأساسية لمواطنيها في الفضاء الإلكتروني.

5. الأمن الإلكتروني هو مجال آخر والذي تتم مناقشته جيداً في الخطاب القانوني الدولي.[3] يشير الأمن الإلكتروني على نطاق واسع قدرة الدولة على حماية نفسها ومؤسساتها ضد تهديدات الفضاء الإلكترونية. التحدي الرئيسي للحكومات هو التأكد من أن مؤسساتها وشعبها محمي في المقام الأول من الهجمات الإلكترونية والتجسس على شبكة الإنترنت. تستثمر الحكومات موارد كبيرة لتحسين قدرات الفضاء الإلكتروني وتعزيز دفاعاتها ضد الهجمات الإلكترونية القريبة الحدوث على الأصول الهامة.[4] الكشوفات الأخيرة التي أدلى بها إدوارد سنودن، تحول محللي الكمبيوتر لمبلغين، عارضين مدى التجسس الإلكتروني الذي يستهدف الوظائف السيادية للعديد من الدول. إضافةً إلى ذلك، ازدهر ارتكاب الجرائم الإلكترونية من قبل الجهات الفاعلة غير الحكومية بما في ذلك السرقة المالية وغيرها من الجرائم العابرة للحدود التي تهدد الأمن القومي والصحة المالية. ويقدر تقرير الضرر السنوي للإقتصاد العالمي بـ 445 بليون دولار.[5]

ب. المداولات في الدورة السنوية الثالثة والخمسين

6. هذا التمهيد العريض هو نفس السبب الذي دفع جمهورية الصين الشعبية لأن تقترح "القانون الدولي في الفضاء الإلكتروني" كبند من بنود جدول الأعمال للتداول في دورته السنوية الثالثة والخمسين لآلكو الذي عقد في طهران في عام 2014، وقُبل بتوافق الآراء. قُدم البيان من قبل الدول الأعضاء التابعين لجمهورية - الصين الشعبية واليابان وجمهورية إيران الإسلامية ونيجيريا. سلط وفد جمهورية الصين الشعبية، في بيانه الضوء على القضايا التالية المتعلقة بالقانون الدولي في الفضاء الإلكتروني: (1) أهمية مبادئ السيادة وعدم التدخل في الفضاء الإلكتروني، والحاجة إلى تحقيق التوازن بين الحق في الكلام والتعبير والأمن الإلكتروني، (2) الإستخدام السلمي للفضاء

---

[2] رؤية مونيكا إيرمرت، مؤتمر المندوبين المفوضين للاتحاد: حوكمة الإنترنت الدبلوماسية على العرض، متوفرة على http://www.ip-watch.org/2014/11/05/itu-plenipotentiary-conference-internet-governance-diplomacy-on-display

[3] [3] انظر عموماً ماري إيلين أوكونيل، الأمن الإلكتروني والقانون الدولي، تشاتام هاوس (2012)، وهي متاحة على العنوان التالي: http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf

[4] انظر عموماً بييرلويجي باغانيني ، احذر من عسكرة الفضاء الافتراضي، http://www.foxnews.com/tech/2014/12/18/beware-militarization-cyberspace/

[5] http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

الإلكتروني ومنع العسكرة الإلكترونية، (3) القواعد الدولية لمكافحة الجريمة الإلكترونية و(4) تطوير وتطبيق القواعد الدولية للفضاء الإلكتروني وأهمية الأمم المتحدة باعتبارها أفضل منتدى لمناقشة وتسوية تلك المعايير والقواعد. بينما رحب مندوب اليابان باقتراح تطوير اتفاقية الجريمة الإلكترونية في الأمم المتحدة، كما حذر من ازدواجية الجهود التي قد تؤدي إلى خلق قواعد مشابهه جداً لإتفاقية بودابست. وأشار مندوب جمهورية إيران الإسلامية لطبيعة نفاذ الهجمات الإلكترونية مبطلاً بعض المبادئ الراسخة للقانون الدولي بما في ذلك حرمة السيادة والسلامة الإقليمية في العالم الحقيقي. وأعرب مندوب نيجيريا عن مخاوف بلاده فيما يتعلق بالخصوصية واستخدام الإنترنت لتعزيز الإرهاب.

7. اعتمد القرار (AALCO/RES/53/S17) وفقاً للمداولات التي أقرت بالحاجة لتطوير وتطبيق القواعد الدولية المتسقة للفضاء الإلكتروني، ودعت الدول الأعضاء للإتصال والتعاون بينهم على هذا الموضوع.

ج. قضايا للمناقشة المركزة في الدورة السنوية الرابعة والخمسين لآلكو

أولاً. ضرورة وملاءمة نموذج الحكم المركزي للأمم المتحدة للفضاء الإلكتروني.

ثانياً. أهمية الموازنة بين الحقوق السيادية للدول والحريات الأساسية للكلام والتعبير لمواطنيها في الفضاء الإلكتروني.

ثالثاً. أهمية القواعد القائمة للحرب (بنظرية الحرب العادلة وقانون الحرب) في تنظيم سلوك الدولة في الحرب الإلكترونية.

رابعاً. ازدهار الجرائم الإلكترونية العابرة للحدود الوطنية والحاجة إلى معاهدة متعددة الأطراف لمنع تصعيدها بشكل فعال.

ثانياً. حوكمة الإنترنت، الحقوق والواجبات السيادية

8. حوكمة الإنترنت، بشكل عام، هي تطوير وتطبيق المبادئ المشتركة والمعايير والقواعد وإجراءات اتخاذ القرارات ووضع البرامج التي تحدد شكل تطور واستخدام الإنترنت . تنص دي ناردیس(DeNardis) على أن "حوكمة الإنترنت عموماً تشير إلى السياسة و قضايا التنسيق التقنية المتصلة مع تبادل المعلومات عبر الإنترنت".[6] طورت ونشرت شبكة الإنترنت في مراحلها المبكرة دون توجيه من العمليات الحكومية الدولية، مثل الإتحاد الدولي للإتصالات، ودون إنشاء قواعد القانون الدولي. أخيراً، كما ذكر في وقت سابق، تطورت حوكمة الإنترنت من خلال عمليات أصحاب المصلحة المتعددة الذين تعاونوا مع الجهات الحكومية وغير الحكومية على إدارة المهام الفنية والتشغيلية، مثل توحيد بروتوكولات الإتصال وإدارة الأسماء والعناوين الرقمية على شبكة الإنترنت.

9. عندما اعتمد أعضاء الإتحاد الدولي للإتصالات أنظمة الإتصالات الدولية (ITRs) في عام 1988، كان الإنترنت لم يصبح بعد شبكة اتصالات عالمية، اجتماعية، اقتصادية، وظاهرة سياسية. ركزت أنظمة الإتصالات الدولية على الربط البيني والتشغيل البيني لخدمات الإتصال الحالية، واستبدال الأنظمة البرقية وأنظمة الهاتف باعتماد

[6] لورا ديناردیس، الناهضة في ميدان حوكمة الإنترنت، سلسلة مقالة عمل مشروع مجتمع المعلومات يالي (17 أيلول/سبتمبر 2010).

الإتحاد الدولي للإتصال في عام 1973. شملت أنظمة الإتصالات الدولية المبادئ العامة بدلاً من القواعد التفصيلية التي شكلت إطاراً مرناً عملياً للتعاون الدولي. كما توسعت شبكة الإنترنت، وعبرت العديد من الدول عن مخاوف بشأن إدارة أصحاب المصلحة المتعددة، بما في ذلك أنه أعطى الولايات المتحدة الأمريكية الهيمنة على الإنترنت وتحديثاته. سعت هذه الدول لتحقيق حوكمة الإنترنت في العمليات الحكومية الدولية والقانون الدولي.[7] في الفترة التي تسبق المرحلة الأولى من القمة العالمية لمجتمع المعلومات (WSIS) في كانون الأول/ ديسمبر 2003، الصين، وبدعم من البلدان النامية، اقترحت إنشاء منظمة دولية للإنترنت واعتماد معاهدة الإنترنت.

10. أدت الخلافات في قمة مجتمع المعلومات الدولي في عام 2003 بين أنصار نهج أصحاب المصلحة المتعددة والمؤيدين أكثر للسيطرة الحكومية والحكومة الدولية إلى أن يُطلب من الأمين العام للأمم المتحدة إلى إنشاء فريق للعمل المعني بحوكمة الإنترنت (WGIG) في عام 2004. عندما واجهت نفس الخلافات، أوصى فريق العمل المعني بحوكمة الإنترنت بإنشاء منتدى حوكمة الإنترنت (IGF). أُقيمت المرحلة الثانية من القمة العالمية في عام 2005، منتدى حوكمة الإنترنت بمثابة منتدى للنقاش بين أصحاب المصلحة المتعددة مع عدم اتخاذ سلطة قرار. قرر الإتحاد الدولي للإتصالات في عام 2006 مراجعة أنظمة الإتصالات الدولية في ظل بيئة اتصالات دولية متغيرة، وعقد المؤتمر العالمي للاتصالات الدولية في عام 2012 لتعديل أنظمة الاتصالات الدولية.[8]

أ. المؤتمر العالمي للإتصالات الدولية (*WCIT 2012*)

11. في الفترة التي سبقت المؤتمر العالمي للإتصالات الدولية 12، جادل أنصار نموذج أصحاب المصلحة المتعددة أن الإتحاد الدولي للإتصالات وبعض أعضاء الإتحاد كانوا يستخدمون المؤتمر العالمي للإتصالات الدولية 12، لجعل حوكمة الإنترنت تحت السيطرة الحكومية والمراقبة الحكومية الدولية، مع نتائج وخيمة للإبتكار، التجارة، التنمية، الديمقراطية، وحقوق الإنسان. وعلى الرغم من ذكر الأمين العام حمدون طورا للإتحاد الدولي للإتصالات أن المؤتمر العالمي للإتصالات الدولية لم يخاطب حوكمة الإنترنت، تضمنت المقترحات المقدمة من أعضاء الإتحاد التغييرات التي تركز على الإنترنت وكيفية التحكم به. كمثال، اقترحت روسيا مادة جديدة على شبكة الإنترنت، والتي تضمنت بنداً يستهدف نموذج أصحاب المصلحة المتعددة: يجب على الدول الأعضاء أن يكون لهم حقوق متساوية في حوكمة الإنترنت، بما في ذلك ما يتعلق بالتخصيص والتعيين وإصلاح ترقيم الإنترنت، التسمية، المعالجة وتحديد الموارد ودعم التشغيل وتطوير البنية التحتية الأساسية للإنترنت. وتضمنت التعديلات الأخرى المقترحة تمويل الإتصالات عبر الإنترنت، التعامل مع البريد المزعج، ومعالجة أمن الشبكة والكمبيوتر.

12. أنتهى المؤتمر العالمي للإتصالات الدولية 12 دون اتفاق. مارس 144 وفداً حقوق التصويت في المؤتمر العالمي للإتصالات الدولية 12، وقّع تسعة وثمانون على تعديل أنظمة الإتصالات الدولية، بما في ذلك العديد من البلدان الأفريقية، البرازيل، الصين، إندونيسيا، إيران، وروسيا، في حين أن خمسة وخمسين لم يوقعوا، بما في ذلك

---

[7] د.بي فيدلر، حوكمة الإنترنت والقانون الدولي: جدل بخصوص تنقيح أنظمة الاتصالات الدولية، رؤى آسيل (ASIL)، نسخة.17، الإصدار .6 (2013).

[8] اي.دي

أستراليا، وأعضاء الاتحاد الأوروبي، كندا، اليابان، والولايات المتحدة. قبل انتهاء المفاوضات، أعلنت الولايات المتحدة عن معارضتها، بناءً على ما يتضمنه تعديل أنظمة الإتصالات الدولية المتعلقة بالإنترنت. على الرغم من أن الأمين العام للاتحاد قد وضح أن المؤتمر العالمي للإتصالات الدولية من شأنه أن يأخذ القرارات بتوافق الآراء، أثبتت المعارضة النشطة من قبل الدول البارزة عدم وجود إجماع تاركاً الاتحاد الدولي للاتصالات مع المعاهدة المعدلة لكل من دعم وعارض من قبل الدول القوية ونسبة كبيرة من عضويتها. [9]

ب. التطورات الاحقة

13. في 7 تشرين الأول/ أكتوبر عام 2013، صدر بيان مونتيفيديو حول مستقبل تعاون الإنترنت من قبل قادة عدد من المنظمات العاملة في مجال تنسيق البنية التحتية التقنية العالمية للإنترنت، والمعروفة بشكل عام ب "أي*" أو مجموعة ("أي-ستار"). من بين أمور أخرى، "أعرب عن قلقه الشديد من تقويض الثقة والأمانة لمستخدمي الإنترنت عالمياً بسبب ما كشف عنه مؤخراً من انتشار للتنصت والمراقبة" و"دعا إلى الإسراع في عولمة وظائف مؤسسة الإنترنت للأسماء والأرقام المخصصة والأرقام المخصصة لإنترنت السلطة، نحو بيئة يمكن فيها جمع أصحاب المصلحة، بما في ذلك جميع الحكومات، والمشاركة على أساس المساواة ". ينظر لهذه الرغبة المتزايدة للإبتعاد عن النهج المركزي للولايات المتحدة كرد فعل لفضيحة المراقبة المستمرة لوكالة الأمن القومي الأمريكية . تم التوقيع على البيان الصادر عن رؤساء مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN)، و حملة هندسة الإنترنت ، لجنة تشييد بناء الإنترنت، اتحاد شبكة الويب العالمية، جمعية الإنترنت، وخمسة سجلات بعنوان الإنترنت الإقليمي (مركز شبكة المعلومات الإفريقي، السجل الأمريكي لأرقام الإنترنت، مركز شبكة معلومات آسيا والمحيط الهادئ، سجل عناوين الإنترنت لأمريكا اللاتينية ومنطقة البحر الكاريبي، و مركز تنسيق الشبكة الأوروبية لنظام شبكة الإنترنت).

14. في نيسان / أبريل عام 2014، اجتمع أصحاب المصلحة المتعددة العالميين حول مستقبل حوكمة الإنترنت (GMMFIG)، وقد استضيف المؤتمر من قبل لجنة أصحاب المصلحة المتعددة رفيعة المستوى، والتي تتألف من ممثلين وزاريين لأثني عشر بلداً (الأرجنتين ، البرازيل ، فرنسا ، غانا ، ألمانيا ، الهند ، اندونيسيا ، جنوب أفريقيا ، جمهورية كوريا ، تونس ، تركيا ، و الولايات المتحدة أمريكا) و 12 عضواً من المجتمع الدولي لأصحاب المصلحة المتعددة. أنتج الإجتماع بياناً غير ملزم لصالح اتخاذ القرارات على أساس توافق الآراء. حيث أنه يعكس التسوية التي لم تدن بشدة المراقبة الجماعية أو تضمين عبارة "حياد الانترنت"، على الرغم من الدعم الأولي لذلك من البرازيل. ويقول القرار النهائي لمؤسسة الإنترنت للأرقام والأسماء المخصصة يجب أن تكون تحت رقابة دولية بحلول أيلول/ سبتمبر عام 2015. [10]

---

[9] للإطلاع على المناقشة المفصلة، انظر
http://www.itu.int/en/wcit-12/Pages/default.aspx

[10] انظر فيليب كوروين، شبكة منديال بيان أصحاب المصلحة المتعددة يختتم العمل الأول عام 2014 حوكمة الإنترنت تريفيكتا ، وهي متاحة على

15. كانت هناك أقلية من الحكومات، بما في ذلك روسيا والصين وإيران والهند، غير راضية عن القرار النهائي وأرادت إدارة متعددة الأطراف للإنترنت، بدلاً من إدارة أوسع لأصحاب المصلحة المتعددين.ومن شأن ذلك أن يعطي الحكومات بشكل أساسي سلطة اتخاذ القرار، على سبيل المثال عن طريق الأمم المتحدة ، وتكون أكثر عرضة لتشجيع الدول الفردية للسيطرة على المجالات الوطنية داخل الحدائق المسورة التي يمكن رصدها بسهولة أكبر وتصفيتها، كما هو الحال مع شبكات الهاتف التي تتأثر بالإتحاد الدولي للإتصالات .

ج. مؤتمر مفوض الإتحاد الدولي للإتصالات عام 2014

16. في مؤتمر مفوض الإتحاد الدولي للإتصالات عام 2014، الذي عقد في بوسان، جمهورية كوريا، كان من المتوقع أن الإتحاد الدولي للإتصالات سيفوض مع دور أعظم في إدارة الإنترنت. على أية حال، فإن هذا لم يتحقق. أصدر المؤتمر مجموعة من القرارات ذات الصلة بالإنترنت التي تحافظ على تقييد الوضع الراهن لمشاركة الإتحاد الدولي للإتصالات.[11] في مناقشات مطولة ومكثفة وجد الفريق العامل التابع للجلسة العامة تسوية لما يشبه بالأحرى مقترحات مبالغ فيها من نهايات مختلفة.على سبيل المثال، اقترحت روسيا التي شرعت في الإتحاد الدولي للإتصالات تخصيص بروتوكول الإنترنت (IP) للعناوين، والتي هي وظيفة تؤدى بالفعل من قبل المنظمات غير الحكومية الدولية الأخرى. قدمت الدول العربية المقترحات التي من شأنها أن تعزز دور الحكومات في اتخاذ القرارات حول الإنترنت، ومن شأنها أن تعطي الإتحاد الدولي للإتصالات دورا في تطوير الأطر القانونية والسياسية لمكافحة المراقبة الدولية غير المشروعة على الإنترنت. وقدمت البرازيل للإتحاد الدولي للإتصالات مقترحات للعمل على قضايا الخاصة على شبكة الإنترنت.[12]

17. ووفقاً للتقارير، انطلقت المناقشة الأكبر خلال اقتراح من الهند التي تؤيد إجراء سلسلة من الدراسات السارية المفعول لدفع تمركز عمل الشبكات.[13] اكتشفت إحدى الدراسات أن "التطوير لتسمية وترقيم النظام من تسمية وترقيم مختلف البلدان يتميز بالسهولة" دراسة آخرى "يوصى النظام الذي يضمن فعالية حركة المنشأ وينوي الإنهاء في نفس البلد بالبقاء داخل البلد". كانت هذه الأفكار بمثابة إعادة تصميم الشبكات القائمة بالإتصالات أو البروتوكولات " و " فوض للإتحاد الدولي للإتصالات بالتوسع"، الذي تمت معارضته بشكل كبير من قبل الدول المتقدمة. بالإضافة إلى المقترحات الهندية اقتراح من المجموعة العربية والذي طالب الإتحاد الدولي للإتصالات البدء بمناقشة صك قانوني

---

http://www.circleid.com/posts/20140504_netmundial_multistakeholder_statement_concludes_act_one_of_2014

[11] مونيكا إيرمرت، مؤتمر المندوبين المفوضين للاتحاد: عرض حوكمة الإنترنت الدبلوماسية ، متوفرة على http://www.ip-watch.org/2014/11/05/itu-plenipotentiary-conference-internet-governance-diplomacy-on-display/

[12] لمزيد من التفاصيل، انظر http://www.itu.int/en/plenipotentiary/2014/Pages/default.aspx

[13] ملاحظة سوبرا 10.

لحماية مستخدمي الإنترنت من المراقبة الجماعية من قبل وكالات الإستخبارات، ربما يمكن أن ينظر لكليهما كتداعي من اكشافات إدوارد سنودن.

18. تم حذف جميع المواقف المتطرفة في المفاوضات. قادت الحكومة التفويض الأكبر للإتحاد الدولي للإتصالات في حوكمة الإنترنت المعارض على نطاق واسع بواسطة الشمال العالمي، مؤكدةً رفضها المستمر لإتخاذ أي إعادة ترتيب أساسية للنطاق القائم. ولكن أُعطي الضوء الأخضر "لمواصلة القيام بأنشطة على الإنترنت الدولي والمتعلقة بقضايا السياسة العامة، ضمن تفويض الإتحاد الدولي للإتصالات بالتعاون والاشتراك مع المنظمات ذات الصلة وأصحاب المصالح، حسب الإقتضاء، مع إيلاء اهتمام خاص لإحتياجات البلدان النامية" كما هو معروض في تحديث القرار 102. أيضا وافقت اثنتين من التكتلات الإقليمية الكبرى - البلدان الصناعية والنامية - على الإعتراف بأن الحكومات، أيضاً، هي "أصحاب المصلحة" و "تستمر في لعب دور مهم جداً في توسيع وتطوير شبكة الإنترنت، على سبيل المثال من خلال الإستثمارات في البنى التحتية و الخدمات".

19. قرار جديد مخصص لتعزيز تبادلات الإنترنت والمبادئ التوجيهية كان من الممكن الإتفاق عليهم، وقد تم سحب المقترحات من قبل الأرجنتين وأمريكا اللاتينية للتبادل لأجل تضمين المراجع القوية عن عمل الاتحاد الدولي للاتصالات في بورصات الإنترنت في قرارات الإنترنت المحدثة 101 و 102. قُدمت السيادة على نطاقات المستوى الأعلى لرموز البلد (ccTLDs) صراحةً استناداً إلى النص من برنامج عمل تونس من مؤتمر القمة العالمي 2003-2005 لمجتمع المعلومات (WSIS). كان هذا الإصلاح مطلوباً من قبل أولئك الذين لا يطمأنون تماماً لهيئة الإنترنت التي مقرها الولايات المتحدة المخصصة للأسماء والأرقام (ICANN)، والتي لديها رقابة تقنية على نطاق نظام الأسماء.

20. الاجتماع الثابت المقبل لمناقشة قضايا التكنولوجيا والإنترنت في الأمم المتحدة هواجتماع على مستوى عالٍ خاص بالجمعية العامة في كانون الاول/ ديسمبر عام 2015. وسيستعرض هذا الاجتماع عقداً من الأنشطة، منذ انعقاد القمة العالمية لمجتمع المعلومات في تونس في عام 2005.

د. السيادة الإلكترونية ومسؤولية الدولة

21. تتوقف المناظرات المؤيدة لمزيد من سيطرة الدولة على حوكمة الإنترنت بشكل أساسي على توسيع سيادة الدولة على الفضاء الإلكتروني. بغض النظر عن النظريات المختلفة للوظيفة القانونية للأرض، هناك اتفاق واسع النطاق أنه وفقاً لمبدأ السيادة الإقليمية تمارس الدولة السلطة الكاملة والحصرية على أراضيها. ماكس هوبر، في تحكيم جوائز جزيرة بالماس، قد أكد هذا المبدأ العام على النحو التالي: "السيادة في العلاقات بين الدول تعني الاستقلال.

الاستقلال فيما يتعلق بجزء من العالم هو حق الممارسة في تلك المسألة بوظائف الدولة، إلى التفرد من أي دول أخرى".[14]

22. وفقاً لمحكمة العدل الدولية، "بين الدول المستقلة، احترام السيادة الإقليمية هو الركيزة الأساسية للعلاقات الدولية."[15] وبالتالي تعني السيادة الإقليمية الخضوع لقواعد المعاهدة أوالعرف القابل للتطبيق للقانون الدولي، وخصوصية الدولة وحدها تخولها الحق في ممارسة السلطة القضائية، خاصة عن طريق إخضاع الأشياء والأشخاص الموجودين في إقليمها للتشريعات المحلية وتطبيق هذه القواعد. وعلاوةً على ذلك، يحق للدولة التحكم في الوصول إلى أراضيها والخروج منها. يبدو أن الحق الأحدث عهداً سيطبق أيضاً على جميع أشكال الاتصالات. السيادة الإقليمية تحمي الدولة ضد أي شكل من أشكال التدخل من جانب الدول الأخرى. حقوق الدول الأخرى، ولا سيما حقهم في السلامة والحرمة في السلم والحرب، جنباً إلى جنب مع الحقوق التي يجوز لكل دولة أن تطلب لرعاياها في أرض أجنبية.

23. وعلى الرغم من التصنيف الصحيح للـ"الفضاء الإلكتروني على هذا النحو" كممارسة الدولة *الدقة COMMUNI* التي تعطي أدلة كافية أن الفضاء الإلكتروني، أو بالأحرى: مكوناته من ذلك، هي ليست في مأمن من السيادة ومن ممارسة السلطة القضائية.[16] من ناحية أخرى، مارست الدول وسوف تستمر في ممارسة، اختصاصها الجنائي تجاه الجرائم الإلكترونية واستمرت في تنظيم الأنشطة في الفضاء الإلكتروني. من ناحية أخرى، من المهم أن نضع في الإعتبار أن "الفضاء الإلكتروني يتطلب بنية مادية ليتواجد". تتوضع المعدات الخاصة عادة داخل إقليم الدولة. وهي مملوكة من قبل الحكومة أو من قبل الشركات. وقد أكدت الدول باستمرار حقها في ممارسة السيطرة على البنية التحتية الإلكترونية التي تقع في أراضي كل منها، لممارسة سلطتها القضائية على أنشطة الفضاء الإلكتروني على أراضيها، وحماية البنية التحتية الإلكترونية ضد أي تدخل عبر الحدود من قبل دول أخرى أو من قبل الأفراد.

24. أعلنت مجموعة الأمم المتحدة للخبراء الحكوميين على أمن المعلومات في تقريرها عام 2013 أن "سيادة الدولة والمعايير الدولية والمبادئ التي تتدفق من السيادة تنطبق على سلوك الدولة للأنشطة ذات الصلة بتكنولوجيا المعلومات والاتصالات وسلطتها على البنية التحتية لتكنولوجيا المعلومات والاتصالات داخل أراضيها." (الفقرة 20.) ومع ذلك، جسدت في المادة 19 من الإعلان العالمي لحقوق الإنسان، حرية التعبير والمعلومات التي يجب أن تروج دون استثناء. يجب أن تخضع ممارسة السيادة من قبل أي دولة لهذا الحق. وقد أعرب عن الاعتراف المقابل

---

[14] وولف هينستون فون هينيغ، الآثار القانونية المترتبة على السيادة الإقليمية في الفضاء الإلكتروني، وهي متاحة على https://ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

[15] محكمة العدل الدولية، وقضية قناة كورفو (مزايا)، نائب محكمة العدل الدولية، 1، في ص. 35 (1949).

[16] ملاحظة سوبرا 13.

لحرية التعبير من خلال القمة العالمية لمجتمع المعلومات لإعلان المبادئ الفقرات 4 و 55 و 59-56 وخطة العمل، الفقرة 24 التي اعتمدت خلال قمة المرحلة الأولى من القمة العالمية في جنيف، كانون الأول/ ديسمبر عام 2003.[17]

25. ومع ذلك، مع احترام الإدارة العالمية للإنترنت، يبدو أن النموذج المهيمن هو"أصحاب المصلحة المتعددة". يكرر هذا الرأي في إعلان المبادئ المعتمدة في مؤتمر القمة العالمي لمجتمع المعلومات الذي عقد في كانون الاول/ ديسمبر عام 2013. بينما تم الإعتراف بالحقوق السيادية للدول على القضايا السياسة العامة المتصلة بالإنترنت، وشدد على أهمية القطاع الخاص والمنظمات الحكومية الدولية في تطوير وتنسيق الإنترنت والقضايا السياسية العامة ذات الصلة.[18]

ثالثاً. الأمن الإلكتروني- عسكرة الفضاء الإلكتروني والجرائم الإلكترونية

26. قد برز الأمن الإلكتروني كتركيز مركزي آخر للطعن القضائي. ونحن ندرك أن الأمن الإلكتروني هنا كقدرة الدولة على حماية نفسها ومؤسساتها ضد التهديدات الإلكترونية. وأصبحت الجيوش في جميع أنحاء العالم أكثر وأكثر اهتماماً بالإنترنت منذ توسعه وازدياد نقاط الضعف. أصبحت البنى التحتية الوطنية الهامة التي تعتمد على شبكات الكمبيوتر عرضة بشكل متزايد إلى الهجمات الإلكترونية. وعلاوةً على ذلك، فإن الإنترنت أصبح أكثر عرضة من أي وقت مضى للجرائم الإلكترونية والتجسس. ونظراً لضخامة التهديدات التي تشكلها الجهات الحكومية وغير الحكومية، يناقش هذا القسم بشكل مختصر تطبيق قواعد ومبادئ القانون الدولي لمعالجة هذه المخاوف.

أ. الحرب الإلكترونية والتجسس

27. زاد الإعتماد العسكري على أنظمة الكمبيوتر والشبكات أضعافاً مضاعفة، وبالتالي فتح المجال "الخامس" للقتال الحربي إلى جانب المجالات المعترف بها تقليديا من البر والبحر والجو والفضاء الخارجي. مصطلح "الحرب الإلكترونية"، بصفة عامة، يشير إلى الحرب التي جرت في الإنترنت من خلال الوسائل والأساليب الإلكترونية. على سبيل المثال، فإن العدوى من شبكة كمبيوتر العدو المحارب مع فيروس خبيث تشكل عملاً من أعمال الحرب الإلكترونية. هناك مجال الكتروني واحد فقط، مشترك من قبل المستخدمين العسكريين والمدنيين، وكل شيء مترابط. وفقاً للقواعد المعاصرة للقانون الإنساني الدولي، فإن التحديات الرئيسية عند اللجوء إلى الحرب الإلكترونية هي لضمان أن توجه الهجمات ضد الأهداف العسكرية فقط، وأن يؤخذ الحرص المستمر لتجنيب السكان المدنيين والبنية التحتية المدنية. وعلاوةً على ذلك، فإن الخسائر المدنية العرضية المتوقعة والضرر يجب أن لايكون مبالغاً فيها بالنسبة للأفضلية العسكرية الملموسة والمباشرة المنتظرة من الهجوم الإلكتروني. فيجب عدم شن الهجوم إذا كان لا يمكن تحقيق هذه الشروط. هذه التحديات تؤكد على أهمية حذر الدول للغاية عند اللجوء إلى الهجمات الإلكترونية.

---

[17] تقرير عن الاجتماع الموضوعي لليونسكو لإعداد المرحلة الثانية من القمة العالمية لمجتمع المعلومات (WSIS 2005)، وهي متاحة على
http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis_tunis_prep_cyberspace_report_en.pdf

[18] وثيقة WSIS-03/GENEVA/DOC/4-E كانون الأول/ ديسمبر 2013، إعلان مبادئ، القمة العالمية لمجتمع المعلومات.الفقرة 49.

28. دون أي شك، القانون الدولي القائم الذي يحكم أنشطة الدولة ينفذ في أي مكان، بما في ذلك في الفضاء الإلكتروني. بالرغم من، تطبيق القواعد القانونية والمفاهيم والمصطلحات الموجودة مسبقاً في التكنولوجيا الجديدة التي ينطوي تفسيرها في ضوء الخصائص المحددة للتكنولوجيا في السؤال. دليل تالين حول القانون الدولي المطبق في الحرب الإلكترونية بمثابة وثيقة قانونية هامة في هذا الصدد.[19] وهي دراسة أكاديمية وغير ملزمة بشأن القانون الدولي، تحديداً شن الحرب العادلة و القانون الإنساني الدولي، التي تطبق على نزاعات الفضاء الإلكتروني و الحرب الإلكترونية . وقد كتب دليل تالين بناءً على دعوة من تالين ومقره المركز الدفاعي التعاوني للناتو للتميز من قبل فريق دولي بما يقارب العشرين خبيراً بين عامي 2009 و 2012.

29. شن الحرب العادلة هي مجموعة من القوانين التي تحكم لجوء الدول إلى القوة في علاقاتها الدولية. اليوم، أهم مصدر لشن الحرب هو ميثاق الأمم المتحدة. الميثاق هو مساعد أساسي في اتخاذ قرار في مثل هذه الظروف، إن وجدت، يمكن للعمليات الإلكترونية أن تصل (1) لتشكل تهديداً دولياً غير مشروعاً أو استخداماً "للقوة"، (2) "هجوماً مسلحاً" يبرر اللجوء إلى قوة ضرورية ومتناسبة للدفاع-عن النفس، أو (3) "تهديداً للسلام"، "الإخلال بالسلم" أو "عملاً عدوانياً" يخضع لتدخل مجلس الأمن الدولي.[20] يعرض دليل تالين بعض الإستنتاجات الرئيسية على "استخدام القوة"، ومسؤولية الدولة في الفضاء الإلكتروني بعد دراسة متأنية للميثاق والقانون الدولي العرفي وغيرها من الصكوك القانونية ذات الصلة:

- قد لا تسمح الدول عمداً بتوضع البنية التحتية الإلكترونية في أراضيها لتستخدم في الأعمال التي تؤثر سلباً على دول أخرى.
- قد تكون الدول مسؤولة عن العمليات الإلكترونية الموجهة ضد دول أخرى، على الرغم من أن تلك العمليات لم تجر من قبل الأجهزة الأمنية. تحديداً، الدول نفسها مسؤولة بموجب القانون الدولي عن تصرفات الأفراد أو الجماعات الذين يعملون تحت إشرافها. على سبيل المثال، الدولة التي تدعو المتسللين للقيام بعمليات الكترونية ضد دول أخرى مسؤولة عن تلك الإجراءات كما لو أنها أجرتها بنفسها.
- حظر استخدام القوة في القانون الدولي ينطبق تماماً على عمليات الفضاء الإلكتروني. رغم أن القانون الدولي لايملك بداية معرفة تماماً لتحديد متى تكون عملية الفضاء الإلكتروني هي استخدام للقوة، وافقت المجموعة الدولية من الخبراء كحد أدنى، على أن أي عملية الكترونية تسبب ضرراً للأفراد أوضرراً بالأهداف يتم وصفها بأنها استخدام للقوة.
- وافق الفريق الدولي من الخبراء على أن العمليات الإلكترونية بمجرد أن تسبب إزعاجاً أو غضباً لا تصنف ضمن استخدامات القوة.

---

[19] دليل تالين حول القانون الدولي المطبق في الحرب الإلكترونية، مطبعة جامعة كامبريدج، عام 2013.
[20] انظر عموماً نيلس ميلسر، الحرب الإلكترونية والقانون الدولي، مصادر معهد الأمم المتحدة لبحوث نزع السلاح(2011).

30. في المقابل، على النحو المذكور أعلاه، القانون الدولي الإنساني (IHL) أو قانون الحرب، الذي يفرض قيوداً قانونية على السلوك في زمن الحرب، ينطبق على الحرب الإلكترونية. استخدام العمليات الإلكترونية في النزاعات المسلحة يمكن أن يشكل احتمال لعواقب إنسانية وخيمة. عندما تتعرض أجهزة الكمبيوتر أو شبكات الدولة لهجوم، تسلل أو حظر، قد يكون هناك خطر على المدنيين بأن يُحرموا من الضروريات الأساسية مثل مياه الشرب، الرعاية الطبية والكهرباء. إذا شُلت أنظمة تحديد المواقع العالمية، قد يكون هناك خطر حدوث سقوط ضحايا من المدنيين- على سبيل المثال، من خلال تعطيل لمروحيات الإنقاذ في عمليات الطيران التي تنقذ الحياة. السدود والمحطات النووية والطائرات وأنظمة التحكم، بسبب اعتمادها على أجهزة الكمبيوتر، هي أيضاً عرضة للهجمات الإلكترونية.[21] الشبكات مترابطة جداً، حيث قد يكون من الصعب الحد من آثار الهجوم ضد جزء واحد من النظام دون الإضرار بالآخرين أو تعطيل النظام برمته. كل هذا يدعو لتطبيق القانون الدولي الإنساني.

31. الفصلين الرابع والخامس من دليل تالين يتعامل حصراً مع تطبيق القانون الدولي الإنساني في الحرب الإلكترونية. دليل دعم الإنقسام التقليدي بين النزاعات المسلحة الدولية وغير الدولية، ويعترف بأن العمليات الإلكترونية وحدها قد تشكل النزاعات المسلحة تبعاً للظروف - بشكل ملحوظ على الآثار المدمرة لهذه العمليات. في هذا الصدد، يعرف الدليل "الهجوم الإلكتروني" بموجب القانون الدولي الإنساني بأنه "عملية إلكترونية، سواء كانت هجومية أو دفاعية، التي من المتوقع أن تسبب الإصابة أو الوفاة لأشخاص أو الأذى أو التدمير لكائنات".

32. وبالمثل، يتلو تقارير على نطاق واسع عن التطفل على البعثات الأجنبية وغيرها من الأنشطة للعديد من الدول، وعوامل التجسس الإلكترونية كما في منشأة حساسة تتعلق بالأمن الإلكتروني. بينما كان التجسس جزء لا يتجزأ من سياسة الحرب الباردة، وذلك بفضل التكنولوجيا، أعمالها الشائنة المطلقة والإفلات من العقاب اليوم أمر لا مثيل له. اتفاقية فيينا للعلاقات الدبلوماسية تؤكد حرمة المراسلات الدبلوماسية وتلقى التزاماً إيجابياً على الدول المضيفة لحماية حرية الاتصال على جزء من بعثة دبلوماسية لجميع الأغراض الرسمية (المادة 27، VCDR). حتى أنها تنص على التزامات مماثلة لبلد ثالث عندما يكون مثل هذا الاتصال عابراً (المادة 40 (3)، VCDR). تحمي اتفاقية فيينا للعلاقات الدبلوماسية بشكل صريح الاتصالات الدبلوماسية التقليدية كمثال دلائل السياح والحقائب والبث اللاسلكي.[22] ودخلت حيز التنفيذ عندما كانت لا تزال تجري تطوير أشكال مبكرة من أجهزة الكمبيوتر والمراسلات- الإلكترونية التي لا تجد إشارة محددة فيه. ومع ذلك، تنص المادة 24 من اتفاقية فيينا للعلاقات الدبلوماسية أن المحفوظات ووثائق البعثة "لا يجوز انتهاك حرمتها في أي وقت وأينما كانت". وبالتالي هذا الحكم يشمل بوضوح مراسلات وبيانات البريد الإلكتروني المخزنة في الأقراص الصلبة وفي "التخزين السحابي".

---

[21] الهجمات الإلكترونية على المنشآت النووية الإيرانية باستخدام فيروس دودة "ستكسنت" هو مثال جيد.انظر عموماً مايكل كيلي، إن هجوم ستكسنت على المحطة النووية الايرانية كان "أكثر خطورة" مما كان يعتقد سابقاً،
http://www.businessinsider.in/The-Stuxnet-Attack-On-Irans-Nuclear-Plant-Was-Far-More-Dangerous-Than-Previously-Thought/articleshow/26113763.cms

[22] اتفاقية فيينا للعلاقات الدبلوماسية فيينا 18 نيسان/أبريل 1961، 500 استراتيجية الأمم المتحدة الانتقالية 95.

33. وعلاوةً على ذلك، ينص دليل تالين بوضوح على أن الدولة تتحمل المسؤولية القانونية الدولية للعملية الإلكترونية التي تعزى إليها والتي تشكل خرقاً لالتزام دولي (المادة 6). بالتالي ينطوي التجسس الإلكتروني للمراسلات الدبلوماسية على انتهاك محدد لقانون المعاهدة (VCDR)، ويمكن أن يعزى إلى الدولة الآمرة به. يقول الدليل أن أي نشاط الكتروني تقوم به المخابرات والجيش والأمن الداخلي والجمارك أو غيرها من الوكالات الحكومية سوف تشارك مسؤولية الدولة بموجب القانون الدولي إذا كان ينتهك التزام قانوني دولي ينطبق على ذلك.

ب. الجرائم الإلكترونية والقانون الدولي

34. الجرائم الإلكترونية والأمن الإلكتروني هي قضايا بالكاد يمكن أن تفصل في بيئة مترابطة. يمكن تعريف الجريمة الإلكترونية على نطاق واسع كأي جريمة ارتكبت ضد أو مستهدفة أجهزة الكمبيوتر، أو ارتكبت من خلال استخدام أجهزة الكمبيوتر أو تكنولوجيا المعلومات والاتصالات. لذلك هذا يمكن أن تنطبق على مجموعة واسعة من الجرائم في جميع أنحاء العالم. خلال مؤتمر الأمم المتحدة الـ 10 لمنع الجريمة ومعاملة المجرمين، تم وضع تعريفين ضمن ورشة العمل ذات الصلة: الجرائم الإلكترونية بالمعنى الضيق (جرائم الحاسوب) تغطي أي سلوك غير قانوني موجه عن طريق العمليات الإلكترونية التي تستهدف أمن نظم الكمبيوتر والبيانات المجهزة بها. الجرائم الإلكترونية بمعنى أوسع (الجرائم المتعلقة بالكمبيوتر) تغطي أي سلوك غير قانوني ارتكب بواسطة، أو فيما يتعلق، بنظام الكمبيوتر أو الشبكة، بما في ذلك جرائم من قبيل الحيازة غير المشروعة وتقديم المعلومات أو توزيع عن طريق نظام الكمبيوتر أو الشبكة.[23]

35. ردع الجريمة هو جزء لا يتجزأ من الأمن الإلكتروني الوطني واستراتيجية حمائية للبنية التحتية للمعلومات الخطيرة. بشكل خاص، يشمل هذا اعتماد التشريعات المناسبة ضد سوء استخدام تكنولوجيا المعلومات والاتصالات لأغراض وأنشطة إجرامية أو أخرى تهدف إلى التأثير على سلامة البنية التحتية الحرجة الوطنية. على المستوى الوطني، يعتبر هذا مسؤولية مشتركة تتطلب العمل المنسق المتصل لمنع، الإعداد، الاستجابة والتعافي من الحوادث من جانب السلطات الحكومية والقطاع الخاص والمواطنين. على المستوى الإقليمي والدولي، هذا يتطلب التعاون والتنسيق مع الشركاء المعنيين.

36. ونظرا لعدد أقل من الصكوك القانونية الدولية التي يمكن استخدامها لردع الجريمة الإلكترونية، يصبح من المناسب التساؤل ما إذا كان القانون العرفي سابق التعامل مع مسألة الجريمة الإلكترونية. يوجد هيكل للقانون الدولي العرفي الذي يعكس سلوك واسع وموحد تقريباً للدول القومية خلال الحروب التقليدية التي تحظى بقبول واسع وكذلك فهم قانون الحرب. للأسف تطبيق قانون الحرب لجريمة الكترونية ينطوي على إشكالية، لأن الإجراءات والآثار المتاحة للدول والجهات الفاعلة غير الحكومية في الفضاء الإلكتروني لا تتطابق بالضرورة مع المبادئ التي تحكم

---

[23] الجرائم المتعلقة بشبكات الحاسوب، مقالة تمهيدية لورشة العمل حول الجرائم المتصلة بشبكة الكمبيوتر، مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، 2000، A/CONF.187/10، الصفحة 5؛ متوفر على:
www.uncjin.org/Documents/congr10/10e.pdf.

الصراعات المسلحة، والطبيعة القصصية لإرتكاب الجريمة في الجرائم الإلكترونية توقع في مشاكل تطبيق تلك المبادئ الأساسية في هذه المنطقة الرمادية.

37. انتشار التكنولوجيات المتقدمة، قد ساهم بفشل النظام المعياري الدولي لتجهيز القيود القانونية على استخدامه، وعدم وجود آليات فعالة للرصد لتنظيم أنشطة الفضاء الإلكتروني لمشكلة تصاعد الجريمة الإلكترونية. التهديدات المحتملة للجرائم الإلكترونية لم تزعج الأشخاص الطبيعيين فقط ولكن وضعت تحدياً كبيراً أيضاً لصناع السياسة والحكومات ووسائل الإعلام. على الرغم من أن الأنشطة في الفضاء الإلكتروني *بحكم القانون* تخضع لسلطة الدولة الفردية، تشكل التعقيدات الفنية المشاركة في الإتصال تحدياً كبيراً للقانون الدولي. وتتفاقم هذه المشكلة بسبب فشل القانون الدولي لجعل الجهات الفاعلة الغير تابعة للدولة والتي لها ريادتها التكنولوجيّة في الفضاء الإلكتروني بموجب تنظيم قواعد أساسها معاهدة محددة، وقد سهلت هذه الجهات الفاعلة الغير تابعة للدولة استغلال فشل النظام القانوني لمواصلة انغماسهم في ارتكاب الجريمة. بالنسبة للدول المتقدمة، قد أظهرت الدول والشركات متعددة الجنسيات أقل اهتمام في وضع إطار تنظيمي فعال لإحباط الأنشطة الإجرامية في الجرائم الإلكترونية. أما بالنسبة للبلدان النامية، تم إيجاد استراتيجيات وحلول رداً على تهديد الجريمة الإلكترونية التي تعتبر تحدياً رئيسياً. وهذا يتطلب من الإنسان التفكير في مدى فعالية النظام القانوني الدولي في تنظيم الجريمة الإلكترونية وكيف يسير نحو معالجة المخاوف الأمنية للفضاء الإلكتروني.

38. وفي هذا الصدد، اعترفت القمة العالمية لمجتمع المعلومات (WSIS) بالمخاطر الحقيقية والهامة التي تتمثل بعدم كفاية الأمن الإلكتروني وانتشار الجريمة الإلكترونية.[24] أحكام الأقسام 108-110 للقمة العالمية لمجتمع المعلومات من جدول أعمال تونس لمجتمع المعلومات، بما في ذلك الملحق، حيث وضعت خطة لتشغيل صاحب المصلحة المتعددة على المستوى الدولي لخطة جنيف للقمة العالمية للعمل، واصفةً عملية تشغيل أصحاب المصلحة المتعددة وفقاً إلى خطوط العمل الإحدى عشر، وتوزيع المسؤوليات لتسهيل تشغيل خطوط العمل المختلفة.[25] في القمة، عيّن قادة وحكومات العالم الإتحاد الدولي للإتصالات لتسهيل تشغيل عمل الخط سي5 للقمة، مكرسة بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والإتصالات.

39. اتفاقية الجريمة الإلكترونية التي تسمى أيضاً باتفاقية بودابست هي المعاهدة المتعددة الأطراف القائمة وحدها، والتي تعالج جرائم الكمبيوتر ذات الصلة تحديداً التي دخلت حيز التنفيذ في 1 تموز/ يوليو 2004، بالإضافة إلى ذلك، يوجد "البروتوكول الإضافي لمؤتمر الجرائم الإلكترونية، بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب من خلال أنظمة الكمبيوتر". تم تصميم اتفاقية لتعزيز التحقيق والملاحقة القضائية عبر الحدود لجرائم الكمبيوتر ذات الصلة من خلال القضاء أو الحد من العقبات الإجرائية والقضائية للتعاون الدولي. ولكن عدم

---

[24] لمزيد من المعلومات حول مؤتمر القمة العالمي لمجتمع المعلومات (WSIS)، انظر /www.itu.int/wsis

[25] مؤتمر القمة العالمي لمجتمع المعلومات برنامج عمل تونس بشأن مجتمع المعلومات، وهي متاحة على العنوان التالي:
www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

الملائمة والثغرات الموروثة في الإتفاقية قد أظهر ضعفاً في ردع الهاكرز. الجرائم الإلكترونية هي منطقة جريمة تتغير باستمرار.

40. في عام التسعينيات، عندما طورت اتفاقية الجرائم الإلكترونية، استخدام الإرهابيون الفضاء الإلكتروني، الروبوتات[26] الهجمات والتصيد[27] إما لم تكن معروفة أو لم تلعب دوراً هاماً كما تفعل اليوم، وبالتالي لا يمكن معالجتها مع حلول محددة. وينطبق الشيء نفسه فيما يتعلق بالوسائل الإجرائية. اعتراض الإتصالات الصوتية عبر بروتوكول الإنترنت (VoIP)، ومقبولية الأدلة الرقمية والإجراءات للتعامل مع الإستخدام الناشئ لتكنولوجيا التشفير ووسائل الاتصال المجهولة هي من القضايا ذات الأهمية الكبيرة ولكنها لم تعالج من قبل اتفاقية الجرائم الإلكترونية. لم تعدّل الإتفاقية أبداً لمدة عشر سنوات من وجودها، وبصرف النظر عن البروتوكول الإضافي على المواد المعادية للأجانب، لم تتم إضافة أي أحكام أو أدوات إضافية.[28]

رابعاً. تعليقات وملاحظات أمانة آلكو

41. الطبيعة الفقهية للإنترت طالبت بنموذج *فريد* لإدارته، وجاء نطاق أصحاب المصلحة المتعددة الحالية إلى حيز الوجود الإضافي رداً على ذلك. ومع ذلك، فإن هذا النطاق، مع السيطرة الغربية المتحكمة فيه، هو أبعد ما يكون عن الإنصاف. تفضل الدول المتطورة نموذج الأمم المتحدة المركزي لموازنة هذا الوضع الشاذ. اختتم مؤخراً مفوض الإتحاد الدولي للاتصالات، المناقشات المكثفة لحوكمة الإنترنت، ولكن لم تكن نتائج ذات قيمة. تقترح أن تكون الدول على استعداد للتنازل قليلا فقط عندما يتعلق الأمر بحماية مصالحها في المسائل المتعلقة بحوكمة الفضاء الإلكتروني. يبدو أن الدول غامضة في إبداء المواقف السياسية في المقترحات، ولكنهم أكثر استعداداً للسماح لهم بالتماشي معهم طالما المقترحات المقدمة من ذوي الآراء المتعارضة أيضاً ليست مدرجة. التحديات القانونية والتقنية والمؤسسية التي تطرحها مسألة الأمن الإلكتروني هي عالمية وبعيدة المدى، ولايمكن معالجتها إلا من خلال استراتيجية متماسكة، مع الأخذ بعين الاعتبار دور أصحاب المصلحة المختلفة والمبادرات القائمة، في إطار من التعاون الدولي. تؤمن الأمانة بقوة بالنهج المتعدد الأطراف والمتصالح، مع الأخذ بعين الإعتبار جميع مطالب أصحاب المصلحة في حوكمة الإنترنت، بينما تحترم حقوق السيادة بين جميع الدول في تنظيم شبكة الإنترنت في سلطتها القضائية، هو أفضل السبل للمضي قدماً في مستقبل المفاوضات.

42. ونظراً للطابع الروائي عن الفضاء الإلكتروني ونظراً لضعف البنية التحتية والمكونات الإلكترونية هناك شكوك ملحوظة بين الحكومات والباحثين القانونيين حول ما إذا كانت قواعد ومبادئ القانون الدولي العرفي التقليدية هي عرضة بشكل كاف لتقديم الإجابات المطلوبة لبعض الأسئلة المقلقة. ولذلك، يوجد أهمية عظمى ليس فقط لموافقة الدول على التطبيق الأساسي للقانون الدولي العرفي للفضاء الإلكتروني، ولكن أيضاً على التفسير المشترك الذي يأخذ

---

[26] بوتنيتس هي مصطلح مختصر لمجموعة تسوية برامج تشغيل أجهزة الكمبيوتر التي هي تحت السيطرة الخارجية. لمزيد من التفاصيل، انظر ويلسون، بوتنيتس، الجرائم الإلكترونية، والإرهاب الإلكتروني: نقاط الضعف وقضايا السياسات للكونغرس 2007، الصفحة 4، متوفر على: www.fas.org/sgp/crs/terror/RL32114.pdf.

[27] مصطلح "التصيد" يصف الفعل الذي يتم القيام به لجعل الضحية تكشف معلومات سرية /شخصية. مصطلح "التصيد" وصف في الأصل استخدام رسائل البريد الإلكتروني إلى "تصيد" كلمات السر والبيانات المالية من بحر من مستخدمي الإنترنت.

[28] الإتحاد الدولي للإتصالات، فهم الجريمة الإلكترونية: الظواهر والتحديات والإستجابة القانونية 126 (2012).

بالإعتبار السمة الوحيدة للفضاء الإلكتروني. وبالتالي من الضروري أن تواصل الحكومات العمل على الصعيد الدولي، لصياغة توافق في الآراء بشأن كيفية تطبيق قواعد السلوك للفضاء الإلكتروني.

43. وعلاوةً على ذلك، فإن التصعيد الأخير لإضفاء الصفة العسكرية للفضاء الإلكتروني مرعبة. ارتفاع الهجمات الإلكترونية على البنى التحتية للعديد من الدول والتجسس الإلكتروني على أنشطة العديد من الدول يدعو لمداولات مفصلة عن القواعد القانونية المعمول بها في مثل هذا السلوك. دليل تالين، الذي يوفر إجابات جزئية لهذه المخاوف، هو صك غير ملزم. الدول الأعضاء في آلكو، متنبهه لعدم حصانة بنيتها التحتية الإلكترونية وقابلية غزوها إلكترونياً من قبل كل من الدولة والجهات الفاعلة من غير الدول، يجب أن تعلن تعهدها نحو الموالاة لإنفاذ ميثاق الأمم المتحدة والصكوك الدولية لحقوق الإنسان والقانون الدولي الإنساني في سلوكهم في الفضاء الإلكتروني.

44. وعلاوةً على ذلك، نظراً للخصائص الفريدة للفضاء الإلكتروني، تستلزم مكافحة الجريمة الإلكترونية اتباع نهج شامل. وبالنظر إلى أن التدابير التقنية وحدها لا يمكن أن تمنع أي جريمة، فمن المهم أن يتم السماح لوكالات إنفاذ القانون على المستوى الوطني بالتحقيق ومقاضاة الجرائم الإلكترونية على نحو فعال. بناء القدرات أمر بالغ الأهمية بالنسبة للدول النامية لإحباط الجرائم الإلكترونية بفعالية، وينبغي على الدول المتقدمة مساعدتهم في تطوير الإستراتيجيات المؤسساتية لآليات بناء القدرات لرفع مستوى الوعي ونقل المعرفة وتعزيز الأمن الإلكتروني على المستوى المحلي. التعاون الثنائي والمتعدد الجنسيات بين الدول الأعضاء في آلكو في هذا الصدد ممكن أن يركز على الحوار والتنسيق فى التعامل مع التهديدات الإلكترونية.

ملحق

مسودة الأمانة

AALCO/ RES/DFT/54/S17

17 نيسان/ أبريل 2015.

قرار حول "القانون الدولي في الفضاء الإلكتروني"

(متداول)

المنظمة الإستشارية القانونية الآسيوية الأفريقية في الدورة الرابعة والخمسين،

بعد النظر في وثيقة الأمانة رقم AALCO/54/BEIJING/2015/SD/S17 المعدة من قبل أمانة آلكو،

يلاحظ مع التقدير بيان استهلالي من نائب الأمين العام،

وإدراكا لأهمية الفضاء الإلكتروني باعتباره جزءاً متمماً للتفاعل الإنساني وتأثيره العميق على الحياة الوطنية للدول الأعضاء،

إدراكاً لضرورة دمقرطة حوكمة الإنترنت في مواصلة الإنصاف وسد "الفجوة الرقمية" السائدة في الدول النامية،

الإعتراف بأهمية الموازنة بين الحقوق السيادية للدول والحريات الأساسية للكلام والتعبير لمواطنيها في الفضاء الإلكتروني،

يلاحظ مع القلق عسكرة الفضاء الإلكتروني والتصعيد في أنواع مختلفة من الهجمات الإلكترونية بما في ذلك الجرائم الإلكترونية التي ترتكبها الدولة والجهات الفاعلة من غير الدول،

1. **تحث** الدول الأعضاء على احترام القانون الدولي، ولا سيما ميثاق الأمم المتحدة وغيرها من الصكوك ذات الصلة بسلوك الدولة في الفضاء الإلكتروني.
2. **تشجع** الدول الأعضاء على المشاركة بنشاط في تداول المحافل الإقليمية والعالمية ذات الصلة بحوكمة الفضاء الإلكتروني.
3. **يقرر** إنشاء فريق عامل مفتوح العضوية على القانون الدولي في الفضاء الإلكتروني لمواصلة مناقشة المسألة من خلال الإجتماعات أو حلقات العمل التي شاركت في رعايتها مع حكومات الدول الأعضاء أو المنظمات الدولية ذات الصلة؛
4. تقرر وضع هذا البند على جدول الأعمال المؤقت للدورة السنوية الخامسة والخمسين.