Organisation de l'aviation civile internationale

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

NOTE DE TRAVAIL

COMITÉ JURIDIQUE – 39e SESSION

(Montréal, 25 – 28 juin 2024)

Point 2 : Examen du Programme général des travaux du Comité juridique

ACTES OU DÉLITS, Y COMPRIS LES CYBERMENACES, QUI INQUIÈTENT LA COMMUNAUTÉ AÉRONAUTIQUE INTERNATIONALE ET QUI NE SONT PEUT-ÊTRE PAS DÛMENT TRAITÉS DANS LES INSTRUMENTS DE DROIT AÉRIEN EXISTANTS

(Note présentée par la République dominicaine)

1. GÉNÉRALITÉS

1.1 À sa 41e session, l'Assemblée de l'OACI a déterminé que certains actes ou délits, y compris les cybermenaces, qui inquiètent la communauté aéronautique internationale, ne sont peut-être pas dûment traités dans les instruments de droit aérien existants. C'est pourquoi elles ont été abordées dans le cadre de travaux juridiques sur la cybersécurité. Nous comprenons que les efforts déployés à cet égard au cours des dernières décennies ont toujours eu pour but de s'adapter aux problèmes actuels. En 2022, le Secrétariat a présenté un rapport du Sous-groupe de recherche sur les aspects juridiques à la 38e session du Comité juridique, réuni à Montréal, rapport dans lequel il a été indiqué que le cadre existant du droit aérien international était partiellement adapté aux cybermenaces contre l'aviation civile.

1.2 Lors des délibérations du Forum des conseillers juridiques en aviation civile (16 et 17 mai 2019), Singapour a présenté des conclusions et des recommandations selon lesquelles les enjeux et les vulnérabilités relatives à la cybersécurité et à la cybersûreté étaient des sous-produits de l'ère numérique. Cette question ne se limite pas aux activités aéronautiques, mais à toutes les activités de la société. Par conséquent, d'un point de vue juridique également, l'aviation peut être abordée comme d'autres secteurs. Aucune ressource ne devrait être épargnée pour relever les défis du cyberespace touchant la sûreté de l'aviation civile. Il faut envisager la question de manière globale, de sorte que les mesures soient déployées dans tous les domaines du secteur. Dans le cas contraire, d'autres lacunes juridiques apparaîtront.

1.3 Nous sommes d'accord avec la Stratégie 2019 de l'OACI pour la cybersécurité de l'aviation, laquelle énonce que « [l]'objectif principal de la législation et de la réglementation internationale, régionale et nationale et sur la cybersécurité de l'aviation civile est d'appuyer la mise en œuvre d'une stratégie exhaustive de cybersécurité afin de protéger l'aviation civile et les voyageurs des effets des cyberattaques ». Cette stratégie dispose donc que « [le]s États membres doivent veiller à ce qu'une législation des règlements appropriés soit formulée et appliquée, conformément aux dispositions de l'OACI, avant de mettre en œuvre une politique nationale de cybersécurité de l'aviation civile ». Des progrès notables ont évidemment été réalisés dans le domaine de la technologie et donc de l'aviation. Il s'ensuit que chaque État a pris des mesures relatives à la transformation numérique, aux cyberattaques, aux

[1] Version en langue espagnole fournie par la République dominicaine.

cybermenaces, à la vie privée et à la protection des données ; et que, dans certains cas, il n'est peut-être pas nécessaire de modifier les directives, lignes directrices, politiques et réglementations nationales et internationales tenant compte des aspects liés à la cybersécurité, en particulier en ce qui a trait à la sûreté et à la sécurité de l'aviation.

1.4 Dans le cadre du Plan d'action 2022 de l'OACI pour la cybersécurité, « [l]États sont encouragés à évaluer leurs cadres juridiques actuels à l'égard de la cybersécurité et de l'aviation civile afin de détecter d'éventuelles lacunes et de s'assurer que la législation appropriée est en place pour les éléments spécifiques de la cybersécurité dans l'aviation civile ». Un autre élément clé est le mécanisme d'application que les États sont encouragés à mettre en œuvre, s'il n'existe pas déjà dans leur cadre législatif national, pour criminaliser les actes de cyberattaque visant l'aviation civile et engager les poursuites nécessaires.

2. ANALYSE

2.1 En 2019, dans le cadre de la Stratégie de cybersécurité de l'OACI, les États ont été invités à examiner s'il convenait de mettre à jour leur législation nationale et, par conséquent, d'adopter une nouvelle législation nationale permettant d'engager des poursuites pour des cyberattaques liées au terrorisme et des attaques visant l'aviation civile. Des lois et des règlements pertinents existent sans doute. Cependant, étant donné qu'en droit, il est essentiel de définir les infractions pour que les sanctions correspondantes soient correctement appliquées, il est urgent que les États disposent de lignes directrices claires et uniformes. Il ne suffit pas de reconnaître l'importance de la cybersécurité dans l'aviation civile internationale. Des lignes directrices ont été publiées, mais la technologie évolue plus vite que nous et nous essayons toujours de la rattraper. Le moment est venu d'établir les obligations juridiques et les responsabilités des États dans ce domaine.

2.2 Des normes facultatives non contraignantes existent, de même que des normes non facultatives contraignantes, comme celles de l'Annexe 17 ; mais il est nécessaire d'établir les moyens d'appliquer les principes du droit international à cet égard et, en même temps, d'approfondir les normes nationales. Les limites actuelles de chaque nation, qu'elles soient législatives ou technologiques, ne nous permettent pas de voir au-delà des probabilités de menaces pesant sur des situations dont il est estimé qu'elles sont corrigées.

2.3 En République dominicaine, la législation, par exemple la loi n° 53-07 (2007), couvre les crimes et délits de haute technicité. Toutefois, nous estimons que les cybermenaces pesant sur l'aviation civile qui se présentent ou pourraient se présenter à l'avenir ne sont pas nécessairement couvertes ou définies dans la loi ou dans notre code pénal. Nous faisons ici référence au cyberterrorisme et au cyberespionnage, ainsi qu'aux attaques contre des infrastructures critiques. En outre, la plupart des affaires traitées par le ministère public concernent l'exécution publique de plaintes privées, c'est-à-dire que la personne concernée doit déposer une plainte et collaborer avec le ministère public tout au long de la procédure, l'accusé peut donc rester impuni. Les définitions doivent être telles que toute affaire traitée soit purement et simplement publique.

2.4 Les organismes de réglementation tendent à imputer les menaces et/ou les failles aux technologies de l'information et de la communication (TIC) ou aux technologies opérationnelles. Certes, ces dernières décennies, l'accent a été mis sur la sécurité des TIC dans tous les domaines administratifs et techniques. Il n'en va cependant pas de même pour les technologies opérationnelles, étant donné que la mise en œuvre de certaines garanties se fait au détriment de l'efficacité de leur fonctionnement dans des domaines tels que la navigation aérienne et les règles de vol. La question de l'efficacité par rapport à la sécurité fait l'objet d'un débat constant.

2.5 La République dominicaine a pris des mesures conformément à sa constitution, en particulier en son article 260, pour s'assurer que les innovations technologiques et leur impact sur l'aviation civile ne mettent pas en danger la sécurité, tout en accordant un fort degré de priorité aux objectifs nationaux suivants : lutter contre l'activité criminelle transnationale, qui met en danger les intérêts de la République et de ses habitants ; et organiser et tenir à jour des systèmes efficaces qui préviennent ou atténuent les dommages causés par les catastrophes naturelles et technologiques.

2.6 En outre, le décret n° 230-18, publié le 19 juin 2018, a établi la Stratégie nationale de cybersécurité 2018-2021 et créé le Centre national de cybersécurité. L'équipe d'intervention en cas de cyberincident sert de point de contact à l'échelle nationale pour la prévention, la détection et la gestion des incidents visant les systèmes d'information gouvernementaux et les infrastructures critiques.

2.7 En 2024, un projet de loi sur la gestion globale de la cybersécurité en République dominicaine est actuellement examiné par le Congrès de la République. Il vise à renforcer le cadre réglementaire de la gestion de la cybersécurité des infrastructures TIC de l'administration publique et des infrastructures critiques dans l'ensemble du pays. Une fois le projet de loi approuvé, le Conseil national de cybersécurité sera constitué en tant qu'organe collégial et autorité suprême du Centre national de cybersécurité, chargé d'établir et de diriger les politiques de gestion du numérique pour les infrastructures TIC de l'administration publique et les infrastructures critiques.

2.8 Ce projet de loi reconnaît les principes énoncés le 12 novembre 2018 dans l'Appel de Paris pour la confiance et la sécurité dans le cyberespace et dans le rapport final de novembre 2019 de la Commission mondiale sur la stabilité du cyberespace. Il couvre, sans distinction, les principes de l'assistance mutuelle, de la prévention des activités illicites, de l'échange d'informations, de la protection des droits de l'homme et de la protection des infrastructures critiques, entre autres.

2.9 Il est important de préciser que, bien que le Centre national de cybersécurité existe depuis 2018, en vertu du projet de loi, il serait rattaché au ministère de la présidence en tant qu'entité de droit public dotée d'une personnalité juridique et d'une autonomie fonctionnelle, budgétaire, administrative, technique et fiscale. L'objectif est de donner au Centre une plus grande indépendance dans l'exécution de ses fonctions.

2.10 De même, le projet de loi traite des infrastructures critiques et des informations sur les incidents de cybersécurité, à savoir les moyens de reconnaître ces incidents, le cadre permettant de les désigner, les procédures administratives correspondantes et une analyse des risques. Il définit les cyberincidences significatives et le système de sanctions. Le projet de loi s'efforce de couvrir des points qui n'ont pas été pris en compte jusqu'à présent.

3. CONCLUSION

3.1 De toute évidence, une action réussie face aux menaces et aux incidents de cybersécurité doit reposer sur un cadre qui réglemente l'adoption de mesures préventives, la gestion de réponses efficaces et la réglementation des infrastructures. Nous sommes confrontés à une situation qui affectera toutes choses, et tout le monde ; c'est donc dans cette optique qu'il faut y faire face. La République dominicaine considère la cybersécurité comme une question de sécurité nationale et a donc pris les mesures correspondantes.

3.2 Nous encourageons les États qui n'ont pas encore pris de telles mesures à le faire avec le même enthousiasme. Nous recommandons à tous les États qui n'ont pas réfléchi à la question d'évaluer leur législation pénale et procédurale, en considérant ce type d'infraction comme un acte public contre la sécurité nationale. Nous demandons également que les infractions pénales comme le cyberterrorisme et le

cyberespionnage soient prises en considération et actualisées, afin qu'elles puissent faire l'objet de poursuites et être correctement définies aux fins de protection de la sûreté de l'aviation, tant au niveau national qu'international. La terminologie devrait également être élargie pour inclure les nouveaux types de cyberattaques et de cybermenaces qui ont vu le jour ces dix dernières années.

— FIN —