منظمة الطيران المدني الدولي

ورقة عمل

LC/39-WP/2-5[1]
10/5/24

اللجنة القانونية – الدورة التاسعة والثلاثون

(مونتريال، ٢٥ إلى ٢٠٢٤/٦/٢٨)

البند رقم ٢ من جدول الأعمال: النظر في برنامج العمل العام للجنة القانونية

الأفعال أو الانتهاكات التي تثير قلق مجتمع الطيران المدني الدولي، بما في ذلك التهديدات الإلكترونية، التي قد تكون الأحكام الواردة بشأنها في المواثيق الحالية لقانون الجو غير كافية

(مقدمة من الجمهورية الدومينيكية)

١- المعلومات الأساسية

١-١ أقرّت الدورة الحادية والأربعون للجمعية العمومية للإيكاو بأن بعض الأعمال أو الجرائم التي تثير قلق أوساط الطيران المدني الدولي، بما في ذلك التهديدات الإلكترونية، قد لا تكون مشمولة بشكل كاف بمواثيق قانون الجو الحالية؛ ولذلك ركز النهج المتبع إزاء تلك التهديدات على الجانب القانوني المتعلق بالأمن الإلكتروني. وندرك أن الجهود التي بذلت في هذا الصدد في العقود الأخيرة انطوت دائما على التأقلم مع المشاكل الراهنة. وفي عام ٢٠٢٢، قدمت الأمانة العامة تقريرا صادراً عن المجموعة الفرعية المعنية ببحث الجوانب القانونية إلى الدورة ٣٨ للجنة القانونية، التي اجتمعت في مونتريال، جاء فيه أن الإطار الحالي لقانون الجو الدولي كاف جزئيا للتصدي للتهديدات الإلكترونية ضد الطيران المدني.

١-٢ وفي وقت لاحق، قدمت سنغافورة في وقائع منتدى المستشارين القانونيين في الطيران المدني (١٦ و٢٠١٩/٥/١٧) استنتاجات وتوصيات مفادها أن "التحديات ومواطن الضعف المتعلقة بالأمن الإلكتروني والسلامة الإلكترونية هي من النواتج الجانبية التي أفرزها العصر الرقمي. ولا تقتصر هذه المسألة على أنشطة الطيران، بل تشمل جميع الأنشطة في مجتمعنا. وبالتالي، ومن المنظور القانوني أيضا، يمكن التعامل مع قطاع الطيران بنفس الطريقة التي تعامل بها القطاعات الأخرى". وينبغي ألا تُدخر أي موارد في التصدي للتحديات الإلكترونية التي تواجه أمن الطيران المدني. ويجب أن يكون التركيز شاملا، بحيث تُنشر التدابير في جميع الميادين المتصلة بالقطاع. وبدون ذلك، سوف تظهر المزيد من الثغرات القانونية.

١-٣ نحن نتفق مع استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران لعام ٢٠١٩ التي تقول إن "الهدف الرئيسي من التشريعات واللوائح الدولية والإقليمية والوطنية بشأن الأمن الإلكتروني في مجال الطيران المدني هو العمل على تنفيذ استراتيجية شاملة للأمن الإلكتروني من أجل حماية قطاع الطيران المدني وجمهور المسافرين من آثار الهجمات الإلكترونية". وتنص الاستراتيجية أيضاً على أنه "يجب على الدول الأعضاء ضمان صياغة التشريعات واللوائح المناسبة وتطبيقها، وفقاً لأحكام الإيكاو، قبل تنفيذ سياسة وطنية للأمن الإلكتروني في مجال الطيران المدني". ومن الواضح أنه قد أُحرز تقدمٌ ملحوظ في التكنولوجيا وبالتالي في مجال الطيران. ولا شك أن كل دولة قد اتخذت تدابير تتعلق بالتحول الرقمي والهجمات الإلكترونية والتهديدات الإلكترونية والخصوصية وحماية البيانات. ولا شك أيضاً أنه قد لا يكون من الضروري في بعض الحالات تعديل

[1] قدمت الجمهورية الدومينيكية النسخة باللغة الإسبانية.

الإرشادات والمبادئ التوجيهية والسياسات واللوائح الوطنية والدولية التي تغطي إدراج الجوانب المتعلقة بالأمن الإلكتروني، لا سيما في مجال السلامة التشغيلية وسلامة الطيران.

١-٤ وبموجب خطة عمل الإيكاو في مجال الأمن الإلكتروني لعام ٢٠٢٢ فإن الدول مدعوة، من جانبها، "إلى تقييم ما لديها من أطر قانونية وطنية في مجال الأمن الإلكتروني والطيران المدني بهدف تحديد الثغرات الحالية وأيضا ضمان توافر التشريعات واللوائح التنظيمية المناسبة لمعالجة عناصر محددة في الأمن الإلكتروني. ويظهر عنصر رئيسي آخر في توافر آلية الإنفاذ التي تشجع الدول على تفعيلها، إن لم تكن موجودة بالفعل في أطرها القانونية الوطنية، لتجريم ومقاضاة الأفعال غير المشروعة ضد الطيران المدني عند ارتكابها باستخدام وسائل إلكترونية."

٢- التحليل

١-٢ في عام ٢٠١٩، ومن خلال استراتيجية الإيكاو للأمن الإلكتروني، وُجِّهت الدول إلى النظر فيما إذا كان ينبغي تحديث تشريعاتها الوطنية، وبالتالي ما إذا كان ينبغي لها أن تعتمد تشريعات وطنية جديدة للتمكين من المقاضاة في الهجمات الإلكترونية المتصلة بالإرهاب والهجمات التي تؤثر سلبا على الطيران المدني. ولا شك أن القوانين واللوائح ذات الصلة موجودة. ومع ذلك، وبالنظر إلى أنَّ من الأهمية بمكان، في المجال القانوني، تعريف الجرائم إذا أريد تنفيذ العقوبات ذات الصلة تنفيذاً صحيحاً، فإن هناك حاجة ملحة إلى أن يكون لدى الدول مبادئ توجيهية واضحة وموحدة. ولا يكفي مجرد الاعتراف بأهمية الأمن الإلكتروني في مجال الطيران المدني الدولي. لقد صدرت المبادئ التوجيهية، بيد أن التكنولوجيا تتطور بشكل أسرع مما نفعل نحن، وما زلنا نحاول اللحاق بالتطورات الجارية. وقد حان الوقت لتحديد الالتزامات والمسؤوليات القانونية التي تقع على عاتق الدول في هذا المجال.

٢-٢ وعلى الرغم من وجود قواعد طوعية وغير ملزمة وقواعد غير طوعية وملزمة، مثل تلك المنصوص عليها في الملحق السابع عشر؛ فإنّ من الضروري تحديد كيفية تطبيق مبادئ القانون الدولي في هذا الصدد وفي نفس الوقت أن تكون أكثر اندماجاً في القواعد الوطنية. ولا تسمح لنا القيود الحالية التي تعانيها كل دولة، سواء كانت تشريعية أو تكنولوجية، برؤية ما وراء احتمالات التهديدات في الحالات التي يُنظر إليها على أنها قد وجدت العلاج.

٣-٢ وفي الجمهورية الدومينيكية، تغطي تشريعات مثل القانون رقم ٥٣-٠٧ (٢٠٠٧) الجرائم والجنح المتعلقة بالتكنولوجيا الرفيعة. ومع ذلك، فإننا نعتبر أن التهديدات الإلكترونية الناشئة حالياً أو التي قد تنشأ في المستقبل ضد الطيران المدني ليست بالضرورة مشمولة أو محددة في القانون أو في قانون العقوبات لدينا. ونشير هنا إلى الإرهاب الإلكتروني والتجسس الإلكتروني، وإلى الهجمات على البنية الأساسية الحيوية. بالإضافة إلى ذلك، تنطوي معظم القضايا التي يتولاها مكتب المدعي العام على إنفاذ علني للشكاوى الخاصة، أي أنه يتعين على الشخص المتضرر تقديم شكواه والمتابعة مع مكتب المدعي العام طوال الإجراءات، مما قد يعني إمكان أن يفلت المتهم من العقاب. ويجب أن تُصاغ التعاريف بحيث تكون أي قضية مطروحة علنية.

٤-٢ وتميل الهيئات التنظيمية إلى إضفاء السرية على التهديدات و/أو أوجه القصور في تكنولوجيا المعلومات والاتصالات (ICT) أو التقنيات التشغيلية. ومن المؤكد أنه كان هناك تركيز واضح في العقود الأخيرة على أمن تكنولوجيا المعلومات والاتصالات في جميع المسائل الإدارية والفنية. غير أن هذا ليس هو الحال بالنسبة للتكنولوجيات التشغيلية، بالنظر إلى أن تنفيذ بعض الضمانات يأتي على حساب تشغيلها بكفاءة في مجالات مثل الملاحة الجوية وقواعد الرحلات الجوية؛ ومسألة الفعالية مقابل السلامة هي محل نقاش مستمر.

٥-٢ واتخذت الجمهورية الدومينيكية تدابير تتماشى مع دستورها، وتحديدا المادة ٢٦٠، لضمان ألا تعرض التطورات التكنولوجية وتأثيرها على الطيران المدني الأمنَ للخطر، مشيرة إلى أن "الأهداف الوطنية ذات الأولوية العليات هي: مكافحة

الأنشطة الإجرامية العابرة للحدود الوطنية التي تعرض مصالح الجمهورية وسكانها للخطر؛ وتنظيم واستدامة النظم الفعالة التي تمنع وقوع الأضرار الناجمة عن الكوارث الطبيعية والتكنولوجية أو تخفف منها".

٢-٦ وفيما بعد، أنشأ المرسوم رقم ٢٣٠-١٨، الذي نُشِر في ٢٠١٨/٦/١٩، الاستراتيجية الوطنية للأمن الإلكتروني للفترة ٢٠١٨-٢٠٢١ كما أنشأ المركز الوطني للأمن الإلكتروني. ويعمل فريق الاستجابة للوقائع الإلكترونية (CSIRT-RD) كنقطة اتصال على مستوى البلاد للوقاية من الوقائع التي تؤثر على أنظمة المعلومات الحكومية والبنية الأساسية الحيوية والكشف عنها وإدارتها.

٢-٧ وفي عام ٢٠٢٤، صِيغ مشروع قانون بشأن الإدارة الشاملة للأمن الإلكتروني في الجمهورية الدومينيكية، وهو معروض حاليا على كونغرس الجمهورية، ويهدف إلى تعزيز الإطار التنظيمي لإدارة الأمن الإلكتروني للإدارة العامة البنية الأساسية لتكنولوجيا المعلومات والاتصالات والبنية الأساسية الحيوية في جميع أنحاء البلاد. وبمجرد الموافقة على مشروع القانون، سيُشكل المجلس الوطني للأمن الإلكتروني باعتباره هيئة تابعة للمركز الوطني للأمن الإلكتروني وأعلى سلطة فيه، وسوف يكون مسؤولاً عن وضع وتوجيه السياسات لإدارة القضايا الإلكترونية المتعلقة بالبنية الأساسية لتكنولوجيا المعلومات والاتصالات للإدارة العامة والبنية الأساسية الحيوية.

٢-٨ ويعترف مشروع القانون هذا بالمبادئ المنصوص عليها في نداء باريس للثقة والأمن في الفضاء الإلكتروني الصادر بتاريخ ٢٠١٨/١١/١٢ وفي التقرير الختامي للجنة العالمية المعنية باستقرار الفضاء الإلكتروني الصادر في نوفمبر ٢٠١٩. وهو يشمل، من دون تمييز، أموراً منها مبادئ المساعدة المتبادلة، ومنع الأنشطة غير المشروعة، وتبادل المعلومات، وحماية حقوق الإنسان، وحماية البنية الأساسية الحيوية.

٢-٩ ولا بد من الإشارة إلى أنه على الرغم من أن المركز الوطني للأمن الإلكتروني موجود منذ عام ٢٠١٨، فإنه بموجب مشروع القانون سيتم إلحاقه بوزارة شؤون الرئاسة ككيان قانوني عام يتمتع بشخصية قانونية واستقلالٍ ذاتي وظيفياً ومن حيث الميزانية، وإدارياً وفنياً ومالياً؛ والهدف من ذلك هو إعطاء المركز استقلالية أكبر في تنفيذ وظائفه.

٢-١٠ وبالمثل، يناقش مشروع القانون البنية الأساسية الحيوية والمعلومات المتعلقة بوقائع الأمن الإلكتروني، أي كيفية التعرف عليها، والإطار الذي سيتم بموجبه تعيينها، والإجراءات الإدارية المقابلة وتحليل المخاطر. ويحدد التأثيرات الإكترونية الكبيرة ونظام العقوبات. ويسعى مشروع القانون إلى تغطية النقاط التي لم تكن محل اعتبار حتى الآن.

٣- الخلاصة

٣-١ من الواضح أن أي عمل ناجع في مواجهة تهديدات ووقائع الأمن الإلكتروني يجب أن يستند إلى إطار عام ينظم اعتماد التدابير الوقائية وإدارة الإجراءات الفعالة وتنظيم البنية الأساسية المعنية. ونحن نواجه وضعا سيؤثر على كل شخص وعلى كل شيء – وهكذا تجب مواجهته. وتعتبر الجمهورية الدومينيكية الأمن الإلكتروني مسألة أمن وطني، وبالتالي اتخذت التدابير إزاء ذلك.

٣-٢ ونشجع الدول الأخرى التي لم تتخذ بعد مثل هذا الإجراءات على أن تفعل ذلك بالقدر نفسه من الحماس. ونوصي جميع الدول التي لم تفكر في هذه المسألة بتقييم تشريعاتها الجزائية والجنائية والإجرائية، واعتبار هذا النوع من الجرائم فعلا عاما يستهدف الأمن الوطني. ونحث أيضا على تحديث الجرائم الجنائية مثل الإرهاب الإلكتروني والتجسس الإلكتروني وإدراجها، حتى يمكن مقاضاة مرتكبيها وتعريفها بالشكل الصحيح لحماية أمن الطيران، على الصعيدين الوطني والدولي على حد سواء. وينبغي أيضا توسيع نطاق المصطلحات لتشمل الأنواع الجديدة من الهجمات الإلكترونية والتهديدات الإلكترونية التي نشأت في العقد الماضي.

– انتهى –