Organización de Aviación Civil Internacional

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

NOTA DE ESTUDIO

COMITÉ JURÍDICO – 39º PERÍODO DE SESIONES

(Montreal, 25 – 28 de junio de 2024)

Cuestión 2: Consideración del programa general de trabajo del Comité Jurídico

ACTOS O INFRACCIONES QUE ATAÑEN A LA COMUNIDAD DE LA AVIACIÓN CIVIL INTERNACIONAL, INCLUIDAS LAS CIBERAMENAZAS, QUE PUDIERAN NO ESTAR PREVISTOS ADECUADAMENTE EN LOS INSTRUMENTOS DE DERECHO AERONÁUTICO ACTUALES

(Nota presentada por la República Dominicana)

1. ANTECEDENTES

1.1 Es importante destacar que, durante el 41° Período de Asamblea de la OACI, se determinó que existen actos o delitos que preocupan a la comunidad de la aviación civil internacional, incluidas las amenazas cibernéticas, que pueden no ser adecuadamente cubiertas por los instrumentos existentes de derecho aeronáutico, razón por la cual su abordaje se ha enfocado en trabajos jurídicos en materia de ciberseguridad. Entendemos que los esfuerzos que estamos empleando en esta materia han sido un trabajo de las últimas décadas, adaptándonos siempre a la problemática de los tiempos. En el 2022, la Secretaría presentó un informe al Subgrupo de Investigación sobre Aspectos Jurídicos ante el 38º período de sesiones del Comité Jurídico, reunido en Montreal, en el que se afirmó que el marco existente de derecho aeronáutico internacional era parcialmente adecuado para abordar las amenazas cibernéticas contra la Aviación Civil.

1.2 Posteriormente, durante el Foro de Consultores Legal sobre Aviación Civil del 16 al 17 de mayo del 2019, en un documento contentivo de los procedimientos del Foro, Singapur presentó hallazgos y recomendaciones donde explica que los *"desafíos y vulnerabilidades relacionados con la ciberseguridad y la seguridad cibernética son productos secundarios de la era digital. Esto es una cuestión que no se limita a las actividades aeronáuticas, sino a todas actividades en nuestra sociedad. En consecuencia, también desde el punto de vista jurídico, la aviación se puede abordar de la misma manera como otros sectores"*. No se debe escatimar ningún recurso en cuanto a cómo se enfrentan los desafíos cibernéticos asociados a la seguridad en materia de aviación civil. Debe haber un enfoque holístico para emplear medidas en todos los campos relativos al sector. De lo contrario, se multiplicarían los vacíos existentes en lo que concierne al ámbito jurídico.

1.3 Estamos en consonancia con el documento contentivo de la Estrategia de Ciberseguridad del 2019 de la OACI, "el objetivo principal de las leyes y reglamentos internacionales, regionales y nacionales sobre ciberseguridad para la aviación civil es apoyar la implementación de una estrategia integral de ciberseguridad dirigida a proteger a la aviación civil y a los viajeros de los efectos de los ciberataques". Adicionalmente, dicho documento orienta a los Estados a que deben "asegurarse de que se formulen y apliquen las leyes y reglamentos pertinentes de conformidad con las disposiciones de la OACI, antes de

[1] Versión en español proporcionada por la República Dominicana.

implantar una política nacional de ciberseguridad para la aviación civil". Es evidente que hay avances notorios en la tecnología y por ende en la aviación, de lo que se puede deducir, que no hay Estado que no haya tomado medidas correspondientes a la transformación digital, ciberataques, ciberamenazas, privacidad y protección datos, pero tampoco es menos cierto, que existan casos en los cuales no sea necesario enmendar los textos de orientación, guías, políticas, regulaciones nacionales e internacionales relativas a la inclusión de aspectos relacionados con la ciberseguridad, específicamente en la seguridad operacional y la seguridad de la aviación.

1.4 Por otro lado, el Plan de Acción de Ciberseguridad del año 2022 de la OACI "alienta a los Estados a evaluar su marco jurídico nacional vigente en el ámbito de la ciberseguridad y de la aviación civil con el fin de detectar carencias y cerciorarse de que existan la legislación y los reglamentos apropiados sobre elementos específicos de la ciberseguridad de la aviación civil. Otro componente clave, que se alienta a los Estados a implantar si no existe ya en sus marcos jurídicos nacionales, es el mecanismo judicial para que los actos ilícitos cometidos contra la aviación civil por medios cibernéticos estén tipificados como delito y sean pasibles de enjuiciamiento".

2. ANÁLISIS

2.1 En el 2019, mediante la Estrategia de Ciberseguridad de la OACI se orientó a los Estados a considerar si sus respectivas legislaciones nacionales debían ser actualizadas; y por lo tanto si se debía adoptar una nueva legislación nacional para permitir el enjuiciamiento de ciberataques relacionados con actos terroristas y aquellos que afectan adversamente a la aviación civil. Indudablemente, existen legislaciones y regulaciones pertinentes. Sin embargo, partiendo de la idea de que, en derecho, la tipificación de faltas es crucial para una correcta implementación de las sanciones a ser aplicadas, urge tener directrices claras y homogéneas entre Estados. No es suficiente que se reconozca simplemente la importancia de la ciberseguridad en la aviación civil internacional. Se han recibido las orientaciones, pero la tecnología evoluciona más rápido que nosotros y nos encontramos en un momento de tratar de equipararnos a lo vigente. Es el momento de plasmar las obligaciones y responsabilidades legales de los Estados en este ámbito.

2.2 Aunque existen normas voluntarias, no vinculantes y normas no voluntarias, vinculantes, como las previstas en el Anexo 17; se requiere establecer cómo aplicar los principios de derecho internacional en este aspecto y a su vez ser más exhaustivos en las normativas nacionales. Las limitaciones actuales, ya sean legislativas o tecnológicas de cada nación, no permiten ver más allá de las probabilidades de amenazas ante situaciones consideradas subsanadas.

2.3 En República Dominicana tenemos legislaciones como la Ley Núm. 53-07, del año 2007 en la cual se contempla crímenes y delitos de alta tecnología. No obstante, consideramos que las ciberamenazas que se presentan y pueden a futuro presentarse en la aviación civil no necesariamente estén contempladas ni tipificadas en la legislación ni en nuestro Código Penal. En este sentido, cabe mencionar términos como ciberterrorismo y ciberespionaje; e igualmente, los ataques a infraestructuras críticas. Adicionalmente, la mayoría de las acciones que se toman desde el Ministerio Público son de acción pública bajo instancia privada. Es decir, que el afectado tiene que querellarse y acompañar al Ministerio Público a todo lo largo del proceso, lo cual implica que en ocasiones un inculpado quede impune. Las tipificaciones de esta naturaleza deben motivar a que sean de acción pública, pura y simple.

2.4 Las entidades de regulación tienden a catalogar las amenazas y/o faltas en tecnologías de la información y comunicaciones (tics) o tecnologías operativas. Ciertamente, el enfoque de las últimas décadas en cuanto a la seguridad de las tics ha sido evidente en toda materia administrativa y técnica. Sin embargo, no es así con las tecnologías operativas, dado que la implementación de ciertas seguridades sacrifica la eficiencia que deben tener estos equipos en áreas como Navegación Aérea y Normas de Vuelo; y es un constante debate sobre la efectividad versus la seguridad.

2.5 República Dominicana ha tomado medidas fundamentadas en su Constitución, específicamente en su artículo 260 para asegurar que la evolución tecnológica y su impacto en la aviación civil no ponga en riesgo la seguridad e indica que *"constituyen objetivos de alta prioridad nacional: combatir actividades criminales transnacionales que pongan en peligro los intereses de la República y de sus habitantes; organizar y sostener sistemas eficaces que prevengan o mitiguen daños ocasionados por desastres naturales y tecnológicos".*

2.6 Posteriormente, el 19 de junio del 2018 se publica el Decreto Núm. 230-18 que establece la Estrategia Nacional de Ciberseguridad 2018 al 2021 y crea el Centro Nacional de Ciberseguridad. Igualmente, se cuenta con el Equipo de Respuesta a Incidente Cibernéticos (CSIRT-RD), el cual funge como punto de contacto, a nivel nacional, para la prevención, detección y gestión de incidentes generados en los sistemas de información del gobierno y en las infraestructuras críticas.

2.7 Ahora en el 2024, se encuentra sometido al Congreso de la República un proyecto de ley sobre la Gestión Integral de la Ciberseguridad en República Dominicana, el cual tiene como objetivo fortalecer el marco normativo para la gestión de la seguridad cibernética de las infraestructuras de tecnologías de la información y comunicación de la Administración Pública y de las infraestructuras críticas en el país. Una vez aprobada esta legislación quedaría a su vez conformado el Consejo Nacional de Ciberseguridad, órgano colegiado y máxima autoridad del Centro Nacional de Ciberseguridad encargado de establecer y orientar las políticas para la gestión de la cibernética de las infraestructuras de tecnologías de la información y comunicación de la administración pública y de las infraestructuras críticas.

2.8 El antes mencionado proyecto de ley reconoce los principios incluidos en el Llamado de París, del 12 de noviembre del 2018, para la Confianza y la Seguridad en el Ciberespacio; los principios del reporte final de la Comisión Global sobre la Estabilidad en el Ciberespacio (GCCS, por sus siglas en inglés) de noviembre del año 2019. Indistintamente, incluye los principios de Colaboración, prevención de actividades ilícitas, intercambio de información, protección de los derechos humanos y protección de las infraestructuras críticas, entre otros.

2.9 Es importante aclarar que, aunque República Dominicana cuenta con un Centro Nacional de Ciberseguridad desde el año 2018, este proyecto de ley propone que dicho centro esté amparado bajo esta legislación, adscrito al Ministerio de la Presidencia, como un ente de derecho público con personalidad jurídica, autonomía funcional, presupuestaria, administrativa, técnica y patrimonial, decisión tomada en busca de crearle al Centro más independencia en la ejecución de sus funciones.

2.10 Igualmente, quedan plasmadas en el documento las infraestructuras críticas e información de los incidentes de ciberseguridad de impacto significativo, es decir cómo serán estos reconocidos y el marco sobre el cual serán designados, los procedimientos administrativos correspondientes conjuntamente con un análisis de riesgo. También se tipifican los impactos cibernéticos significativos y el régimen sancionador. El proyecto de ley ha tratado de abarcar puntos que hasta ahora no habían sido considerados.

3. CONCLUSIÓN

3.1 Es evidente que para ser efectivos ante las amenazas e incidentes relacionados a la ciberseguridad debe existir un marco que norme la adopción de medidas para prevención y gestión de respuestas efectivas; además, de la regulación de las respectivas infraestructuras. Estamos frente a una situación de impacto transversal y así debe enfrentarse. República Dominicana entiende que la ciberseguridad es un asunto de seguridad nacional y por tal razón, ha tomado las medidas correspondientes.

3.2 Motivamos a que los demás Estados que no han tomado acciones como éstas, lo hagan con similar entusiasmo. Recomendamos que todos los Estados que no han realizado una introspección en esta materia, evalúen sus legislaciones penales, criminales y procedimentales asumiendo este tipo de delitos como acción pública frente a la seguridad nacional. Adicionalmente, instamos a que se actualicen e incluyan estos tipos de delitos penales, tales como ciberterrorismo y ciberespionaje, a los fines de que estos puedan ser perseguidos y adecuadamente tipificados para la protección de la seguridad aeronáutica tanto a nivel nacional como internacional. Igualmente, ampliar los términos e incluir las nuevas variaciones de ciberataques y ciberamenzas que han surgido en la última década.

— FIN —